

Written Supervisory Procedures Manual

CIM Securities, LLC

Effective: January 2024

Amended Dates: February 1, 2024;

TABLE OF CONTENTS

INTRODUCTION	14
1 DESIGNATION OF SUPERVISORS AND OFFICES	15
1.1 Designation Of Supervisors	15
1.2 Designation Of Offices	15
2 GENERAL EMPLOYEE POLICIES	16
2.1 Standards Of Conduct	16
2.2 Outside Business Activities	16
2.3 Private Securities Transactions	17
2.4 Employee And Employee Related Accounts	18
2.4.1 Employee And Employee Related Accounts Defined	18
2.4.2 Outside Accounts	19
2.4.3 Review Of Transactions	20
2.4.4 Insider Trading	21
2.4.5 Sharing In Accounts	21
2.4.6 Prohibition On Purchases Of Initial Public Offerings (IPOs)	22
2.4.7 Research Restrictions	22
2.4.8 Restrictions On Personal Accounts Of Certain Firm Personnel	22
2.5 Gifts, Gratuities And Entertainment	22
2.5.1 Gifts To Others	23
2.5.2 Accepting Gifts	24
2.5.3 Entertainment	24
2.5.4 Gifts Or Payments To Public Officials Under State Laws	25
2.6 Privacy Policy	25
2.7 Reporting Possible Law Or Rule Violations	26
2.7.1 Reporting	27
2.7.2 Confidentiality Of Employee Reporting	27
2.7.3 Notification Of Chief Compliance Officer	27
2.7.4 Investigation	27
2.7.5 Anti-Retaliation	27
2.7.6 Federal Whistleblower Laws And Rules	28
2.8 Solicitation Of Charitable Contributions	28
2.9 Media Contact Is Limited To Certain Authorized Employees	28
2.10 Requests For Information From Outside Sources	29
2.11 Internal Reviews And Investigations	30
2.12 Internal Disciplinary Actions	30
2.12.1 When Disciplinary Action Is Considered	30
2.12.2 Who Determines Disciplinary Action	30
2.12.3 Types Of Discipline	30
2.12.4 Additional Action	31
2.12.5 Considerations In Determining Type Of Discipline	32
2.13 Employee Obligation To Notify The Firm And The Firm's Obligation To Report	32
2.13.1 Reporting Requirements	33
2.14 Money Laundering	34
2.14.1 Background	34
2.14.2 Shell Companies	35
2.14.3 Penalties	35
2.14.4 Treasury Dept. OFAC List	36
2.14.5 Preventing Money Laundering	36
2.14.6 Cash Deposits Not Accepted	39
2.14.7 Reports Of AML Non-Compliance And Other Potential Crimes	39
2.14.8 Currency Transaction Reporting	40

2.14.9 Recordkeeping Requirements	40
2.14.10 AML Compliance Officer	40
2.14.11 Identity Theft.....	41
2.15 Cybersecurity	42
2.16 Emergency Business Recovery Procedures	43
2.17 Prohibited Activities	43
2.17.1 Use Of Firm Name	44
2.17.2 High Pressure Sales Tactics	44
2.17.3 Providing Tax Advice Not Permitted	44
2.17.4 Rebates Of Commission	44
2.17.5 Sharing Commissions Or Fees With Non-Registered Persons	44
2.17.6 Accepting Compensation From Others	44
2.17.7 Settling Complaints Or Errors Directly With Customers	45
2.17.8 Borrowing From And Lending To Customers	45
2.17.9 Personal Funds Deposited In Customer Accounts	45
2.17.10 Prohibition Against Guarantees.....	45
2.17.11 Fees And Other Charges	46
2.17.12 Customer Signatures.....	46
2.17.13 Rumors	46
2.17.14 Misrepresentations	46
2.17.15 Bribes	47
2.17.16 Acting Without Registration	47
2.18 Cybersecurity Policy	47
2.19 Computer Records, Equipment And Software.....	48
2.19.1 Laptop Computers And Other Mobile Devices	49
2.19.2 Reporting Lost Devices	49
2.19.3 Identifying And Reporting Data Breaches	49
2.19.4 Software	49
2.19.5 Prohibited Downloading	49
2.20 Electronic Communications Policy	50
2.20.1 Failure To Comply	51
2.20.2 Consent To Policy	51
2.21 Advertising And Publishing Activities.....	51
2.22 Employees Acting As Trustees, Executors, Or Other Fiduciary Capacities	52
2.23 Use Of Titles	52
2.24 Annual Certification.....	52
3 TRAINING AND EDUCATION	53
3.1 Annual Compliance Meeting.....	53
3.2 Continuing Education.....	54
3.2.1 Regulatory Element.....	54
3.2.2 Firm Element	55
3.2.3 Registered Persons Who Fail To Complete Requirements	57
3.2.4 Maintaining Terminated Persons' Registration	57
4 EMPLOYMENT, REGISTRATION AND LICENSING.....	58
4.1 Employment.....	58
4.1.1 Hiring Procedures.....	58
4.1.2 Termination Procedures	64
4.2 Registration And Licensing	66
4.2.1 Persons Registered Prior To October 1, 2018	67
4.2.2 Registered Representatives	67
4.2.3 Registered Principals	67
4.2.4 Expiration Of Registrations.....	69
4.2.5 Persons Exempt From Registration	69
4.2.6 FSAWP Waivers.....	69
4.2.7 Other Registrations	69
4.2.8 Qualified Persons Serving In The Armed Forces.....	70

4.2.9 CRD Electronic Filings	70
4.2.10 State Registrations	70
4.2.11 Parking Registrations	70
4.2.12 Form U4.....	70
4.2.13 Amendments To Form U4 Or Form U5.....	71
4.2.14 Assignment Of RR Numbers (IF APPLICABLE)	71
4.2.15 Maintaining Terminated Persons' Registration	71
4.3 Statutorily Disqualified Persons	71
4.3.1 Introduction	72
4.3.2 Hiring Or Retaining Employment Of A Statutorily Disqualified Person	72
4.3.3 Regulatory Filings.....	72
4.3.4 Supervision	73
4.3.5 Reporting Statutory Disqualifications	73
4.4 Broker-Dealer Registration	73
4.4.1 Form BD	73
4.4.2 Member Application And Associated Person Registration (MAP Rules)	74
4.4.3 Regulatory Contact Information.....	74
4.4.4 FINRA Entitlement Program	75
4.4.5 Regulatory Filings.....	75
4.4.6 Reporting Requirements	75
4.5 Heightened Supervision.....	76
4.5.1 Introduction	77
4.5.2 Identifying Employees For Heightened Supervision	77
4.5.3 Criteria For Identifying Candidates For Heightened Supervision	77
4.5.4 Heightened Supervision Memorandum	77
4.5.5 Scope Of Potential Heightened Supervision	78
4.5.6 Certification By RR's Supervisor	78
5 COMMUNICATIONS WITH THE PUBLIC	79
5.1 Introduction	79
5.2 Definitions	79
5.3 Retail Communications.....	80
5.3.1 FINRA Filing Requirements.....	81
5.4 Institutional Communications	82
5.5 General Standards.....	83
5.5.1 Comparisons	84
5.5.2 Disclosure Of The Firm's Name	84
5.5.3 Use Of Non-Member Or OBA Names (DBAs)	84
5.5.4 Tax Considerations	85
5.5.5 Disclosure Of Fees, Expenses And Standardized Performance	85
5.5.6 Recommendations	85
5.5.7 Prospectuses Filed With The SEC	86
5.5.8 Limitations On Use Of FINRA's Name And Any Other Corporate Name Owned By FINRA	86
5.6 Approval.....	86
5.7 SIPC Membership.....	87
5.8 Recordkeeping Requirements For Retail And Institutional Communications.....	88
5.9 Outgoing Communications	88
5.9.1 Sending Communications From Personal Computers And Other Non-Firm Facilities	88
5.9.2 Review And Approval	89
5.9.3 Content Guidelines	90
5.9.4 Letters And Notes.....	91
5.9.5 Research (Not applicable at Present)	91
5.9.6 Other Communications Defined As "Research"	91
5.10 Incoming Correspondence.....	92
5.10.1 Review Of Incoming Correspondence	92
5.10.2 Offices Without Resident Supervisors.....	93
5.10.3 Personal Mail.....	93

5.10.4 Inter-Office Communications	93
5.10.5 Internal Use Only	94
5.10.6 Squawk Box, Conference Calls, And Other Internal Communication Systems	94
5.11 Complaints	94
5.11.1 Complaint Defined	95
5.11.2 Handling Of Customer Complaints	95
5.11.3 Oral Complaints	95
5.11.4 Complaints Received By Clearing Firm (Not applicable at Present)	96
5.11.5 Records Of Complaints	96
5.11.6 Notice To Customers	96
5.11.7 Reporting Of Customer Complaints	96
5.12 Customer Privacy Policies And Procedures	97
5.12.1 Introduction	97
5.12.2 "Public" vs. "Nonpublic" Personal Information About Customers	97
5.12.3 Sharing Nonpublic Financial Information	98
5.12.4 Customer Notification	98
5.12.5 Affiliate Marketing	98
5.12.6 Introduction	99
5.12.7 Telephone Calls	99
5.12.8 Wireless Communications	100
5.12.9 Outsourcing Telemarketing	100
5.12.10 Unencrypted Consumer Account Numbers	100
5.12.11 Submission Of Billing Information	100
5.12.12 Abandoned Calls	100
5.12.13 Credit Card Laundering	101
5.12.14 Other Prohibited Activities	101
5.12.15 Do Not Call Lists	101
5.12.16 National Do-Not-Call Registry	102
5.12.17 State Restrictions	102
5.12.18 Internal Do Not Call List	102
5.12.19 Facsimile Transmissions	102
5.12.20 Established Business Relationship	102
5.13 Public Appearances	103
5.13.1 General Guidelines	104
5.13.2 Seminars	104
5.13.3 Approval	104
5.13.4 Radio, TV, And Other Extemporaneous Presentations	104
5.13.5 Securities Sold By Prospectus	105
5.13.6 Options (NOT APPLICABLE AT PRESENT)	105
5.13.7 Collateralized Mortgage Obligations (CMOs)	105
5.13.8 Mutual Funds	105
5.13.9 Cold Caller Requirements	105
5.13.10 Permissible Cold Caller Activities	105
5.13.11 Prohibited Cold Caller Activities	106
5.13.12 Telemarketing Restrictions	106
5.13.13 Scripts	106
5.14 Electronic Communications	106
5.14.1 Electronic Communications Systems And Devices	106
5.14.2 Education And Training	106
5.14.3 Commercial E-Mail Procedures	107
5.14.4 Review Of Electronic Communications	107
5.14.5 Advertising	109
5.14.6 Internet	109
5.14.7 Hyperlinks	111
5.14.8 Prohibition Against Automatic Erasing/Deleting	111
5.14.9 Policy Violations	112

5.15 Identification Of Sources	112
6 FINANCIAL AND OPERATIONS PROCEDURES	113
6.1 Qualification Of Operations Personnel	113
6.2 Books And Records	113
6.2.1 Introduction	113
6.2.2 Electronic Storage Of Records	114
6.2.3 Availability Of Records In Offices	115
6.3 Calculation And Reporting Of Net Capital	115
6.4 Reports	115
6.4.1 Annual Audit Report	116
6.4.2 Risk Reports	116
6.4.3 Custody Report And Requirements	116
6.4.4 Exemption Report.....	116
6.5 Reconciliations And Bank Records	117
6.6 Designation Of Accountant	117
6.7 Guarantees By, Or Flow Through Benefits For, Members	117
6.8 General Ledger And Suspense Accounts	118
6.9 Financial Reporting	119
6.9.1 Part-Time, Off-Site Or Multiply Registered FINOP.....	119
6.9.2 Financial Statements	119
6.9.3 Disclosure Of Financial Condition	120
6.9.4 Notification Rule ("Early Warning Rule")	120
6.10 Regulation T And Extension Of Credit To Customers – NOT APPLICABLE AT PRESENT	120
6.10.1 Compliance With Regulation T – If applicable	121
6.10.2 Customer Margin Balance Report – If applicable.....	121
6.11 Fees And Service Charges.....	121
6.11.1 Notification Of Customers	122
6.12 Fidelity Bonding	122
6.13 Independent Verification Of Assets	122
6.14 Cash Deposits Not Accepted.....	122
6.15 Cash Equivalents.....	123
6.16 Risk Management.....	123
6.16.1 Risk Practices Regarding Employment And Employees	123
6.16.2 New Accounts	124
6.16.3 Technology Management.....	125
6.16.4 Protection Of Customer Information And Records.....	125
6.16.5 Credit Risk Management.....	126
6.16.6 Liquidity Risk Management	126
6.16.7 New Products	127
6.17 Business Continuity Plan	128
6.17.1 Designation Of Responsibilities.....	128
6.17.2 Retention And Location Of The Plan.....	129
6.17.3 Implementation Of The Plan.....	129
6.17.4 Emergency Response Team.....	130
6.17.5 Emergency Contact List	130
6.17.6 Alternative Business Locations	130
6.17.7 Data Back-Up And Recovery	130
6.17.8 Mission Critical Systems	131
6.17.9 Financial And Operational Assessments	131
6.17.10 Alternative Market Entry	132
6.17.11 Alternative Communications.....	132
6.17.12 Regulatory Reporting	133
6.17.13 Business Constituent, Bank, And Counter-Party Impact	133
6.17.14 Other Obligations To Customers.....	134
6.17.15 Emergency Contact Information.....	135
6.17.16 Widespread Health Emergencies.....	135

6.17.17 Education Of Employees.....	136
6.17.18 Updating, Annual Review, And Testing.....	136
6.18 Industry Testing	137
6.19 Customer Payments For Purchases.....	137
6.19.1 Checks Payable To Clearing Firm	137
6.19.2 Guaranteed Accounts – Not applicable at present	137
6.20 Transmittals Of Customer Funds And Securities	138
6.20.1 Checking Account Safeguards	138
6.20.2 Prepayments And Extensions	138
6.20.3 Employees Authorized To Transmit Customer Assets From Accounts	138
6.20.4 Issuing Checks To Customers	139
6.20.5 Persons Receiving Assets In Person	139
6.20.6 Transmittals To Third Parties	139
6.20.7 Authorization Records For Negotiable Instruments Drawn From A Customers Account – If Applicable	140
6.20.8 Transmittals To An Alternate Address	140
6.20.9 Transmittals To Outside Entities	140
6.20.10 Transmittals Between Customers And Registered Representatives	140
6.20.11 Suspicious Or Questionable Activities	141
6.21 Customer Protection	141
6.21.1 Introduction.....	141
6.21.2 Exemptions.....	141
6.22 Customer Confirmations And Statements - Not applicable at Present	143
6.22.1 Confirmations – Not applicable at Present.....	143
6.22.2 Customer Statements Only Are Provided To Customers – Not applicable at Present	144
6.22.3 Control Of Blank Confirmations And Statements – Not applicable at Present	144
6.22.4 Undeliverable Mail	144
6.22.5 Holding Customer Mail Prohibited.....	145
6.23 Lost Securityholders And Unresponsive Payees – Not applicable at Present	145
6.23.1 Searches For Lost Securityholders	145
6.23.2 Unnegotiated Checks	145
6.24 Subordination Agreements With Investors	145
6.25 Expense-Sharing Agreements.....	146
6.26 Electronic Delivery And Signatures	146
6.26.1 Electronic Delivery To Customers	146
6.26.2 Electronic Signatures	147
6.26.3 FINRA Access	147
6.27 Transfer Of Accounts – Not applicable at Present	147
6.28 Solicitation Of Proxies.....	147
6.29 Customer Requests For References	147
6.30 Audit Letters.....	148
6.31 Annual Disclosure Of FINRA BrokerCheck	148
6.32 Carrying Agreements – Not applicable at Present	148
6.33 Clearing Firm Exception Reports – Not applicable at Present	148
6.34 Short Interest Report	149
6.35 Electronic Blue Sheets.....	149
6.36 Regulatory Fees And Assessments	149
6.37 Regulatory Requests	149
6.37.1 Information Provided Via Portable Media Device.....	150
6.38 Outsourcing	150
6.38.1 Cybersecurity.....	150
6.38.2 Books And Records.....	151
7 ANTI-MONEY LAUNDERING (AML) PROGRAM	152
7.1 Introduction	152
7.1.1 Definitions.....	152
7.2 AML Compliance Officer.....	152

7.3 Independent Testing	154
7.4 Training Program	154
7.5 Bank Secrecy Act (BSA) Filings	155
7.6 OFAC List And Blocked Property	155
7.6.1 Prohibited Transactions.....	156
7.6.2 Risk Factors.....	156
7.6.3 Blocking Requirements	157
7.6.4 Monitoring Procedures	158
7.6.5 Other Requests To Monitor Accounts	158
7.6.6 Blocking Property And Disbursements.....	158
7.6.7 Reporting Blocked Property And Legal Actions	158
7.6.8 Role Of Operations Personnel	159
7.7 Currency Reporting Requirements	159
7.7.1 Transactions Involving Currency Over \$10,000	160
7.7.2 Transactions Involving Currency Or Bearer Instruments Over \$10,000 Transferred Into Or Outside The U.S.....	160
7.7.3 State Reporting Requirements.....	160
7.8 Foreign Financial Account Reporting Requirements And Recordkeeping (FBAR)	160
7.9 Recordkeeping Requirements (Joint Rule and Travel Rule)	161
7.9.1 Fund Transfers And Transmittals	161
7.9.2 Other Recordkeeping Requirements.....	162
7.10 DVP/RVP Accounts	162
7.11 Omnibus Accounts And Transactions In Low-Priced Securities	162
7.12 Detecting Potential Money Laundering.....	163
7.12.1 Clearing Firm AML Procedures – Not applicable at Present	164
7.12.2 Foreign Currency Transactions	164
7.12.3 IPOs In Emerging Markets	164
7.13 Information Sharing Between Financial Institutions	165
7.14 Suspicious Activities	165
7.14.1 Identifying Potential Suspicious Activity	166
7.14.2 When A Report Must Be Filed.....	166
7.14.3 Filing A Report And Emergency Notification	167
7.14.4 Retention Of Records.....	167
7.14.5 Providing SARs Information To SROs	167
7.14.6 Prohibition Against Disclosure.....	168
7.14.7 Politically Exposed Persons (PEP)	168
7.15 Requests And Written Notices From Regulators, Enforcement Agencies, And Other Authorized Persons	168
7.15.1 Federal Banking Agency Requests -- 120-Hour Rule.....	168
7.15.2 Information Sharing With Enforcement Agencies	169
7.15.3 National Security Letters	169
7.15.4 Grand Jury Subpoenas	169
7.15.5 Foreign Bank Correspondent Accounts	170
7.15.6 Requests By Law Enforcement To Maintain Accounts	170
7.16 Accounts Requiring Approval By The AML Compliance Officer.....	170
7.17 Customer Identification Program (CIP).....	171
7.17.1 Definition Of Customer Under CIP Rule.....	171
7.17.2 Accounts Opened By Other Financial Institutions.....	171
7.17.3 Master Accounts And Sub-Accounts.....	173
7.17.4 Customer Due Diligence (CDD)	174
7.17.5 CIP Records	182
7.17.6 Comparison With Government Lists	182
7.18 Identity Theft Prevention Program (Red Flags Rule)	183
7.18.1 Introduction – ITPP Not Applicable at Present Time (7.18.1-7.18.3)	184
7.18.2 Establishment, Administration, And Updates Of The ITPP	184
7.18.3 Red Flags	185

7.18.4 Identifying And Responding To Red Flags.....	185
7.18.5 Compromised Accounts	188
7.19 Due Diligence For Correspondent And Private Banking Accounts	189
7.19.1 Definitions.....	190
7.19.2 Due Diligence For Correspondent Accounts For Foreign Financial Institutions	191
7.19.3 Due Diligence For Private Banking Accounts	193
7.19.4 Enhanced Scrutiny For Accounts Of Senior Foreign Political Figures.....	194
7.20 Shell Companies.....	194
8 INSIDER TRADING	196
8.1 Insider Trading Policies And Procedures	197
8.2 Prohibition Against Acting On Or Disclosing Inside Information.....	197
8.3 Tippees Are Insiders.....	197
8.4 Misuse Constitutes Fraud	198
8.5 Annual Certification.....	198
8.6 Firm Policy Memorandum Regarding Insider Trading.....	198
8.7 Employee, Employee-Related, And Proprietary Trading.....	201
8.8 Watch List	201
8.9 10b5-1 Plans.....	202
9 ACCOUNTS	204
9.1 New Accounts.....	204
9.1.1 Trusted Contact Person	204
9.1.2 Regulation Best Interest (BI)	205
9.1.3 Designation Of Accounts.....	205
9.1.4 Anti-Money Laundering (AML) New Account Requirements	205
9.1.5 Customer Due Diligence (CDD)	208
9.1.6 SIPC Disclosure	216
9.1.7 Approval	216
9.1.8 Customer Account Information.....	216
9.1.9 Addresses On Customer Accounts	217
9.1.10 Account Documents	217
9.1.11 Predispute Arbitration Agreements With Customers	217
9.1.12 Revisions To Customer Agreements	218
9.1.13 Accounts Requiring Notification To Customer's Employer.....	218
9.1.14 Post Office Addresses.....	219
9.1.15 Unacceptable Accounts.....	219
9.2 Transferring Accounts.....	219
9.2.1 Accounts Transferring In – Not applicable at Present.....	219
9.2.2 Accounts Transferring Out – Not applicable at Present.....	219
9.3 Accounts And Securities Subject To Blocking.....	219
9.4 Updating Account Information And Periodic Affirmation	220
9.5 Sweep And Cash Management Account (CMA) Programs.....	220
9.6 Margin Accounts – Not applicable at Present.....	221
9.6.1 Opening Margin Accounts	221
9.6.2 Employee Accounts.....	221
9.6.3 Disclosures	221
9.6.4 Equal Credit Opportunity Act Requirements	222
9.6.5 Arranging Credit	223
9.6.6 Suitability/Regulation BI	223
9.6.7 Margin Requirements	223
9.6.8 New Issues	223
9.6.9 Credit On Restricted Securities	223
9.6.10 Fiduciary Accounts	223
9.6.11 Portfolio Margin Accounts	223
9.7 Third Party Accounts	224
9.8 Discretion For Orders And Accounts	224
9.9 Accounts For Minors – If applicable	225

9.10 Coverdell Education Savings Accounts – If applicable	225
9.11 Accounts For Senior Investors	226
9.11.1 General Requirements	227
9.11.2 Opening Accounts For Specified Adults	228
9.11.3 Recommendations To Senior Investors	228
9.11.4 Diminished Mental Capacity	229
9.11.5 Potential Indication Of Elder Financial Exploitation	229
9.11.6 Escalating Issues Involving Senior Investors	230
9.11.7 Financial Exploitation - Temporary Holds	230
9.11.8 Reverse Mortgages- Not applicable at Present	231
9.11.9 Luncheon Programs And Seminars	231
9.11.10 Advertising Targeting Seniors	232
9.12 Incompetent Persons	232
9.13 Trust Accounts	232
9.14 Registered Persons (RRs) Being A Customer's Beneficiary Or Holding A Position Of Trust	233
9.15 Correspondent And Private Banking Accounts And Accounts For Senior Foreign Political Figures	234
9.15.1 Summary Of Requirements	234
9.15.2 Definitions	234
9.15.3 Prohibition Against Correspondent Accounts For Foreign Shell Banks	235
9.15.4 Foreign Bank Certification	235
9.15.5 Accounts For Foreign Political Figures	235
9.16 Wealth Events	235
9.17 Pension And Retirement Accounts - Non-Fiduciary	236
9.17.1 Recommendations and Fiduciary Status Prohibited	236
9.17.2 Fiduciary Status Defined – Replaced by Reg BI. Please refer to Reg BI section of this manual	236
9.17.3 Disclosures To Plans	237
9.17.4 Individual Retirement Accounts (IRAs)	238
9.17.5 Employer-Sponsored Plans	239
9.17.6 Definitions	241
9.18 Foreign Accounts	243
9.19 Payments To Unregistered Persons	243
9.19.1 Definition Of Eligibility	244
9.19.2 Referrals	244
9.19.3 Referrals To Others	245
9.19.4 Referrals To The Firm	245
9.20 Death Of A Customer	246
9.21 Active Accounts	246
9.22 Concentrations – Not applicable at Present	247
10 SUPERVISORY SYSTEM, PROCEDURES, AND CONTROLS	248
10.1 Introduction	248
10.2 Responsibility	249
10.3 Controls	249
10.3.1 Verification And Testing	249
10.3.2 Risk Management	249
10.3.3 Outside Auditors	250
10.4 Written Compliance And Supervisory Procedures	250
10.5 Chief Compliance Officer (CCO)	250
10.6 Internal Inspections	251
10.7 Review And Testing Of Procedures And Controls	252
10.7.1 Conducting Risk-Based Reviews And Testing	252
10.7.2 Findings And Follow-Up	252
10.8 Internal Investigations Of Transactions	253
10.8.1 Internal Investigation Reports	253
10.9 Escalation Of Issues	254
10.10 Annual Report And Certification Of Compliance And Supervisory Processes	254
10.10.1 Meetings Between CEO And CCO	254

10.10.2 Annual Report To CEO	254
10.11 Supervision Of Supervisors	255
10.11.1 Supervision Of Customer Account Activity	256
10.12 Conflicts Of Interest	257
10.13 Cross Reference To Other Supervisory Control Subjects	257
11 OFFICES	259
11.1 Office Designations	259
11.1.1 Branch Office	260
11.1.2 Non-Branch Locations	260
11.1.3 Offices Of Supervisory Jurisdiction (OSJ)	261
11.1.4 Branch Offices Assigned To OSJs	262
11.2 Approval Of Persons To Operate In Non-Branch Locations	262
11.2.1 Primary Residence Offices	262
11.3 Supervision Of Non-Branch Locations	263
11.4 Supervision Of Producing Managers	263
11.5 Office Records	263
11.5.1 Retention Of Records At The Office	263
11.5.2 Forwarding Records To Home Office	264
11.5.3 Access To Records	264
11.5.4 Regulatory Requests For Records	264
11.6 Changes In Branch Offices	265
11.7 Closing Offices	265
11.8 Use Of Office Space By Others	265
11.9 Cybersecurity	266
11.9.1 Branch Technical Controls	267
11.10 Office Inspections	267
11.10.1 Risk-Based Inspection Cycle	268
11.10.2 Conducting Inspections	269
11.10.3 Temporary Relief For Remote Inspections	269
11.10.4 Reports	269
11.11 Display Of Certificates	270
11.12 Availability Of Rules	270
12 INVESTMENT BANKING	271
12.1 Introduction	271
12.2 Information Barrier and Confidentiality Issues	271
12.2.1 Information Barrier Procedures	271
12.2.2 Origination Meeting Process And Information Sharing	271
12.3 Restricted And Watch Lists	272
12.3.1 Watch List	272
12.3.2 Restricted List	273
12.4 Review Of Investment Banking Business	274
12.5 Investment Banker Personal Investments	275
12.6 Licensing And Registration	276
12.7 Gifts And Entertainment	276
12.8 Participation In Compliance Meetings, Continuing Education, And Internal Audits/Reviews	276
12.9 Inquiries And Investigations	277
12.10 Anti-Money Laundering (AML)	277
12.10.1 Overview Of The Customer Identification Program Of The USA PATRIOT Act	277
12.11 Communications	279
12.11.1 Prohibited Communications Between Bankers And Customers	279
12.11.2 Communication With Other Business Units	279
12.11.3 "Public Side" Employees (Sales and Trading, etc.)	280
12.11.4 Interactions Between Research Analysts And Investment Bankers – Not Applicable at Present (Sections 12.11.4 – 12.11.4.3.2)	280
12.11.5 Emerging Growth Companies (EGCs)	281

12.12 Prohibition Against Offering Favorable Research To Induce Investment Banking Business – NOT APPLICABLE AT PRESENT	282
12.13 New Issues	282
12.14 New Product Approval Process	283
12.15 Pitch Materials	284
12.15.1 Definition	284
12.15.2 Approval Of Pitch Materials	284
12.15.3 Other Disclosures And Guidelines	284
12.15.4 Pitch Materials: Non-Permissible Items	284
12.15.5 Document Retention	285
12.16 Commitment Committee	285
12.17 Commitments	285
12.17.1 Representing Two Sides Of A Banking Transaction	286
12.18 Fairness Opinions	286
12.18.1 Disclosures	287
12.18.2 Approval	287
12.19 Origination, Record Retention, Closed Deal Files	288
12.19.1 Due Diligence	288
12.19.2 Investment Banking's Responsibility	288
12.19.3 Required Document Retention	288
12.19.4 M&A Closed Deal Files – Not applicable at Present	289
13 PRIVATE PLACEMENTS AND OFFERINGS	291
13.1 Introduction	291
13.1.1 Private Securities Offerings Principal	291
13.1.2 Definition Of Terms	291
13.1.3 "Private Placement" Defined	292
13.2 Blue Sky Requirements	292
13.3 The Firm's Participation In Private Placements	293
13.3.1 Due Diligence	293
13.3.2 Agreement With The Issuer	294
13.3.3 Dollar Amount Of The Offering And Integration Issues	294
13.3.4 Form D	294
13.3.5 Submissions To FINRA	295
13.4 Sales Of Private Placements	295
13.4.1 Regulation Best Interest (BI)	295
13.4.2 Restricted Nature Of Private Placement Securities	296
13.4.3 Retail Communications	296
13.4.4 Filing Requirements For Private Placement Of Securities	297
13.4.5 Filing Requirements For Private Placement Of Securities Issued By A Member Firm	297
13.4.6 Purchaser Questionnaires	297
13.4.7 Purchaser Representatives	297
13.4.8 Offering Memorandum	298
13.4.9 Oral Representations	298
13.4.10 Offeree Access To Information	298
13.4.11 Solicitation	298
13.4.12 Investment Seminars Or Meetings	300
13.4.13 Subscription Agreements	300
13.5 Regulation D	301
13.5.1 Disqualification Of Felons And Other "Bad Actors"	301
13.5.2 Due Diligence	302
13.5.3 Investigation Practices	302
13.6 Private Investment In Public Equity (PIPE)	304
13.6.1 Introduction	304
13.6.2 Underwriting	304
13.6.3 Compliance Notification	305
13.6.4 Registration Statement Integration	305

13.6.5 Eligible Investors	305
13.6.6 Marketing Restrictions	305
13.6.7 Information Flow	307
13.7 Conservation Donation Transactions (CDTs) – If applicable	308
13.8 Private Equity Funds	309
14 CYBERSECURITY	310
14.1 Assignment Of Responsibility	310
14.2 Identification Of Risks	310
14.3 Risk Assessments	310
14.3.1 Asset Inventory	311
14.4 Insider Threat	311
14.4.1 Identifying Potentially Malicious Activity	311
14.5 Third Party Vendors	311
14.5.1 Vendor Selection and Due Diligence	312
14.6 Encryption Of Data	312
14.7 Identity Access Management (IAM) and User Entitlements	312
14.7.1 Privileged User Controls	312
14.8 Security Information and Event Management (SIEM) and User and Entity Behavioral Analytic (UEBA) Tools	312
14.9 Data Loss Prevention (DLP)	313
14.10 Penetration Testing (PEN)	313
14.11 Retirement Of Equipment Containing Data	313
14.12 Detection Of Unauthorized Activity	314
14.12.1 Cloud-Based E-mail Account Takeovers (ATOs)	314
14.13 Cybersecurity Incident Response Program	314
14.14 Recovery	315
14.15 Business Continuity/Pandemic Responses	315
14.15.1 Measures for Associated Persons	315
14.15.2 Measures for Firms	316
14.16 Reports To Senior Management	316
14.17 Training	316
14.18 Other Policies	317
15 REGULATION BEST INTEREST (BI)	318
15.1 Summary Of Key Requirements	318
15.2 General Obligations	318
15.2.1 Disclosure	319
15.2.2 Care	320
15.2.3 Conflict Of Interest	323
15.2.4 Compliance	323
15.3 Form CRS	324
15.4 Training	325
15.5 Monitoring Accounts	325
15.5.1 Monitoring	325
15.6 Dual Registrants	326
15.6.1 Recordkeeping	326
15.7 Definitions	326
15.8 Cross References To Sections In This Manual	328
16. INSURANCE PRODUCTS	330

INTRODUCTION

CIM Securities, LLC (CIM Securities) will conduct its business consistent with the highest standards of commercial honor and just and equitable principles of trade. Keeping our customers' interest foremost is key to CIM Securities's success. The trust of our customers and CIM Securities's reputation are of paramount importance. Effective supervision is an integral part of achieving our goals in serving our customers.

"Compliance" is not a static event; it is a process which evolves in tandem with regulations that govern our industry and the circumstances of each particular interaction. This manual includes CIM Securities's supervisory policies and procedures to provide guidance to designated supervisors in their oversight of the Firm's business. It is a working document and reference for supervisors and will be updated when necessary.

It is recognized that supervision must be a flexible tool for use by those charged with managing the Firm's various activities. While it is generally expected these procedures will be followed, supervisors are encouraged to adapt these procedures to the needs of CIM Securities, their particular department, and the employees and customers of CIM Securities. These procedures are meant to be a basic framework upon which supervisors oversee the Firm's activities.

This manual does not attempt to set forth all of the rules and regulations with which employees must be familiar, nor does it attempt to deal with all situations involving unusual circumstances. When questions arise, refer them to Compliance for assistance.

Supervision may be delegated to others, where appropriate; however, designated supervisors are responsible for ultimate supervision of assigned areas. The term "employee" as used in this manual includes RRs (and others as identified by CIM Securities) who may be independent contractors for tax and compensation purposes.

This manual is the property of CIM Securities, LLC (CIM Securities) and may not be provided to anyone outside the Firm without the permission of Compliance or the Firm's counsel.

1 DESIGNATION OF SUPERVISORS AND OFFICES

1.1 Designation Of Supervisors

[FINRA Rule 3110(a)]

This section includes CIM Securities's designated supervisors responsible for supervision of the areas of business indicated.

Amended Dates: 11/14/2023; 12/1/2023; 1/16/2024;

Area/ Department Supervised	Name/Title/ Location of Supervisor	Registration Status	Effective Date of Supervision	RRs Supervised
Establish policies and procedures including supervisory controls and testing of those procedures	Vincent Bruno – CCO	Series 24,79, 7	11-14-2023	John (Jack) Myers Bryan Emerson
	Rico Conte – CEO Banking Principal/IB Supervisor	Series 24,79, 7	11-14-2023; 1-16-2024	
CEO	Rico Conte	Series 24,79, 7	1-16-2024	
CCO	Vincent Bruno	Series 24,79, 7	11-14-2023	
Financial Operations	Marlon Bevaun	Series 27	12-1-2023	

1.2 Designation Of Offices

[FINRA Rule 3110(f); MSRB Rule G-27(b)(iii) and G-27(g)]

AMENDED DATES: JANUARY 2024

CIM Securities maintains the following office(s):

Office Location	Type of Office*	Designated Supervisor(s)	Designated Person To Explain Office Records	Type(s) of Business Conducted at Office
New Jersey	OSJ - MAIN	Rico Conte	Vincent Bruno	Private Placements of Securities
Jack Office	Non-OSJ	Rico Conte	John Myers	Private Placements of Securities

2 GENERAL EMPLOYEE POLICIES

2.1 Standards Of Conduct

[FINRA Rule 2010]

It is CIM Securities's policy and mandate to its employees to conduct CIM Securities's business under the high standards and principles of the rules governing our industry. Employees are expected to deal with customers in a fair and honest way, with the customer's interest of primary concern.

Compliance will distribute compliance policies and procedures to all employees and from time to time will issue updates, as needed.

2.2 Outside Business Activities

[FINRA Rule 3270]

Responsibility	CCO
Resources	<ul style="list-style-type: none">• Requests to engage in outside business activities• Annual certifications• Other potential indicators such as incoming or outgoing correspondence
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Employee's supervisor:<ul style="list-style-type: none">○ Question employee regarding potential unapproved outside business activities referenced in correspondence or other indicators of outside business activity○ Refer requests to Compliance• Compliance:<ul style="list-style-type: none">○ Consider whether the proposed activity will:<ul style="list-style-type: none">▪ Interfere with or otherwise compromise the employee's responsibilities to CIM Securities and its customers▪ Be viewed by customers or the public as part of CIM Securities's business based upon the nature of the proposed activity and the manner in which it will be offered○ Determine whether the activity is an outside business activity or if it would be considered a private securities transaction subject to the requirements of the next section○ Determine any limitations to be imposed prior to approval○ Notify employee of approval/disapproval and any limitations, in writing
Record	<ul style="list-style-type: none">• Retention for 3 years, 2 years in a readily accessible location:<ul style="list-style-type: none">○ Outside Business Activity Request forms including approval/disapproval and any limitations on the activity

	<ul style="list-style-type: none"> ○ Written notification to the employee and his/her supervisor
--	---

Employees are required to disclose to CIM Securities, in writing, any outside business activities and obtain approval prior to engaging in such activity. Charitable activities are not included in this requirement unless the employee is being compensated. This policy applies to all employees (or other relationships such as RRs acting as independent contractors registered with CIM Securities); it does not apply to private securities transactions which are discussed in the next section.

Outside business activities may include a wide range of activities including but not limited to the following:

- Employment with an outside entity
- Acting as an independent contractor to an outside party
- Serving as an officer, director, or partner
- Acting as a finder
- Referring someone and receiving a referral fee
- Receiving compensation or having the reasonable expectation of compensation from any other person as a result of a business activity outside the scope of employment or other relationship with CIM Securities

Compensation may include salary, stock options or warrants, referral fees, or providing of services or products as remuneration. Generally, remuneration consisting of anything of present or future value for services rendered may be considered compensation.

Employees requesting approval to engage in outside business activities must complete the Outside Business Activity Request form and submit it to Compliance **prior to** engaging in the activity. Compliance will approve or disapprove the outside business activity in writing and notify the employee and the employee's supervisor.

2.3 Private Securities Transactions

[FINRA Rule 3280]

Responsibility	CCO
Resources	<ul style="list-style-type: none"> • Requests to engage in private securities transactions • Annual certifications • Indications of potential "selling away" such as in correspondence
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Employee's supervisor: <ul style="list-style-type: none"> ○ Refer requests or indications of private securities transactions to Compliance • Compliance: <ul style="list-style-type: none"> ○ Review requests and certifications ○ Follow up with RR and supervisor regarding indicators of selling away ○ Notify employee by memo (with a copy to the employee's supervisor) whether the private securities transaction is approved ○ If approved: <ul style="list-style-type: none"> ▪ Obtain information regarding outside investor

	<ul style="list-style-type: none"> ▪ Require immediate notification of any transaction as it occurs ▪ Arrange for recording of any transactions on the firm's books and records ▪ Establish required supervision of the outside transactions ○ For unapproved transactions, take corrective action which may include: <ul style="list-style-type: none"> ▪ Disciplinary action against the RR (letter of reprimand; fine, suspension; termination) ▪ Notification to private securities investors that CIM Securities is not associated with the investment
Record	<ul style="list-style-type: none"> • Record of approval or disapproval • Records of transactions and review/action taken • Records of action taken for unapproved transactions

Private securities transactions are defined by FINRA as any securities transaction outside the regular course or scope of an employee's employment with CIM Securities (sometimes referred to as "selling away"). This does not include outside securities accounts approved by CIM Securities, transactions with immediate family members where the employee receives no selling compensation, and personal transactions in investment company and variable annuity securities.

Outside private securities transactions require prior approval by Compliance. Information is required about the outside investor and the transaction which must be reported immediately upon completion and will be recorded on CIM Securities's books and records. Compliance or the designated supervisor will supervise and review all private securities transactions.

RRs should note that promissory notes often are securities. Even if a promissory note is not deemed a security, the RR has the obligation to obtain CIM Securities's permission **before** engaging in any outside business activity involving the offer of promissory notes.

2.4 Employee And Employee Related Accounts

2.4.1 Employee And Employee Related Accounts Defined

[FINRA Rule 3110(d)(4)]

Employee and employee related accounts ("covered accounts") are subject to review by CIM Securities. Covered accounts include:

- the spouse of a person associated with the member;
- a child of the person associated with the member or such person's spouse, provided that the child resides in the same household as or is financially dependent upon the person associated with the member;
- any other related individual over whose account the person associated with the member has control; or
- any other individual over whose account the associated person of the member has control and to whose financial support such person materially contributes.

In addition, accounts subject to review include any account where an employee has a beneficial interest or the authority to make investment decisions (for example, trust accounts, accounts for minors, *etc.*).

2.4.2 Outside Accounts

[FINRA Rule 3210; FINRA FAQs on Rule 3210: <https://www.finra.org/rules-guidance/rulebooks/finra-rules/3210/faq>; NYSE Rule 407]

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• Requests for outside accounts• Annual certifications• Other
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Employee's supervisor:<ul style="list-style-type: none">○ Refer requests to Compliance• Compliance:<ul style="list-style-type: none">○ Review requests and certifications○ Notify employee by memo of approval or disapproval○ Notify firm carrying the employee's outside account by letter regarding to whom duplicate confirmations and statements should be sent. If the carrying firm is a non-member and the ability to receive confirmations and statements is limited, consider whether the account should be approved.○ Review confirmations and statements as they are received. Review for:<ul style="list-style-type: none">▪ Transactions in securities restricted by CIM Securities▪ Transactions in new issues▪ Transactions potentially involving insider trading or other rule/law violation▪ Large debit balances, very active trading, or other trading activity that may be of concern○ For transactions in restricted securities, contact the employee and take corrective action which may include cancellation of the transaction○ For trading activity that may be indicative of law or rule violations, conduct an internal investigation
Record	<ul style="list-style-type: none">• Approval/disapproval of outside account in employee's file• Confirmations/statements initialed and filed in employee's file• Record of internal investigation, if applicable• Quarterly report to FINRA of internal investigations, if CIM Securities engages in investment banking activities

It is the general policy of CIM Securities to require that employees maintain their securities accounts at CIM Securities. Exceptions require written approval by Compliance prior to opening the account. Compliance will request duplicate confirmations and statements from the other dealer carrying the employee's account. This includes accounts with a commodities firm to trade security futures and any accounts where the employee has a beneficial interest.

Accounts for the following where the employee is presumed to have a beneficial interest include:

- a spouse

- a child of the employee or the employee's spouse, provided the child resides in the same household or is financially dependent upon the employee
- any other related individual over whose account the employee has control
- any other individual over whose account the employee has control and to whose financial support the employee materially contributes

There may be exceptions to the presumption if the employee can demonstrate to Compliance that the employee derives no economic benefit from, and exercises no control over, the account.

The employee is also obligated to notify in writing the broker-dealer or other institution prior to opening the account that the employee is associated with CIM Securities. Accounts opened prior to association with CIM Securities are subject to the same approval requirement by Compliance and notification to the carrying institution within 30 days of employment with CIM Securities.

These requirements do not apply to accounts limited exclusively to transactions in unit investment trusts and variable contracts or redeemable securities in mutual funds.

2.4.3 Review Of Transactions

[FINRA Rule 3110(d)]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • Order records • Customer monthly statements
Frequency	<ul style="list-style-type: none"> • Daily (order records) • Monthly (customer monthly statements)
Action	<ul style="list-style-type: none"> • Review employee and employee related accounts for possible concerns regarding: <ul style="list-style-type: none"> ○ Very active trading ○ Sizeable debit balances ○ Bounced checks ○ High risk trading patterns ○ Transfers between accounts, particularly employee or related accounts and customer accounts ○ Insider trading • Where items of concern are identified, action to be taken depends on the circumstances and may include conducting an internal investigation to identify potential rule/law violations
Record	<ul style="list-style-type: none"> • Record of review of orders and actions taken, if applicable • Record of internal investigation, if applicable • Record of review of accounts and actions taken, if applicable • Quarterly report to FINRA of internal investigations, if CIM Securities engages in investment banking activities

Transactions in employee and employee-related accounts are reviewed daily. Employees will be contacted about transactions that are potentially contrary to rules or Firm policy.

2.4.4 Insider Trading

[SEC Securities Exchange Act of 1934 Rule 10b-5 and Section 10]

Employees are prohibited from effecting transactions based on knowledge of material, non-public information. The chapter *INSIDER TRADING* explains CIM Securities's policy and all employees are expected to be familiar with the policy.

2.4.5 Sharing In Accounts

[FINRA Rule 2150]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • New account forms • Requests to open accounts jointly with customers
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • RR's supervisor: <ul style="list-style-type: none"> ○ When approving new accounts, identify accounts where an RR is potentially sharing in the account ○ Confer with employee as to the nature of the shared account (what is the relationship between the employee and the other account owner, allocation of profits and losses) ○ Refer shared accounts or requests to share in an account to Compliance • Compliance: <ul style="list-style-type: none"> ○ Require written request from employee and written authorization from customer ○ Review and determine whether shared account is appropriate ○ Approve or disapprove the request ○ Notify employee and supervisor of approval or disapproval
Record	<ul style="list-style-type: none"> • Copies of employee request, customer's written authorization, and notation of approval or disapproval is retained with the new account records for the account

CIM Securities and its registered employees may not share directly or indirectly in the profits or losses of a customer's account (with the exception of performance-based fees specifically permitted under rules governing investment adviser and other permitted arrangements). As a general policy, registered employees may not participate in an account that includes customers who are not family members of the employee.

A registered employee may be a joint owner in an account with a customer only under the following conditions:

- the employee submits a written request to Compliance accompanied by signed authorization from the customer
- the employee is a disclosed owner of the account
- the employee shares in losses and gains only in proportion to the employee's monetary contribution to the account (not applicable to accounts shared with immediate family members)
- the employee receives written approval from Compliance

2.4.6 Prohibition On Purchases Of Initial Public Offerings (IPOs)

[FINRA Rule 5130]

Employees and their immediate families (parents, spouse, children, in-laws, siblings) are prohibited from purchasing IPOs. This includes sales to anyone materially supported by an employee or a member of the employee's immediate family. Details regarding this prohibition are in the chapter *CORPORATE SECURITIES UNDERWRITING* in the section *Restrictions On Purchases Of Initial Public Offerings (IPOs)*.

2.4.7 Research Restrictions

Employee accounts are restricted from acting on a new or changed research recommendation for 24 hours from the time of announcement or publication. Restrictions are announced internally and trading activity is monitored for compliance. Failure to comply may result in cancellation of the transaction, and any resulting loss will be charged to the employee.

2.4.8 Restrictions On Personal Accounts Of Certain Firm Personnel

Personnel in certain departments such as research, trading, and investment banking may be subject to additional requirements or restrictions on the trading in their personal accounts. Affected personnel will be provided with any additional policies affecting their personal transactions.

2.5 Gifts, Gratuities And Entertainment

[FINRA Rule 2310(c)(2)(A), 2320(g)(4)(A), 2341(l)(5) and 3220; FINRA FAQs: <https://link.edgepilot.com/s/55d23a57/glVpBJJgE06xkTj8tlhDnQ?u=https://www.finra.org/rules-guidance/key-topics/gifts-gratuities-and-non-cash-compensation/faqs>; FINRA guidance: <https://link.edgepilot.com/s/1c493ce2/Rx7c69-n8Eu6Z8tJ9RH6sQ?u=https://www.finra.org/rules-guidance/key-topics/gifts-gratuities-and-non-cash-compensation>]

Responsibility	CCO
Resources	<ul style="list-style-type: none"> • Requests to give or receive gifts • Expense reports • Annual certification
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • RR's supervisor: <ul style="list-style-type: none"> ○ Refer requests regarding gifts and gratuities to Compliance

	<ul style="list-style-type: none"> ○ Review expense reports for reasonableness and compliance with expense policies and approve or disapprove • Compliance: <ul style="list-style-type: none"> ○ Review and approve or disapprove gifts and gratuities to be given, aggregated on a calendar year basis to determine compliance with the \$100 annual limit • FINOP: <ul style="list-style-type: none"> ○ File Form LM-10 with Dept. of Labor if necessary
Record	<ul style="list-style-type: none"> • Gift Approval Forms are maintained in a branch/department file • Expense reports are maintained in Accounting • FINOP maintains a file for LM-10 filings

Gifts, gratuities, and entertainment are subject to regulators' limitations. Failure to comply may result in fines or other regulatory actions against the employee and CIM Securities. **It is important for all employees to know and comply with this policy.** Questions regarding this policy on gifts and entertainment should be referred to Compliance. Key requirements include:

- **Gifts to others are limited to \$100 per year per person** (other than "personal gifts" defined in the policy).
 - Multiple gifts to the same person are aggregated, *i.e.*, the total of all gifts in any year firm-wide cannot exceed \$100 to one person.
 - "Personal gifts" are excluded (as discussed below).
- **Receiving** gifts is limited.
- An **employee must host entertainment** to avoid entertainment being considered a "gift" subject to limitations.
- **Records of entertainment** must include details of who was entertained and the nature of entertainment.
- **Gifts to labor union employees require prior Compliance approval.**
- **Gifts to public officials require prior Compliance approval.**
- **Your supervisor must be notified** of gifts to others.
- **Your supervisor must be notified** of gifts received (other than personal gifts).
- Gift requirements (whether the gift is given or received) **do not apply to personal gifts** to immediate family members (parents, children, grandparents, siblings, spouse, in-laws) who also happen to be customers and where the gift is unrelated to CIM Securities's business. The policy also does not apply to occasional personal gifts to others (such as a wedding gift or a congratulatory gift for the birth of a child).
- **If CIM Securities pays for the gift** or reimburses the employee for the cost of the gift, the gift is subject to the requirements of this policy.
- **Gifts incidental to entertainment** (*e.g.*, a golf shirt given during a golf outing, *etc.*) are considered gifts subject to reporting to Compliance and the gift limitations.

2.5.1 Gifts To Others

Employees are required to submit the Gift Approval Form to their supervisor prior to giving a gift (other than a *de minimis* gift described below). Gifts relating to CIM Securities's business are limited to \$100 per year per person. Gifts of tickets to sporting events or similar gifts where the employee does not accompany the recipient are subject to the limitations on gifts and gratuities. Such gifts may not be so frequent or so expensive as to raise a suggestion of unethical conduct.

Employees of regulators are also subject to rule limitations regarding gifts to them from broker-dealers and their employees. Compliance should be contacted for guidance before giving gifts to employees of regulators.

Gifts and gratuities are not permitted when given for the purpose of influencing or rewarding the action of a person in connection with the publication of information which has or is intended to have an effect upon the market price of any security.

2.5.1.1 De Minimis And Promotional Items

The policy does not apply to gifts of *de minimis* value (such as pens, notepads, or modest desk ornaments) or to promotional items of nominal value with CIM Securities's logo (*e.g.*, umbrellas, tote bags or shirts). Promotional items must be valued substantially below the \$100 limit to be excluded from the gift policy. Items of higher value (near \$100 or more), even if they include CIM Securities's logo, are considered "gifts" subject to this policy.

FINRA excludes customary leucite tombstones, plaques or other decorative items commemorating a business transaction. This exemption is very limited; other items are considered gifts subject to the policy, even if they commemorate a business transaction.

2.5.1.2 Aggregation Of Gifts

The annual gift limitation is the aggregate of all gifts given to any one individual. For example, a gift of a \$75.00 ticket to a football game in November (as a gift and not as entertainment discussed below) and then a holiday gift of a \$50.00 bottle of wine to the same person in the same year would be in violation of the \$100 limitation.

Each recipient is limited to \$100 in **total** gifts during any calendar year.

2.5.1.3 Valuation Of Gifts

Gifts are valued at the higher of cost or market value excluding tax and delivery charges. For tickets, it is the higher of cost or face value. If gifts are given to multiple recipients, the names of all recipients are recorded and the value of the gift is prorated among recipients. For example, a \$250 fruit basket given to an office of three individuals is permitted since the value of the gift prorated is less than the \$100 limitation per person.

2.5.2 Accepting Gifts

Employees may not solicit gifts or gratuities from customers or other persons with business dealings with CIM Securities. Employees are not permitted to accept gifts from outside vendors currently doing business with CIM Securities or seeking future business without the written approval of Compliance. This policy does not include customary business lunches or entertainment; promotional items (caps, T-shirts, pens, *etc.*); or gifts of nominal (less than \$100.00) value. When accepting gifts from customers or other business-related persons, the employee is required to submit the Gift Approval Form to his or her supervisor.

2.5.3 Entertainment

Entertainment of customers or prospective customers must be reasonable and not so expensive it raises a suggestion of unethical conduct. All entertainment and related expenses must be detailed on an expense form with receipts attached for expenses over \$25.00. Expense forms should be submitted to the appropriate supervisor within 30 days of incurring the expenses.

The limitation on gifts and gratuities does not apply to usual business entertainment such as dinners or sporting events where the employee hosts the entertainment, though such expenses should be reasonable. "Entertainment" includes a broad range of activities such as trips, parties, and other activities where an employee hosts someone related to CIM Securities's business. Questions regarding the reasonableness of proposed entertainment and related expenses should be referred to Compliance.

2.5.3.1 Gifts Incidental To Business Entertainment

Items given in conjunction with entertainment (a golf shirt at a golf outing; a fruit basket delivered to a customer's room during a firm outing) are considered gifts subject to the \$100 limitation.

2.5.4 Gifts Or Payments To Public Officials Under State Laws

[Various state laws]

A "public official" is anyone who is elected or appointed to an office or is an employee of a "public entity" including any teacher or professor employed by a public entity. A "public entity" is broadly defined and includes political bodies, municipalities and their governing bodies (school district, school board, etc.), public universities and colleges as well as any other municipal entity. This policy also includes honorarium payments (payments for any speech given, article published, or attendance at any public or private conference, convention, meeting, social event, or similar gathering).

Some public entities are statutorily authorized to charge the cost of inspections of regulated entities. A public official may, therefore, receive payment for statutorily-authorized expenses. For example, if a state securities official appears at an office to conduct an inspection, the state may, if authorized in state statutes, charge CIM Securities for expenses related to conducting the inspection.

Prior approval from Compliance is required for gifts or entertainment involving public officials.

2.6 Privacy Policy

[SEC Regulation S-P]

Information regarding customer accounts for individuals is subject to SEC Regulation S-P "Privacy Of Consumer Financial Information." This section explains employees' obligation to maintain the privacy of information. A section *Customer Privacy Policies And Procedures* in the chapter *COMMUNICATIONS WITH THE PUBLIC* outlines firm procedures.

1. Regulation S-P requirements apply to individual and not institutional accounts and include U.S. and foreign accounts.
2. Protected information is termed "nonpublic personal information." This is information obtained by CIM Securities that is not deemed "public information" which is defined as information that may be obtained from three sources: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.
3. At the time an account is opened the customer is provided with CIM Securities's privacy policy and is given the opportunity to opt out of arrangements to share nonpublic information with nonaffiliated third parties. The privacy policy is also provided to customers on an annual basis.
4. Employees are prohibited from sharing or releasing nonpublic personal information other than to authorized parties. This includes a prohibition against:
 - o Sending internal reports or other information about firm customers to a non-affiliated 3rd party (unless authorized).

- Sending internal or other documents that include customer non public information to your personal e-mail address.

Questions about providing customer information should be referred to Compliance.

2.7 Reporting Possible Law Or Rule Violations

[SEC Securities Exchange Act of 1934 Section 21F; SEC Rule 21F; FINRA Rule 4530(b)]

Responsibility	<ul style="list-style-type: none"> • Chief Compliance Officer (or, if the CCO is involved in the potential wrongdoing, an alternate senior manager)
Resources	<ul style="list-style-type: none"> • Reports of possible law or rule violations from employees • Referrals from outside sources such as regulators
Frequency	<ul style="list-style-type: none"> • Investigate reports: As required • Employee education: At least annually
Action	<ul style="list-style-type: none"> • Acknowledge the employee's report and advise confidentiality will be maintained and there will be no retaliation for reporting • Determine who will be involved in the investigation and notify those persons of the confidentiality of the investigation • Conduct the investigation using tools appropriate to the issue (interviewing employees, reviewing internal/external reports, engaging counsel, etc.) • Determine whether there was potential wrongdoing and decide whether a report should be made to regulators • Take internal corrective action, as appropriate • Advise the reporting employee of the status of the investigation • Include reporting of possible law or rule violations and CIM Securities's process for internal investigations as part of regular employee education
Record	<ul style="list-style-type: none"> • Report from employee • Information regarding the investigation including records reviewed, who is involved, what steps taken, reports to regulators (if appropriate), conclusion of investigation • Records of employee education including how education is conducted (classes, online education, compliance memos, etc.), who participates, subjects included, and when it occurs

It is the intent of CIM Securities to adhere to all laws and regulations that apply to the organization; the underlying purpose of this policy is to support the organization's goal of legal compliance. The support of all employees is necessary to achieve compliance with various laws and regulations.

2.7.1 Reporting

Employees should report possible crimes or rule violations involving CIM Securities, a department, or an employee or employees as well as outside vendors or service providers. Reporting may be made to any or all of the following, particularly where the employee's supervisor may be involved in the possible wrongdoing.

1. Chief Compliance Officer
2. Investment Banking Supervisor

2.7.2 Confidentiality Of Employee Reporting

All reports will be treated as confidential. The employee's identification will be kept confidential other than to those who need to know such as the compliance officer or counsel or someone else conducting an investigation. Any person identified in the report as a potential wrongdoer will not be provided the name of the person who has filed a report.

2.7.3 Notification Of Chief Compliance Officer

A supervisor or other manager who receives a report of possible violations should immediately refer the matter to the Chief Compliance Officer who is responsible for conducting an investigation and overseeing the review until its conclusion, including potential reporting to a regulator. If the Chief Compliance Officer is involved in the potential wrongdoing, the member of management to whom the issue is reported will be responsible for conducting the investigation.

2.7.4 Investigation

CIM Securities will promptly investigate the reported possible wrongdoing and determine what action is required. Outside counsel may be engaged as part of the investigation. The reporting employee will be advised of the conclusion or resolution of the investigation.

2.7.5 Anti-Retaliation

CIM Securities will not retaliate against an employee who reports some practice of CIM Securities, a department, or employee(s) or of another individual or entity with whom CIM Securities has a business relationship that may represent a rule or law violation. CIM Securities will not retaliate against employees who disclose or threaten to disclose (to CIM Securities or a public body such as a regulator) any activity, policy, or practice of CIM Securities that the employee believes is in violation of a law, or a rule, or regulation mandated pursuant to law.

Supervisors and others are prohibited from engaging in discipline, threats, or discriminatory actions against employees for engaging in whistleblowing activities.

2.7.6 Federal Whistleblower Laws And Rules

The Securities Exchange Act includes Sec. 21F and the SEC has adopted Rule 21F to implement Sec. 21F that provides for reporting possible violation of federal securities laws and potential rewards for information that leads to successful enforcement of a covered judicial or administrative action where monetary sanctions equal \$1,000,000 or more. The Sarbanes-Oxley Act of 2002 (which governs public companies) and the Foreign Corrupt Practices Act (FCPA) also have whistleblower provisions.

2.8 Solicitation Of Charitable Contributions

[FINRA Notice to Members 06-21]

Responsibility	CCO, IB Supervisor
Resources	<ul style="list-style-type: none">Charitable Contribution Approval Request Form
Frequency	<ul style="list-style-type: none">As required
Action	<ul style="list-style-type: none">Review contribution to identify potential conflicts of interestApprove or disapprove
Record	<ul style="list-style-type: none">Charitable Contribution Approval Request forms

When an employee or an agent of a customer such as a mutual fund, pension plan, or investment manager solicits a substantial charitable contribution from CIM Securities or an RR, there may be a conflict of interest. For example, if an investment manager requests a \$10,000 contribution to a charity, this could be construed as a condition for the investment manager to direct business to CIM Securities. There can be no quid pro quo between contributions and business conducted with CIM Securities.

To avoid potential conflicts of interest, CIM Securities has established the following guidelines for handling such requests.

1. Charitable giving by CIM Securities or foundations created by CIM Securities is subject to review by the CEO or the CEO's designee on at least an annual basis.
2. Contributions of \$10,000 or more solicited by an employee or agent of a customer require the prior approval of Compliance and will require the approval of someone representing the customer other than the person soliciting the contribution.
3. Contributions cannot be based on the actual or anticipated level of business done by the customer.
4. These requirements do not apply to a retail customer who solicits a charitable contribution when acting in his or her individual capacity.

2.9 Media Contact Is Limited To Certain Authorized Employees

Responsibility	CCO, IB Supervisor
Resources	<ul style="list-style-type: none">Requests to communicate with the media

	<ul style="list-style-type: none"> • Indications an unauthorized person has had media contact
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • For requests, determine nature of contact and whether the individual is or should be authorized to engage in the contact • If necessary, notify the employee whether contact will be permitted and provide guidelines • For unauthorized contact, confer with the employee (and the employee's supervisor, if appropriate)
Record	<ul style="list-style-type: none"> • Maintain a list of authorized persons and limitations on their contact, if appropriate

CIM Securities is sometimes contacted by media representatives (television, radio, newspapers, magazines, and other types of media). Employees who are contacted by media representatives are not permitted to comment but must refer the representative to one of the following individuals within CIM Securities:

- Compliance Officer

Individuals authorized to speak to the media are expected to make comments consistent with good taste and CIM Securities's opinion or position on matters discussed.

2.10 Requests For Information From Outside Sources

Responsibility	CCO
Resources	<ul style="list-style-type: none"> • Written or oral requests for information • Subpoenas • Other
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Compliance: Provide response, as appropriate
Record	<ul style="list-style-type: none"> • Retain record of response in legal, regulatory, or other files

CIM Securities and its employees are sometimes contacted by outside parties such as regulators (SEC, FINRA, exchanges, state and other regulators), attorneys and governmental agencies (e.g., the IRS) that request information about customer accounts, CIM Securities activities, or an individual employee's activities.

Information regarding customer accounts, CIM Securities and its employees is considered confidential and may be released only to those authorized to receive it. Any requests from outside parties (other than the principal or authorized person on behalf of an account requesting information on the account) should be immediately referred to Compliance for response. This includes requests received in any form whether written, by phone, or in person. This also includes visits by regulators. Proof of identification should be requested and Compliance immediately notified.

2.11 Internal Reviews And Investigations

If necessary, CIM Securities may conduct an internal review or investigation. Employees may be requested for information that may include an employee's signed written statement. Failure to provide requested information may result in disciplinary action, including termination.

2.12 Internal Disciplinary Actions

CIM Securities's goal in administering discipline is to take measures to maintain the quality of service provided to our customers by encouraging appropriate behavior. The expected result of these measures is the deterrence of inappropriate behavior and, when improper activity occurs, to take corrective action commensurate with the activity.

2.12.1 When Disciplinary Action Is Considered

Although it is impossible to list all circumstances in which discipline may be imposed, disciplinary action will be considered when there is:

- An admitted violation of company policy, regulatory rules or regulations, or federal/state laws.
- A determination of an actual or probable violation of company policy, regulatory rules or regulations, or federal/state laws.

2.12.2 Who Determines Disciplinary Action

Although Compliance will not always be the primary decision maker in determining disciplinary action, it is **essential** that Compliance be notified **in advance** of all disciplinary actions in order to analyze such actions for regulatory reporting purposes and for adequate recordkeeping of disciplinary information. Compliance may modify the terms of discipline outlined in the policy depending on the facts and circumstances of the situation.

2.12.3 Types Of Discipline

There is a range of possible disciplinary action; the level of discipline will be determined by Compliance. Compliance will collaborate with the individual's supervisor who will be copied on any communications to the individual regarding the disciplinary action.

Letter of Caution (LOC): An LOC is a memorandum that specifies a possible violation and/or serves as a warning of inappropriate behavior. The LOC outlines the expected behavior and the possible consequences of future violations similar in nature. The LOC requires the recipient's signature certifying his/her receipt of the memorandum and understanding of the matter.

Admonishment: An Admonishment is a memorandum that formally reprimands an individual based on admitted or determined violations. The Admonishment specifies the admitted or determined violation and the expected behavior. It specifies the possible consequences of future violations similar in nature and may be administered with a **Non-reportable** or **Reportable Fine** (see below). The Admonishment requires the recipient's signature certifying his/her receipt of the memorandum and understanding of the matter.

Non-reportable Fine: A Non-reportable Fine is a monetary sanction that is less in amount than that which is required to be reported to a self-regulatory organization (SRO). Non-reportable fines will usually be attached to an **Admonishment** (see above) and/or **Suspension of Employment**. In any event, the admitted or determined violation will be specified along with the expected behavior and possible consequences of future violations similar in nature.

Non-reportable fines will be withheld from a producing-employee's commissions. In the case of a non-producing employee, the fine will be collected in the form of personal or certified check or money order. The amount of the fine may be donated, in the name of the company, to a local charity.

Reportable Fine: A Reportable Fine is a monetary sanction that is greater than or equal to the amount that is required to be reported to an SRO. Reportable fines will usually be attached to an **Admonishment** (see above) and/or **Suspension of Employment**. In any event, the admitted or determined violation will be specified along with the expected behavior and possible consequences of future violations similar in nature.

Reportable fines will be withheld from a producing-employee's commissions. In the case of a non-producing employee, the fine will be collected in the form of personal or certified check or money order. The amount of the fine may be donated, in the name of the company, to a local charity.

Suspension of Employment: An employee may be suspended for violations of applicable company policy, regulatory rules or regulations, or federal/state laws. Prior to Suspension of Employment, the employee will be informed of the violation, the expected behavior, and the terms of the suspension.

While under suspension, employees may not:

- Have direct or indirect contact with customers
- Act as a registered representative
- Represent oneself as a registered representative
- Give investment advice or counsel
- Receive compensation
- Transact business in any securities account (other than a personal account)
- Have contact with company employees except the employee's supervisor or Compliance
- Enter into any company premises

A Suspension of Employment memorandum will be delivered to the employee. This document will specify the admitted or determined violation and the expected behavior. It will also specify the possible consequences of future violations similar in nature. The Suspension of Employment memorandum may require the recipient's signature certifying his/her receipt of the memorandum and understanding of the matter. Suspensions will be reported by Compliance to the appropriate SRO(s).

Termination of Employment: An employee's employment may be terminated for violations of company policy, regulatory rules or regulations, or federal/state laws. The employee will be informed of the violation and termination of employment.

Termination will be reported by Compliance to the appropriate SRO(s).

2.12.4 Additional Action

The employee may be subject to Heightened Supervision as outlined in the chapter *EMPLOYMENT, REGISTRATION AND LICENSING*. The employee also may be excluded for a specified period of time from forms of special recognition offered by CIM Securities. The employee may also be subject to added education, re-testing for licensing, title downgrading, or other remedial actions deemed appropriate by Compliance.

2.12.5 Considerations In Determining Type Of Discipline

The nature of the inappropriate conduct is important in determining the type of discipline to be imposed. The more serious the conduct, the more severe the discipline. An employee's prior complaint and disciplinary history will be considered in determining the appropriate level of discipline. The activity's risk to CIM Securities, injury to customers, and the employee's cooperation may all be factors (among others) in determining the discipline.

2.13 Employee Obligation To Notify The Firm And The Firm's Obligation To Report

[FINRA Rule 4530]

Responsibility	CCO
Resources	<ul style="list-style-type: none">• Information provided by employees including information from Annual Employee Certifications• Lawsuits and arbitrations• Regulatory actions• Criminal actions• FINRA compliance reports
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Determine whether information or events are reportable including updating the RR's Form U4 or U5• File information electronically with FINRA
Record	<ul style="list-style-type: none">• Record of electronic filings• Records of updates to Form U4 or U5

Regulators require reporting of certain events and updating of Forms U4 and U5 when previously-filed information changes. **Employees are obligated to notify Compliance if there are changes to Form U4 responses and report other information required by rule or by CIM Securities.**

The following is an excerpt from FINRA Rule 4530 that outlines events that require reporting:

1. the member or an associated person of the member:
 - has been found to have violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body, self-regulatory organization or business or professional organization;
 - is the subject of any written customer complaint involving allegations of theft or misappropriation of funds or securities or of forgery;
 - is named as a defendant or respondent in any proceeding brought by a domestic or foreign regulatory body or self-regulatory organization alleging the violation of any provision of the Exchange Act, or of any other federal, state or foreign securities, insurance or commodities statute, or of any rule or regulation thereunder, or of any provision of the by-laws, rules or similar

- governing instruments of any securities, insurance or commodities domestic or foreign regulatory body or self-regulatory organization;
- is denied registration or is expelled, enjoined, directed to cease and desist, suspended or otherwise disciplined by any securities, insurance or commodities industry domestic or foreign regulatory body or self-regulatory organization or is denied membership or continued membership in any such self-regulatory organization; or is barred from becoming associated with any member of any such self-regulatory organization;
 - is indicted, or convicted of, or pleads guilty to, or pleads no contest to, any felony; or any misdemeanor that involves the purchase or sale of any security, the taking of a false oath, the making of a false report, bribery, perjury, burglary, larceny, theft, robbery, extortion, forgery, counterfeiting, fraudulent concealment, embezzlement, fraudulent conversion, or misappropriation of funds, or securities, or a conspiracy to commit any of these offenses, or substantially equivalent activity in a domestic, military or foreign court;
 - is a director, controlling stockholder, partner, officer or sole proprietor of, or an associated person with, a broker, dealer, investment company, investment advisor, underwriter or insurance company that was suspended, expelled or had its registration denied or revoked by any domestic or foreign regulatory body, jurisdiction or organization or is associated in such a capacity with a bank, trust company or other financial institution that was convicted of or pleaded no contest to, any felony or misdemeanor in a domestic or foreign court;
 - is a defendant or respondent in any securities- or commodities-related civil litigation or arbitration, is a defendant or respondent in any financial-related insurance civil litigation or arbitration, or is the subject of any claim for damages by a customer, broker or dealer that relates to the provision of financial services or relates to a financial transaction, and such civil litigation, arbitration or claim for damages has been disposed of by judgment, award or settlement for an amount exceeding \$15,000. However, when the member is the defendant or respondent or is the subject of any claim for damages by a customer, broker or dealer, then the reporting to FINRA shall be required only when such judgment, award or settlement is for an amount exceeding \$25,000; or
 - is, or is involved in the sale of any financial instrument, the provision of any investment advice or the financing of any such activities with any person who is, subject to a "statutory disqualification" as that term is defined in the Exchange Act. The report shall include the name of the person subject to the statutory disqualification and details concerning the disqualification; or
2. an associated person of the member is the subject of any disciplinary action taken by the member involving suspension, termination, the withholding of compensation or of any other remuneration in excess of \$2,500, the imposition of fines in excess of \$2,500 or is otherwise disciplined in any manner that would have a significant limitation on the individual's activities on a temporary or permanent basis.

In addition, employees are required to promptly report any of the following to Compliance:

- A temporary or permanent injunction issued by any court and involving securities, commodities, insurance, or banking matters
- Any customer complaint (securities or commodities) including a written complaint, civil litigation, or arbitration
- An arrest, indictment, arraignment, conviction, pleading guilty or no contest to any felony or misdemeanor (other than misdemeanor traffic offenses)
- A bankruptcy proceeding or unsatisfied liens or judgments

2.13.1 Reporting Requirements

CIM Securities will report specified events involving the firm or an associated person to FINRA via the Regulatory Filings Application on the FINRA Firm Gateway no later than 30 calendar days after CIM Securities knows of the event. This is in addition to any obligation to update an associated person's U4 or U5 or CIM Securities's Form BD.

CIM Securities will promptly report to FINRA (not later than 30 calendar days after CIM Securities has concluded or reasonably should have concluded) that an associated person of CIM Securities or CIM Securities itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization. Conduct reported will be conduct that has a significant monetary result with respect to CIM Securities, customers, or markets, or multiple instances of any violative conduct.

Relating to reported events, CIM Securities will file with FINRA copies of the following. Events already reported on Form U4 with an affirmative request to satisfy Rule 4530 reporting requirements and FINRA findings and actions will not be reported separately.

1. any indictment, information or other criminal complaint or plea agreement for conduct reportable under paragraph (a)(1)(E) of this Rule;
2. any complaint in which a member is named as a defendant or respondent in any securities- or commodities-related private civil litigation, or is named as a defendant or respondent in any financial-related insurance private civil litigation;
3. any securities- or commodities-related arbitration claim, or financial-related insurance arbitration claim, filed against a member in any forum other than the FINRA Dispute Resolution forum;
4. any indictment, information or other criminal complaint, any plea agreement, or any private civil complaint or arbitration claim against a person associated with a member that is reportable under question 14 on Form U4, irrespective of any dollar thresholds Form U4 imposes for notification, unless, in the case of an arbitration claim, the claim has been filed in the FINRA Dispute Resolution forum.

2.14 Money Laundering

[FINRA Rule 3310; Bank Secrecy Act]

Money laundering is a serious crime potentially related to the funding of terrorist activities. It is the subject of extensive federal regulations that impose requirements on financial institutions, such as broker-dealers and their employees, to detect and prevent potential money laundering activities. This is an obligation of each employee of CIM Securities.

Money laundering is the movement of criminally derived funds to conceal the true source, ownership, or use of the funds. The funds are filtered through a maze or series of transactions, so the funds are "cleaned" to look like proceeds from legal activities.

In general, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash profits from criminal activity are converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to separate further the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund further criminal or legitimate activities.

Engaging in money laundering is a federal crime with severe penalties for those engaged in criminal activities and those who facilitate, intentionally or inadvertently, money laundering. It is important that CIM Securities, as well as all employees, remain diligent and active participants in CIM Securities's anti-money laundering (AML) program.

2.14.1 Background

The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its accompanying regulation, is a tool the U.S. government uses to fight drug trafficking, money laundering, and other crimes. Congress enacted the BSA to prevent financial service providers (such as banks and broker-dealers) from being used as intermediaries for, or to hide the transfer or deposit of, money derived from criminal activity. Money

laundering schemes may include the use of wire transfers, cash, bearer instruments, travelers' checks, money orders, cashiers' checks, and other negotiable instruments.

CIM Securities is required to comply with the reporting, recordkeeping, and record retention requirements of the BSA. The requirements govern the payment, receipt, or transfer of currency within and into and out of the U.S. and foreign financial transactions and accounts.

2.14.2 Shell Companies

[FinCEN advisory on shell companies: <https://www.fincen.gov/resources/statutes-regulations/guidance/potential-money-laundering-risks-related-shell-companies>]

Shell companies may represent potential money laundering risks. "Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. It is important for employees to be aware of the risks involved in dealing with shell companies.

Most shell companies are formed for legitimate business purposes such as to hold stock or intangible assets of another business entity or to facilitate domestic and cross-border currency and asset transfers and corporate mergers. Unfortunately, shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate, and ownership and transactional information can be concealed from regulatory and law enforcement authorities. Most states do not collect or require disclosure of ownership information at the formation stage or after.

Agents, also known as intermediaries or nominee incorporation services (NIS), can play a central role in the formation and maintenance of shell companies. Agents and NIS firms offer a wide range of services that may include offering an office address, mail-forwarding services, local telephone listings, and other services that may give the appearance of a locally-established business. Some agents and NIS firms also provide nominee services which can preserve a client's anonymity. Some risk indicators of shell companies potentially engaged in money laundering are:

- An inability to obtain (through Internet searches, commercial database searches, or direct inquiries to the company's foreign correspondent bank) information necessary to identify originators or beneficiaries of wire transfers.
- A foreign correspondent bank exceeds the anticipated volume projected in its client profile for wire transfers in a given period or an individual company exhibits a high amount of sporadic activity that is inconsistent with normal business patterns.
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or service number.
- Goods or services of the company do not match the company's profile based on information previously provided.
- Transacting businesses share the same address, provide only a registered agent's address, or raise other address-related inconsistencies.
- An unusually large number and variety of beneficiaries receive wire transfers from one company.
- Frequent involvement of beneficiaries located in high-risk, offshore financial centers.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

2.14.3 Penalties

Participation in a money laundering scheme or the knowing receipt of proceeds from criminal activities is a crime. CIM Securities and its employees are subject to severe criminal, civil, and regulatory penalties if they facilitate or

participate in money laundering activities. Violations by employees may result in internal disciplinary action including termination.

An employee may be deemed to be facilitating or participating in money laundering by engaging in a transaction with a customer (accept a deposit, arrange a withdrawal, effect a trade, *etc.*) when he or she is aware of, or willfully ignores, the fact that the customer is engaged in illegal activities.

2.14.4 Treasury Dept. OFAC List

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) is responsible for publishing sanctions against persons, corporations, and other entities including foreign governments that have been identified by the U.S. Government as engaging in criminal activities including drug trafficking and terrorist activities. CIM Securities is obligated to check its accounts against the lists of blockings to ensure it does not engage in prohibited transactions which include securities transactions and transfer of assets out of a blocked account or to a blocked person or entity.

CIM Securities has procedures to monitor the OFAC lists and comply with requirements to block property and notify OFAC when required. Questions regarding CIM Securities's program should be referred to the AML Compliance Officer. More information is also available at the OFAC web site at www.treas.gov/ofac.

2.14.5 Preventing Money Laundering

SEE THE FIRM'S AML MANUAL FOR MORE INFORMATION.

There are a number of ways CIM Securities and its employees can avoid money laundering schemes.

2.14.5.1 Knowing The Customer

Being familiar with the customer's financial resources, business activities, and sources of funds are avenues for knowing the customer. Knowing the customer occurs at the time an account is opened as well as during the operation of a customer's account.

The identity of customers must be verified when a new account is opened. Procedures for verifying customer ID are explained in the chapter *ACCOUNTS* in the section *New Accounts*.

2.14.5.2 Risk Indicators

[NASD Notice to Members 02-21; FINRA Small Firm AML Template]

The following are examples of risk indicators (red flags) that may suggest potential money laundering.

<i>Customer accounts (opening, other activities related to establishing accounts)</i>
--

The customer exhibits unusual concern regarding CIM Securities's compliance with government reporting requirements and CIM Securities's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

The customer is reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
The customer's background is questionable or differs from expectations based on business activities.
The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect or refuses to provide information.
The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).
The customer has no discernible reason for using CIM Securities's service.
<i>Customer account transactions</i>
The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
The customer wishes to engage in transactions that lack business sense or apparent investment strategy or that are inconsistent with the customer's stated business strategy.
The customer engages in suspicious activity involving the practice of depositing penny stocks, liquidates them, and wires proceeds. A request to liquidate shares may also represent engaging in an unregistered distribution of penny stocks which may also be a red flag. [FINRA Regulatory Notice 09-05]
The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from CIM Securities's policies relating to the deposit of cash and cash equivalents.
The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
For no apparent business purpose or other reason, the customer has multiple accounts under a single name or multiple names (including family members or corporate entities); there may be a large number of inter-account or third-party transfers.
The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
The customer requests that a transaction be processed in such a manner to avoid CIM Securities's normal documentation requirements.
The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
Transactions patterns show a sudden change inconsistent with normal activities.
The customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
Two or more accounts trade an illiquid stock suddenly and simultaneously.
The customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.

Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
Customer's trading patterns suggest that he or she may have inside information.
The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
Large numbers of securities transactions across a number of jurisdictions.
Buying and selling securities with no purpose or in unusual circumstances (e.g., churning at customer's request).
<i>Penny Stock Company Related Transactions</i>
Company has no business, no revenues and no product.
Company has experienced frequent or continuous changes in its business structure.
Officers or insiders of the issuer are associated with multiple penny stock issuers.
Company undergoes frequent material changes in business strategy or its line of business.
Officers or insiders of the issuer have a history of securities violations.
Company has not made disclosures in SEC or other regulatory filings.
Company has been the subject of a prior trading suspension.
<i>Customer avoidance of reporting and recordkeeping</i>
Reluctant to provide information needed to file reports or fails to proceed with transaction.
Tries to persuade an employee not to file required reports or not to maintain required records.
"Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
<i>Transactions involving insurance products</i>
Cancels an insurance contract and directs funds to a third party.
Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.
Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.
Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.
Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
Purchases an insurance product with no concern for investment objective or performance.
Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.
<i>Customer wire and other transfers or deposits</i>
The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.
Many small, incoming wire transfers or deposits made using checks and money orders almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.
Physical certificate is titled differently than the account.
Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
Customer's explanation of how he or she acquired the certificate does not make sense or changes.
Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.
<i>Other indicators</i>
Law enforcement subpoenas.
Payment by third-party check or money transfer without an apparent connection to the customer.
Payments to third-party without apparent connection to customer.
No concern regarding the cost of transactions or fees (<i>i.e.</i> , surrender fees, higher than necessary commissions, <i>etc.</i>).

2.14.6 Cash Deposits Not Accepted

CIM Securities does not accept cash deposits or cash equivalents (money orders, travelers checks). Customers who attempt to deposit cash should be advised to submit a personal check to his or her account.

2.14.7 Reports Of AML Non-Compliance And Other Potential Crimes

All employees are obligated to promptly report to the AML Compliance Officer any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of CIM Securities. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with CIM Securities, a customer, or prospective customer) are required to be reported. This includes suspicion that CIM Securities is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the Bank Secrecy Act reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to report it.

SAR reports: Broker-dealers are required to file Suspicious Activity Reports (SARs) for transactions that may be indicative of money laundering activity.

By law, CIM Securities and its employees cannot disclose to the customer or anyone other than authorized regulators that it has filed a SAR. Questions regarding SAR filings should be referred to Compliance.

2.14.8 Currency Transaction Reporting

The Bank Secrecy Act requires broker-dealers to report certain transactions relating to currency transactions, as follows:

- Report cash or currency deposits of more than \$10,000, including multiple deposits on the same day that would total more than \$10,000. A currency Transaction Report (CTR) is filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department. Some state regulators also require reporting of currency transactions.
- Report currency or bearer instruments over \$10,000 transferred into or out of the U.S. The Currency and Monetary Instrument Transportation Report (CMIR) is filed with the U.S. Customs Service.

2.14.8.1 Prohibition Against Structuring Deposits To Avoid Reporting

Cash or currency deposits or attempted deposits which appear to be part of a deposit structure to avoid IRS or Customs currency reporting requirements or firm limitations, or are otherwise suspicious, may not be accepted and must be reported to Compliance. Employees are prohibited from:

- aiding or advising a customer in structuring a transaction to avoid reporting requirements
- holding instruments for deposit on succeeding days
- transporting cash or cash equivalents or bearer instruments to a bank on behalf of a customer

2.14.9 Recordkeeping Requirements

In addition to reporting requirements, broker-dealers are subject to requirements to maintain records of transfers of funds (including wire fund transfers) of \$3,000 or more. This includes transfers between accounts that are not for the same owner and transfers to third parties including banks and other financial institutions. Records of transfers are available for inspection by regulators and other appropriate authorities, when requested.

2.14.10 AML Compliance Officer

CIM Securities has designated an AML Compliance Officer who is responsible for overseeing CIM Securities's anti-money laundering program. The AML Officer may be contacted whenever an employee has questions about CIM Securities's program, a current or prospective account, or activities or transactions that raise questions about potential money laundering activities. An employee may also provide information anonymously to the AML Officer.

The AML Officer is responsible for investigating suspected money laundering activities and taking corrective action when necessary.

2.14.11 Identity Theft

Identity thieves use someone's personal identifying information to open new accounts and misuse existing accounts. CIM Securities has established an Identity Theft Prevention Program (ITPP) to help detect and prevent identity theft. Many elements of detecting or preventing identity theft are similar to anti-money laundering (AML) requirements that are included in these policies.

The ITPP is based on identifying "red flags" that indicate identity theft may have occurred. ***It is the responsibility of all employees to be alert and report to the AML Compliance Officer any new or existing customers who may be engaged in violations of anti-money laundering regulations or identity theft or who have reported identity theft.***

Following is a list of potential identity theft red flags.

Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency
1. A fraud or active duty alert is included on a consumer credit report. An "active duty" alert is an alert a military person may add to his/her credit report to identify potential identity theft.
2. A notice of credit freeze is given in response to a request for a consumer credit report.
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.
Category: Suspicious Documents
5. Identification presented looks altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.
7. Information on the identification differs from what the identification presenter is saying.
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.
9. The application looks like it has been altered, forged or torn up and reassembled.
Category: Suspicious Personal Identifying Information
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.
11. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.

14. The SSN presented was used by someone else opening an account or other customers.
15. The address or telephone number presented has been used by many other people opening accounts or other customers.
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.
17. Inconsistencies exist between what is presented and what our firm has on file.
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.
Category: Suspicious Account Activity
19. Soon after CIM Securities gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.
22. An account that is inactive for a long time is suddenly used again.
23. Mail CIM Securities sends to a customer is returned repeatedly as undeliverable even though the account remains active.
24. We learn that a customer is not getting his or her paper account statements.
25. We are notified that there are unauthorized charges or transactions to the account.
Category: Notice From Other Sources
26. An outside agency, law enforcement, a clearing firm, or other source notifies CIM Securities that an account has been opened or used fraudulently.
27. CIM Securities is notified of potential unauthorized access to customer personal information due to data loss from an outside provider or a breach of an outside provider's data.
28. Notice from a customer of the loss of information (e.g., loss of wallet, birth certificate, etc.).

2.15 Cybersecurity

Cybersecurity is generally defined as maintaining the security of cyber systems. Cybercrimes are broadly defined as any illegal activity that involves a computer, another digital device, or a computer network. Cybercrime includes common cybersecurity threats like social engineering, software, vulnerability exploits, and network attacks. The U.S. financial system makes institutions attractive targets to criminals, including terrorists and state actors targeting websites, systems, and employees to steal customer and commercial credentials and proprietary information.

Employees should immediately report to Compliance any perceived cybersecurity threat. The chapter *CYBERSECURITY* in this manual addresses details of CIM Securities's efforts to ensure the integrity of its systems.

2.16 Emergency Business Recovery Procedures

[FINRA Rule 4370]

CIM Securities has a *Business Continuity Plan* that assigns responsibilities and outlines procedures in the event of a disaster or emergency which impacts CIM Securities's ability to continue conducting business (also termed a "significant business disruption"). Examples of a major disruption include a regional power outage; disruption at another company that provides services critical to CIM Securities's business; and destruction of an office or other facilities by natural causes or by other means. The Plan designates employees who are responsible for employee safety and protection of firm property, records, and customer assets.

In the event of a disruption, employees will be given instructions by authorized personnel. Depending on the nature of the emergency, it may be necessary to use alternative communication systems; transfer personnel and/or business activities to alternative office space; or transfer CIM Securities's business to other brokerage firms or financial institutions until normal operations can be resumed.

CIM Securities has established procedures for contacting employees in the event of an emergency. If CIM Securities conducts a test of its emergency procedures, all employees are required to participate as if the emergency were real. Past emergencies affecting the securities industry have shown that preparedness and cooperation are key to maximizing the safety of employees and minimizing business interruptions. It is important for all employees to follow instructions from senior management and other authorized key personnel during any drill or when an emergency occurs.

Questions regarding CIM Securities's Business Continuity Plan may be referred to Compliance.

2.17 Prohibited Activities

Responsibility	CCO; IB Supervisor
Resources	<ul style="list-style-type: none">• Various (referral of items, direct identification, review of transactions, correspondence, <i>etc.</i> depending on the nature of the prohibited activity)
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Take corrective action which may include:<ul style="list-style-type: none">○ Conferring with the employee○ Referring the matter to Compliance○ Issuing a written admonition○ Restricting the activities of or transactions handled by the employee○ Suspending the employee○ Termination
Record	<ul style="list-style-type: none">• The record of action taken depends on the nature and seriousness of the prohibited activity. Records, if needed, may be in different forms, including the following:<ul style="list-style-type: none">○ Designated supervisors may record action taken in supervisory logs, Daytimers, memos to employees' files, <i>etc.</i>○ Compliance may record action by memo to the employee's file

2.17.1 Use Of Firm Name

No employee may use CIM Securities's name in any manner which could be reasonably misinterpreted to indicate a tie-in between CIM Securities and any outside activity of the employee.

2.17.2 High Pressure Sales Tactics

CIM Securities and its RRs will not engage in high pressure sales tactics which may include excessive telephone calls, implying that a price may change on a security if the customer doesn't act immediately, or falsely representing that there is a limited supply of a security at a particular price.

2.17.3 Providing Tax Advice Not Permitted

Employees may not give tax advice to customers since CIM Securities and its employees are not engaged in the practice of providing tax advice. Customers requiring specific tax guidance should be referred to their personal tax advisers.

2.17.4 Rebates Of Commission

[FINRA Rule 2040]

Employees are prohibited from rebating to anyone, directly or indirectly, any commission or compensation received.

2.17.5 Sharing Commissions Or Fees With Non-Registered Persons

[FINRA Rule 2040]

With few exceptions, regulations generally prohibit the sharing of commissions or compensation with non-registered persons. Any payment, finder's fee, or sharing arrangement involving a non-registered person must be referred to Compliance for review.

2.17.6 Accepting Compensation From Others

R Rs are prohibited from accepting direct or indirect compensation (finders' fees, commissions, *etc.*) for Firm-related business other than through Firm-approved products or programs or with the prior approval of Compliance.

2.17.7 Settling Complaints Or Errors Directly With Customers

Employees may not make payments to customers of any kind to resolve an error or customer complaint. Errors and complaints must be brought to the attention of the employee's designated supervisor.

2.17.8 Borrowing From And Lending To Customers

[FINRA Rule 3240; FINRA Notice to Members 04-14]

Registered employees are generally not permitted to borrow from or lend to their own customers. "RR" as used in this policy refers to **any** registered employee of CIM Securities.

This restriction does NOT apply when an employee enters into a loan arrangement with a customer who is:

1. an immediate family member (defined as parents; grandparents; in-laws; spouse; siblings; children; grandchildren; cousins; aunts or uncles; nieces or nephews; and any other person whom the RR supports, directly or indirectly, to a material extent);
2. a financial institution in the business of providing credit, financing, or loans AND where the terms of the lending arrangement are those that would also be available to the general public doing business with those institutions;
3. another registered employee of CIM Securities;
4. someone (or an entity) who has a personal relationship with the RR and the lending arrangement arises from the personal relationship rather than an RR/customer relationship; or,
5. someone (or an entity) that has a business relationship outside the RR/customer relationship.

Any proposed loan with the RR's customer (other than a loan with a family member or financial institution in item numbers 1 and 2 above) requires the PRIOR review and approval by Compliance. RRs requesting exceptions must complete the RR/Customer Lending Arrangement Request form and submit it to Compliance prior to effecting the loan arrangement. Compliance will retain written approvals for at least 3 years after the date that the borrowing or lending arrangement has terminated or for at least 3 years after the RR has terminated employment with CIM Securities.

2.17.9 Personal Funds Deposited In Customer Accounts

In general, employees are not permitted to deposit personal funds or securities in customers' accounts or deposit customers' personal funds or securities in employee accounts. The same prohibitions apply to withdrawals. Exceptions should be reviewed by Compliance.

2.17.10 Prohibition Against Guarantees

[FINRA Rule 2150]

CIM Securities and its employees are prohibited from guaranteeing a customer against loss in any securities transaction. Designated supervisors are responsible for identifying prohibited guarantees in correspondence or other written communications with public customers. Options or written agreements that establish the future price of a transaction such as repurchase agreements are not included in this prohibition.

2.17.11 Fees And Other Charges

Employees are not permitted to charge fees or assess other charges to customers or customers' accounts unless they are expressly permitted by CIM Securities.

2.17.12 Customer Signatures

Employees are not permitted to sign documents on behalf of customers, even when doing so is meant to accommodate a customer's request. Customer signatures must be original by the customer on all documents.

2.17.13 Rumors

[FINRA Rule 6140(e)]

Responsibility	CCO, IB Principal
Resources	<ul style="list-style-type: none">• Correspondence (electronic or written)
Frequency	<ul style="list-style-type: none">• Daily• Periodically - training
Action	<ul style="list-style-type: none">• As part of routine reviews of correspondence, look for communications that appear to spread rumors<ul style="list-style-type: none">○ Contact RR regarding source of information○ If false rumors are identified, contact Compliance○ Corrective action may include contacting recipients of correspondence containing false rumors; enhanced training for RR; disciplinary action appropriate to the offense• For scheduled training, include the prohibition against spreading false rumors
Record	<ul style="list-style-type: none">• Correspondence with record of reviewer's initials and action taken, if appropriate• Record of training sessions (who attended, dates conducted, subject matter included)

No employee may spread any rumors or misinformation that the employee knows to be false or misleading. This includes rumors of a sensational character that might reasonably be expected to affect market conditions. Discussion of unsubstantiated information published by a widely circulated public media is not prohibited providing the source and unsubstantiated nature are also disclosed.

2.17.14 Misrepresentations

Employees may not disseminate any information that falsely states or implies guarantees or approval of securities by the government or other institution such as government guarantee of securities that carry no such guarantee. SIPC may not be misrepresented as a guarantor of a customer's account against losses from transactions.

2.17.15 Bribes

No employee may offer or solicit explicit inducements to or from employees or representatives of other institutions or foreign governmental or political officials to obtain business. Entertainment and gifts in reasonable amounts are not included in this prohibition and are discussed in the section *Gifts, Gratuities And Entertainment*.

2.17.16 Acting Without Registration

Responsibility	CCO, IB Supervisor
Resources	<ul style="list-style-type: none">• New account forms• Notices of registration status from Compliance• Reports of transactions effected by RRs not licensed in the customer's state of residency
Frequency	<ul style="list-style-type: none">• Ongoing
Action	<ul style="list-style-type: none">• Review new account forms to identify any out-of-state accounts where the RR may not be registered• Review reports of transactions identifying unlicensed activity and follow up with RR• Immediately refer any RRs requiring state registration to Compliance
Record	<ul style="list-style-type: none">• Include a notation on the New Account form or report noting action taken• Supervisor's log, daytimer, or other record, as needed

No employee may engage in activities that require registration (selling securities, soliciting accounts, trading, *etc.*) unless registered in the appropriate capacities. Questions regarding the need for registration should be referred to Compliance.

2.18 Cybersecurity Policy

Cybersecurity is everyone's responsibility. Loss of data or systems can have a serious effect on the conduct of business and CIM Securities and its employees. Some aspects of cybersecurity are included in the Electronic Communications Policy. This policy summarizes key issues to maintain cybersecurity.

1. Employees must protect passwords assigned to them and not share them with anyone not authorized to receive the information.
2. Employees may not access data, files, or systems where they are not authorized to have access.
3. Electronic devices used for Firm business must be authorized by CIM Securities. Personal devices may not be used for Firm business unless specifically authorized.
4. All devices must include virus, spyware, and other intrusion protections required by CIM Securities. All mobile personal devices must maintain a separate, secure, encrypted mobile device management application for all Firm activities including e-mail, calendar, and other activities.

5. Only software approved by CIM Securities may be used for Firm business. Software must be updated promptly when updates are provided.
6. Devices must have a locking mechanism to prevent others from accessing data.
7. All access to Firm systems or transmission of data must be conducted through secure systems and networks.
8. Devices must be physically secured at all times to prevent the risk of theft or loss.
9. Your supervisor and Compliance must be notified immediately if devices with customer information are lost or stolen.
10. Do not open e-mails and particularly attachments from unknown sources and sources that appear to be genuine but ask for confidential information (potential phishing).
11. Software, services and applications that violate Firm policy will be removed.
12. Failure to comply may result in additional training, written notices, fines, suspension, or termination of employment.

2.19 Computer Records, Equipment And Software

Responsibility	CCO
Resources	<ul style="list-style-type: none"> Records of employees with company-issued laptops or other devices Disks and other computer records maintained by a terminating employee Reports of lost devices
Frequency	<ul style="list-style-type: none"> As required
Action	<ul style="list-style-type: none"> Issue firm laptops or other mobile devices to employees and maintain a record of laptops Provide employees with education and policy information about proper use of computer and other electronic equipment including appropriate security measures and accessing customer information Instruct offices to secure equipment and information Secure disks, computers, software, and other firm property when an employee terminates Do not permit removal of firm equipment without approval Take action regarding lost devices including remote deactivation, if available, and assessment of whether a breach of customer information has or may occur
Record	<ul style="list-style-type: none"> Records of laptops or other devices and to whom they are provided Records of lost devices and actions taken

CIM Securities considers its computer records, systems, and software to be corporate assets. Employees are responsible for protecting these assets from unauthorized use, destruction, or unauthorized modification. This includes a prohibition against violating copyright laws or licensing agreements applicable to computer software.

Physical equipment (PCs, printers, software, diskettes, *etc.*) must be placed in a secure location to avoid theft, tampering, unauthorized use, and environmental hazards (water, smoke, magnets, *etc.*). The use of personal computers for CIM Securities business is subject to the same guidelines and restrictions as CIM Securities computers.

When an employee terminates, any disks or other storage medium that includes proprietary information, including customer information, are considered property of CIM Securities and must be left with CIM Securities.

2.19.1 Laptop Computers And Other Mobile Devices

Employees who use laptops or other mobile devices for Firm business are responsible for the security of the device and the information contained on it. Serious security breaches can occur if a device containing or capable of accessing confidential information is lost or stolen.

Employees who use laptops for company business are required to comply with the following requirements:

- Attend training on security breaches and handling of computer equipment and confidential information.

2.19.2 Reporting Lost Devices

- The loss of a mobile device **must be immediately reported to Compliance.**

2.19.3 Identifying And Reporting Data Breaches

- All employees are required to immediately report an identified potential intrusion into a mobile device or into CIM Securities's systems.

2.19.4 Software

Software installed and used on electronic devices is limited to software approved by CIM Securities. CIM Securities will install or provide authorized software for business use including anti-virus and anti-malware protection.

Employees are strictly prohibited from installing software other than what is authorized by CIM Securities.

2.19.5 Prohibited Downloading

Employees are prohibited from:

- Downloading customer and other confidential firm information from CIM Securities's mainframe or other central records, unless specifically authorized
- Using portable devices such as USB key drives, MP3 players, mobile phones, and other devices for downloading information
- Downloading programs from the Web to CIM Securities computers unless specifically authorized

2.20 Electronic Communications Policy

[FINRA Rule 3110(b)(4), 3110.07, 3110.08 and 3110.09]

This policy governs the use of electronic communications by employees including part-time employees and independent contractors. It applies during business hours and after-business hours. ***This is an important policy; employees will be required to certify annually that they are familiar with and will comply with the policy.***

1. Firm electronic systems or communications devices are for firm business purposes and business communications must conform to accepted business standards and regulatory requirements.

- Inappropriate communications (profanity, obscenity, threats, otherwise offensive content) are prohibited. Report threatening or harassing communications to Compliance.
- Communications must include current and valid information.
- Copyrighted material cannot be sent unless authorized; contact Compliance for assistance.
- Copyrighted software cannot be copied or transmitted to others unless authorized.
- References and/or links to web sites are a form of communications requiring Compliance approval prior to use.
- Communications that must be accompanied by a prospectus may not be sent electronically unless the prospectus is available as an electronic attachment or an electronic link is provided to access the prospectus.
- CIM Securities and its employees are prohibited from sponsoring a social media site or using a communication device that includes technology which automatically erases or deletes content.

2. Electronic business communications must be accessed and transmitted only through firm-sponsored systems.

- Regulators require retention of business communications and firm systems are designed to comply with retention requirements.
- Approved firm-sponsored systems include:
 - Compliance-approved external systems/computers (requires specific approval for departments and/or employees)
- The use of personal e-mail accounts for business communications is prohibited.
- Encryption of information may be required by CIM Securities; employees may not independently encrypt communications on firm systems.
- Home computers or other personal devices and external systems may not be used for business purposes (unless specifically approved by Compliance).

3. Consider electronic communications as public communications; protect confidential information.

- Do not confuse phone conversations or face-to-face communications with electronic communications. Your electronic conversation is subject to review and retention and may be the subject of subpoena in a civil or regulatory action.
- Confidential communications must not be sent on portable devices in public places unless encrypted.
- Do not view confidential information where unauthorized persons may have access (elevators, other public places).
- Safeguard portable devices to avoid unauthorized access to firm business.
- Safeguard passwords.
- Close open pages and sign out when the device is not in use.

4. There are restrictions on unsolicited e-mails under the CAN-SPAM Act of 2003.

- Unsolicited "mass" commercial e-mails are prohibited.

- "Commercial" e-mail includes any electronic messages that send a commercial advertisement or promote a commercial product or service. It does not include e-mail where there is an existing business relationship.
- Recipients may "opt-out" of receiving future e-mails. Forward such requests to Compliance.
- "Address harvesting" or "dictionary attacks" may not be used to obtain e-mail addresses off the Internet.
- E-mails sent from firm systems will include required identification of CIM Securities and disclosures or disclaimers.

5. Social media sites, blogs, and other electronic forums or communications systems may NOT be used for business communications.

Employees may not participate in social networking sites (Facebook, LinkedIn, Twitter, etc.), chat rooms, message boards, web logs, blogging, or other electronic forums or external communications systems for business communications.

6. Electronic communications will be reviewed, monitored and audited by CIM Securities.

- All electronic communications are subject to review and retention.
- Communications that require pre-use approval may not be transmitted prior to review by the designated supervisor. This includes:
 - Retail communications.
 - Communications that must be accompanied by a prospectus (Compliance approval required).
 - Advertising (Compliance approval required).

7. Use of the Internet related to CIM Securities's business is subject to restrictions.

- Employees are prohibited from posting information to the Internet without prior firm approval.
- Accessing offensive sites is prohibited. CIM Securities may block sites that are offensive or contrary to the conduct of business.

2.20.1 Failure To Comply

Failure to comply with this policy may lead to disciplinary action. Non-compliance may generate one or more of the following:

- Oral and/or written warning or notification
- Education/training
- Suspension of electronic communications privileges permanently or for a set period of time
- Regulatory discipline
- Suspension or termination of employment

2.20.2 Consent To Policy

Use of CIM Securities's electronic communications systems represents the employee's consent to the terms outlined in this Policy, including consent for CIM Securities to monitor and audit content and/or usage.

2.21 Advertising And Publishing Activities

Prior to issuing any advertising or writing any books, articles, newsletters, or other materials to be published in public media (magazines, newspaper, computer bulletin boards, Internet, *etc.*) for public access, employees must

contact Compliance for review and approval. Approval is not required for use of CIM Securities-issued research or other materials approved by CIM Securities and intended for public distribution.

2.22 Employees Acting As Trustees, Executors, Or Other Fiduciary Capacities

Employees usually will not act in a fiduciary capacity (e.g., trustee, executor) for a customer's account unless the account is for a relative of the employee. Exceptions require the approval of Compliance who should be notified by written memo requesting the exception and the reasons for the exception.

2.23 Use Of Titles

Employees may not use titles unrelated to their activities with CIM Securities. The use of any other title requires the prior approval of Compliance. Examples of the types of titles not specifically related to CIM Securities's activities include (but are not limited to) C.P.A., J.D., M.B.A., or Attorney at Law.

2.24 Annual Certification

Responsibility	CCO
Resources	<ul style="list-style-type: none">• Annual certification form
Frequency	<ul style="list-style-type: none">• Annual
Action	<ul style="list-style-type: none">• Send forms to employees for completion• Review completed forms• Take appropriate action which may include:<ul style="list-style-type: none">○ Inquiring regarding reported outside business activities○ Inquiring regarding reported outside securities accounts○ Conferring with the employee and/or employee's supervisor for any other reported information requiring follow up○ Filing updates to the employee's Form U4, if necessary
Record	<ul style="list-style-type: none">• Annual certifications are retained in an annual file for employee certifications

CIM Securities will, on an annual basis, ask employees to complete an Annual Certification form. The purpose of this form is to ensure CIM Securities's records are current regarding items to be reported to CIM Securities (outside business activities, outside accounts, etc.).

3 TRAINING AND EDUCATION

3.1 Annual Compliance Meeting

[FINRA Rule 3110(a)(7) and 3110.04]

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• List of RRs and registered principals by branch, department, or for CIM Securities
Frequency	<ul style="list-style-type: none">• Annual
Action	<ul style="list-style-type: none">• Determine appropriate subjects to include in meetings, depending on RRs and principals who are participants• Conduct compliance meetings or interviews with RRs and principals• If electronic media is used to conduct meetings, designate a local supervisor to complete an attendance record to ensure RRs and principals arrive on time and attend the entire meeting• If on-demand webcasts are used:<ul style="list-style-type: none">○ Users are assigned a unique user ID and password○ Records of attendance are maintained electronically in "read-only" format○ Each user will be advised he or she has the opportunity to e-mail or telephone questions to the presenter and receive answers in a timely manner○ Each user will be advised of Q+As available on CIM Securities's intranet and Q+As will be updated when questions are received○ The number of minutes the webcast stays on is tracked○ The webcast is configured as click-as-you-go○ At the end of the webcast a pop-up box requires the user to attest that the entire webcast was viewed (or a separate attestation will be required)• Ensure all subject RRs and principals complete the required annual meeting or interview• For RRs and principals who do not complete the requirement, take corrective action which may include contact with the RR's or principal's supervisor; limitation on business activities until the requirement is completed; other corrective action determined as appropriate for the circumstances
Record	<ul style="list-style-type: none">• A record of when and where meetings are conducted, subjects discussed, and who attended is retained by Compliance• A record of corrective action is retained in the RR's or principal's file

As required by FINRA rules, RRs and registered principals are required to attend an annual compliance meeting or interview.

CIM Securities intends to employ the use of electronic media in conducting the annual compliance meeting. The use of this media will permit the attendees to interact with the presenters to ask and have questions answered in real-time or otherwise engage the presenters in dialogue.

3.2 Continuing Education

[FINRA Rule 1240; FINRA Regulatory Notice 21-41; FINRA CE web site: <http://www.finra.org/industry/continuing-education>; FINRA FAQs: https://www.finra.org/registration-exams-ce/continuing-education/ce-transformation-faq?utm_source=MM&utm_medium=email&utm_campaign=O%5FWeekly%5FUpdate%5F111721%5FFINAL]

Registered employees are subject to SRO continuing education requirements composed of two distinct elements. Registered employees are required to complete both elements at specified time intervals. The two elements are:

Regulatory Element: This element is a computer-based training program that focuses on compliance, regulatory, ethical, and sales practice standards. Its content is derived from rules and regulations as well as standards and practices widely accepted within the industry. This element is administered by FINRA through a web-based delivery system.

Firm Element: All registered employees dealing with public customers and their supervisors are required to complete continuing education administered by CIM Securities.

3.2.1 Regulatory Element

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • CRD Firm Queues and related reports • CRD notifications of inactive registrations
Frequency	<ul style="list-style-type: none"> • Ongoing
Action	<ul style="list-style-type: none"> • Review CRD Firm queue • Request queue reports • Notify affected persons of requirements • Schedule web-based training • Review CRD notifications of inactive registrations • Notify designated supervisors of restricted persons • Review activity of restricted persons during restricted period <ul style="list-style-type: none"> ◦ Impose disciplinary action if appropriate including cancellation of commissions, letters of admonition, other appropriate action
Record	<ul style="list-style-type: none"> • Queue reports, FINRA notices, and records of notifying employees are maintained in registration files • Reviews of restricted person activities and action taken

3.2.1.1 Who Is Subject To The Requirements

All registered persons are subject to the regulatory element **ANNUALLY**.

3.2.1.2 When Requirements Must Be Completed

The regulatory element is to be completed by 12/31 each calendar year. RRs must complete training using their FinPro accounts. Registered persons who fail to complete required CE within the prescribed time frame will have their registration status changed to "CE inactive" by FINRA and are prohibited from engaging in activities requiring registration until the required CE is successfully completed.

For registered persons who become subject to statutory disqualification or disciplinary action as defined under the rules, the regulatory element must be completed within 120 days of the posting date of the disciplinary action and every three years after that date.

3.2.1.3 Regulatory Element Contact Person

[FINRA Rule 1250(a)(7)]

The CCO will notify FINRA of the name and email address of the contact person to receive CRD notices. Changes will be reported within 30 days of the change. Annually, by the 17th business day following the end of the calendar year, the contact person information will be reviewed and updated, if necessary.

3.2.2 Firm Element

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• Information regarding firm products, services, training needs• Guidance from regulators• Current regulatory concerns• Disciplinary actions
Frequency	<ul style="list-style-type: none">• Annual and ongoing
Action	<ul style="list-style-type: none">• Develop needs analyses; training plans; and training materials• Identify employees who are subject to the requirement (covered persons)• Monitor completion of requirements• Restrict covered persons who do not complete requirements• At year-end, determine whether objectives were met and whether training was effective
Record	<ul style="list-style-type: none">• Needs analyses; training plans; training materials• Dates of training, contents of training, lists of attendees• Copies of training material used• Certifications• Webcast Usage Reports

	<ul style="list-style-type: none"> • Evaluations • Records (memos, notes, <i>etc.</i>) of actions restricting covered persons
--	---

3.2.2.1 Who Is Subject To The Requirements

All registered persons who do business with the public and their supervisors are subject to the firm element. Firm element continuing education is required regardless of the length of registration or employment in the securities industry. The Firm will provide Firm Element CE through the use of a third party vendor.

3.2.2.2 Firm Requirements

CIM Securities is required to:

- identify job functions and persons subject to the requirement
- prepare an annual needs analysis including gathering information about products and services and training topics
- determine training objectives
- develop a written training plan
- implement the training plan
- retain a record of participation
- develop a method of evaluating the effectiveness of the training
- consider the evaluations in developing the next year's needs analysis
- restrict covered persons who do not complete the requirement

CIM Securities's internal program may include videos, computer training, in-person presentations, and other methods of conveying training material including a combination of methods.

3.2.2.3 Annual Needs Analysis

An annual needs analysis is prepared for covered persons.

In developing the needs analysis, the following methods will be used:

- Feedback from regulators including recent audits, regulatory alerts, and CE feedback will be evaluated
- Customer complaints, arbitrations, and other litigation involving the firm will be evaluated
- New business lines or marketing strategies will be evaluated

Needs analyses will be completed by December 31 (or shortly thereafter) each year for the upcoming calendar year.

3.2.2.4 Evaluating The Firm Element Program

Participants are asked to complete an evaluation form to evaluate the effectiveness of the firm element continuing education program. These evaluations are considered when designing the next year's continuing education program.

3.2.3 Registered Persons Who Fail To Complete Requirements

Registered persons who fail to complete the requirements of continuing education cannot conduct any duties that require registration or earn commissions or other compensation related to such activities. Registrations are considered "inactive" until continuing education requirements are completed.

The CCO will notify affected persons and their supervisors by phone, email and/or written memorandum when their registration becomes inactive and when the requirement is satisfied, and inactive status is lifted. The FINOP will also be notified by memorandum. Copies of memos will be retained in the individual's registration file.

3.2.4 Maintaining Terminated Persons' Registration

[FINRA Rule 1240(c); FINRA Regulatory Notice 21-31]

Individuals who terminate their RR or principal registration categories may maintain their qualification(s) for five years following termination of terminated registration categories subject to the following conditions:

- The person was registered for at least one year immediately preceding termination of the registration category, and the person was not subject to a statutory disqualification and is not during the term of the Maintaining Qualifications Program (MQP).
- The person must satisfy CE requirements as outlined in FINRA Rule 1240(c).

4 EMPLOYMENT, REGISTRATION AND LICENSING

4.1 Employment

4.1.1 Hiring Procedures

[FINRA Regulatory Notice 07-55]

This section outlines hiring requirements.

4.1.1.1 RR Interview Guidelines

[FINRA Notice to Members 07-06]

At the time an RR is being considered for hire, the following are areas the hiring manager should consider:

1. Discuss with the applicant the nature of the applicant's prior customers and the types of securities sold while associated with prior employers. If customers' investments include investment company products (mutual funds, variable annuities), determine whether CIM Securities has dealer or servicing agreements in place and, if not and the RR is hired, plan for suitability reviews and notification to customers of investment options and costs of switching investments.
2. Obtain the applicant's explanations regarding any customer complaints and regulatory actions to determine the merit, to the extent practicable, of each before hiring.
3. Ask the applicant about the existence of and nature of any pending proceedings, customer complaints, regulatory investigations, or arbitrations not listed in the CRD.
4. Discuss the reasons for the applicant's frequent change of employers, if applicable.
5. Obtain the RR's prior year W-2.
6. Ask the RR whether he or she signed an employment contract with the present employer and if so, obtain a copy from the RR.

4.1.1.2 Prospective RRs Require Pre-Clearance By Compliance

Information regarding RRs who are being considered for hire should be referred to Compliance for review of the individual's CRD record and background check. This review requires the written permission of the RR. The RR may sign page 4 of Form U4 or a separate form. Information regarding complaints, regulatory actions, and other information determined by Compliance will be referred to the hiring manager for consideration in extending an offer of employment.

4.1.1.3 Qualification Of Supervisors

[FINRA Rule 3110(a)(6)]

Responsibility	<ul style="list-style-type: none">• Hiring Supervisor – CCO confirms qualifications.• Compliance - determine registration requirements.
-----------------------	--

Resources	<ul style="list-style-type: none"> • Individuals identified as potential supervisors • Background information on candidate including registration status
Frequency	<ul style="list-style-type: none"> • As required when a supervisory position is to be filled
Action	<ul style="list-style-type: none"> • Hiring supervisor: <ul style="list-style-type: none"> ○ Evaluate candidate's qualifications including experience and knowledge ○ Arrange for training, if necessary • Compliance: <ul style="list-style-type: none"> ○ Confirm individual has required registration qualifications and, if not, arrange for the individual to complete the required exams ○ Notify the hiring supervisor of added qualifications required and remind him/her the individual may not act as a supervisor until necessary registrations are obtained (unless a regulator allows for a grace period to act as a supervisor before registration is completed) ○ Provide supervisory policies/procedures to the candidate if not already available to him/her
Record	<ul style="list-style-type: none"> • Hiring manager's consent to appoint the candidate to a supervisory position • Background and registration information in candidate's file • Record of training (if necessary) including a description of training and when completed • Record of providing supervisory policies/procedures

The manager and/or CCO who hires or appoints a supervisor is responsible for determining that the individual is qualified for the supervisory position. Individuals are required to have at least one year of direct experience or two years of related experience in the area to be supervised.

4.1.1.4 Background Investigation

[FINRA Rule 3110(e)]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • Employment application • Form U4 • Form U5 filed by prior employer • Public records • Outside background check services
Frequency	<ul style="list-style-type: none"> • When new employees are hired
Action	<ul style="list-style-type: none"> • Identify outside services, if any, to conduct background investigations <ul style="list-style-type: none"> ○ Where an outside service is used, review capabilities and references • Obtain records for review

	<ul style="list-style-type: none"> • Within 30 calendar days of filing the initial or transfer Form U4, verify the accuracy and completeness of information: <ul style="list-style-type: none"> ○ Contact prior employers for 3 years ○ Obtain additional information from employee, if necessary, and verify ○ Review notification from FINRA regarding public records information missing or contrary to filed U4 ○ Submit revised U4 within 30 days to reflect information received from FINRA public records search • Within 60 days of filing an application for a transferring RR, review the most recent U5 (including any amendments) and take follow up action, if necessary • Conduct further investigation where reviews reveal patterns of negative information such as customer complaints, bankruptcies, liens, criminal activity, litigation, or other negative information • Where discrepancies or incomplete information are identified, contact the employee for further information and investigate further, if needed • Evaluate negative information and its impact on the employment of the individual, consulting with the employee's supervisor
Record	<ul style="list-style-type: none"> • Review of outside services to conduct background investigations • Review of public records • Form U5 and results of review • Form U4 with related reviews and results of reviews including public records • Contact with prior employers for 3 years including contact person and date contacted • Reviews of discrepancies or missing information and action taken including consultation with employee and supervisor • Action taken, if any, after reviews conducted

Background investigations are conducted on all new employees. New employees must be accurate and complete in the information provided to CIM Securities at time of hire. Failure to do so may result in termination.

Records to be provided by a new employee may include:

- Driver's license or passport to verify identity
- Completed Form U4 (required for all registered persons)
- Prior firm's Form U5 filed on behalf of a registered person
- Other information requested by CIM Securities

Reviews conducted will include:

- Contact with at least the last three years' employers
- Form U5 from prior employer
- Form U4 filed with CIM Securities
- Review of public records by FINRA for information regarding criminal and bankruptcy records, civil litigation, judgements and liens
- Other reviews which may include a review of credit records

New employees will be required to reconcile discrepancies or missing information which may affect the employee's eligibility for hire. U4s will be updated within 30 days of notice from FINRA regarding public record discrepancies.

4.1.1.5 Fingerprints

[SEC Securities Exchange Act of 1934 Rule 17f-2; FINRA Rule 1010(d)]

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• Notifications regarding registration and other applicants
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• If necessary, identify third parties (local law enforcement officials, <i>etc.</i>) to take fingerprints and:<ul style="list-style-type: none">◦ Notify the third parties of securities industry fingerprinting requirements including identification verification procedures◦ Provide applicants with a list of acceptable third-party vendors• If fingerprints are not received by the CRD within 30 days of filing Form U4, notify appropriate supervisor that activities requiring registration must cease
Record	<ul style="list-style-type: none">• Registration files for employees include records of CRD filings and submission of fingerprints

The Firm will require all new applicants to file electronic fingerprints within 30 days of filing Form U4.

If fingerprints are not received by the CRD within 30 days, the employee must cease engaging in activities that require registration. Compliance will notify the appropriate supervisor and employee of deficiencies, and the supervisor is responsible for restricting the applicant's activities until fingerprints have been received by the CRD.

4.1.1.6 Policies And Procedures

At the time of hire, Compliance will provide the RR with a current copy of CIM Securities's policies and procedures either in hard copy or by notifying the RR of the location of policies and procedures in electronic form. At time of hire and at least annually thereafter, the RR will be asked to acknowledge, in writing or electronically, that the policies were received, and that the RR is responsible for complying.

4.1.1.7 New Employee Questionnaire

New employees will be asked to complete CIM Securities's U-4 Disclosure Notice. Any "Yes" answers will be referred to Compliance for review, including the filing of a Materiality Consultation with FINRA if applicable. See below.

Amended Rule 1100 – Materiality Consultation prior to hiring RRs with one or more criminal matters or two or more specified risk events.

A written request for a materiality consultation pursuant to Rule 1017(a)(7) must address the issues that are central to the materiality consultation. Thus, the materiality consultation would focus on, and the firm would need to provide information relating to, the conduct underlying the individual's "final criminal matters" and "specified risk events," as well as other matters relating to the subject person, such as disciplinary actions taken by FINRA or other industry authorities, adverse examination findings, customer complaints, pending or unadjudicated matters, terminations for cause or other incidents that could indicate a threat to public investors. The Department of Member Supervision's (Member Supervision) assessment in the materiality consultation would consider, among other things:

- whether the "final criminal matters" or "specified risk events" are customer-related;
- whether they represent discrete actions or are based on the same underlying conduct;
- the anticipated activities of the person;
- the disciplinary history, experience and background of the proposed supervisors, if applicable;
- the disciplinary history, supervisory practices, standards, systems and internal controls of the member firm and whether they are reasonably designed to achieve compliance with applicable securities laws and regulations and FINRA rules;
- whether the member firm employs or intends to employ in any capacity multiple persons with one or more "final criminal matters" or two or more "specified risk events" in the prior five years; and
- any other investor protection concerns raised by seeking to make the person an owner, control person, principal or registered person of the member firm.

4.1.1.8 Enhanced Compensation

[SEC Chairman letter to broker-dealers dated August 31, 2009: <http://www.sec.gov/news/press/2009/2009-189-letter.pdf>]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor, CCO
Resources	<ul style="list-style-type: none"> • Details of RR compensation agreements
Frequency	<ul style="list-style-type: none"> • As required when RRs are hired with enhanced compensation agreements
Action	<ul style="list-style-type: none"> • Determine the terms of any enhanced compensation • Where commission targets or higher payouts on specific securities or products are included in compensation arrangements, include consideration of those incentives in regular reviews of the RR's business during the term of the compensation agreement to identify any improper activity to maximize commissions such as churning or unsuitable recommendations • Where potential improper activities are identified, take corrective action which may include conferring with the RR, conferring with Compliance, contacting customers, cancelling transactions, or any other corrective action deemed appropriate for the situation

Record	<ul style="list-style-type: none"> • Compensation agreements • Review of RR transactions including notation of corrective action taken, where appropriate
---------------	---

CIM Securities may hire experienced RRs from other broker-dealers and offer enhanced compensation to attract qualified individuals for employment and to assist in the transition period when an RR moves from another firm. Compensation agreements may include up-front bonuses, higher payouts for a period of time, payment of licensing fees (where CIM Securities otherwise would not pay them), and other enhanced compensation determined at the time an offer is made.

4.1.1.9 Recruitment Practices And Account Transfers (If Applicable)

[FINRA FAQs: <https://www.finra.org/rules-guidance/guidance/faqs/frequently-asked-questions-regarding-finra-rule-2273>]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor, CCO
Resources	<ul style="list-style-type: none"> • Newly-hired RRs
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Instruct responsible persons to provide the required communication to former customers transferring to CIM Securities • Monitor accounts transferred within 3 months of the RR's hire to confirm communications are provided
Record	<ul style="list-style-type: none"> • New RRs including date of hire • Communications provided to former customers

When an RR is hired by CIM Securities, each former customer transferring to CIM Securities will be provided, in paper or electronic form, an educational communication prepared by FINRA. The requirement applies for 3 months following the date the RR begins employment with CIM Securities.

The communication will be provided when:

- The former customer of the RR is contacted by CIM Securities or through a representative to transfer assets; or
- A former customer, without individual contact, transfers assets to an account assigned, or to be assigned, to the RR.

Events that trigger the requirement include oral or written communications by the newly-hired RR:

- informing the former customer that he or she is now associated with the recruiting firm;
- suggesting that the former customer consider transferring his or her assets or account to the recruiting firm;
- informing the former customer that the recruiting firm may offer better or different products or services; or

- discussing with the former customer the fee or pricing structure of the recruiting firm.

Communication with a group of customers via a mass mailing, e-mail, or automated phone calls or voicemails also triggers the requirement to provide the disclosure to the customers.

The educational communication must be provided as follows:

- at the time of first individualized contact regarding transferring assets to CIM Securities.
 - If first contact is in writing, the disclosure must accompany the written communication.
 - If by electronic communication, a hyperlink to the disclosure may be included.
 - If oral, the RR must notify the customer that an educational communication that includes important considerations about transferring assets will be provided no later than 3 business days after the contact.
- If the customer seeks to transfer assets but there has been no individualized contact with the customer, the communication must be sent to the customer with the transfer approval documentation.

If the former customer states he or she will not transfer assets, the educational communication requirement does not apply. Should the former customer decide to transfer assets within 3 months of the RR's employment, the communication must be provided with the account transfer approval documentation.

4.1.1.9.1 Exceptions

"Former customer" includes any customer that had a securities account assigned to a registered person at the representative's previous firm. The term "former customer" does not include a customer account that meets the definition of an "institutional account" as defined in FINRA Rule 4512(c); accounts held by a natural person do not qualify for the institutional account exception.

The Rule does not apply to circumstances where a customer's account is proposed to be transferred to CIM Securities via a bulk transfer or due to a change of broker-dealer of record.

4.1.2 Termination Procedures

[FINRA Corporation By-Laws Article V Section 3; FINRA Rule 3110(f); FINRA Regulatory Notice 19-10]

Responsibility	<ul style="list-style-type: none"> • CCO, IB Supervisor
Resources	<ul style="list-style-type: none"> • Notification from RR or supervisor of termination
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Immediately notify Compliance of terminating registered employees • Immediately notify Compliance of terminating non-registered employees where termination was caused by theft or fraud • Immediately notify Human Resources of terminating registered and non-registered employees • Secure computers and computer files • Retrieve office keys, company credit cards, <i>etc.</i> from terminated employee • Regarding customers of the departing RR: <ul style="list-style-type: none"> ○ Promptly reassign accounts

	<ul style="list-style-type: none"> ○ Promptly and clearly communicate to customers how accounts will continue to be serviced ○ Provide timely and complete answers, if known, when customers ask questions about the RR including, when asked, the choice of the newly assigned RR or an alternative RR or the availability of transferring the account to another firm ○ If the departing RR has consented and the customer asks, provide reasonable contact information (phone number, e-mail or mailing address) • Compliance will file Form U5 for terminating RRs • Compliance will provide the terminated RR with a copy of the RR's Form U5 within 30 days of termination
Record	<ul style="list-style-type: none"> • The CRD retains copies of Form U5

4.1.2.1 Notification To Compliance

Whenever an employee terminates employment from CIM Securities, the designated supervisor is responsible for immediately notifying Compliance. Notification to Compliance regarding registered employees should include:

- Name of terminated person and RR number(s)
- Type of termination (voluntary, permitted to resign, discharged, *etc.*)
- If the termination is not voluntary, an explanation of the reason for termination
- Date of termination
- Any known compliance problems at the time of termination

4.1.2.2 Securing And Retrieving Firm Property

If applicable, designated supervisors are responsible for retrieving CIM Securities property from terminated employees including office keys, company credit cards, computer files, customer files, and any other items which are the property of CIM Securities.

4.1.2.3 Reassignment Of Accounts

If applicable, designated supervisors are responsible for reassigning the accounts of terminated RRs.

4.1.2.4 Responding To Customer Inquiries

As applicable, designated supervisors should instruct branch or department employees, including RRs receiving reassigned accounts, to only indicate the employee is no longer with CIM Securities if asked why the RR is gone. No details or speculation regarding the departure should be given to customers or anyone else outside CIM Securities unless authorized by Compliance to do so.

If asked by a customer, the customer may be advised he/she may be serviced by the newly assigned RR or an alternative RR or may transfer the account to another firm. If the departing RR consents, reasonable contact information may be provided in response to inquiries (phone number, e-mail or mailing address).

4.1.2.5 Form U5

Compliance is responsible for filing Form U5 for any terminated registered employee. Compliance will also send, within 30 days of termination, a copy of Form U5 to the former employee.

4.2 Registration And Licensing

[FINRA Corporation By-Laws Article V; FINRA Rule 1200 series; FINRA Regulatory Notice 17-30; FINRA FAQs: <https://www.finra.org/registration-exams-ce/qualification-exams/fag>; NASDAQ Rule 1000 series]

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• New hire notices• Change of status notices• Requests for registration• CRD Late Filing Fee Report
Frequency	<ul style="list-style-type: none">• Quarterly - review CRD Late Filing Fee Report• As required for new hires and requests for registration• Periodically - confirm personnel are registered as required and those with "permissive registration" do not act outside the scope of their assigned functions
Action	<ul style="list-style-type: none">• Identify employees who require registration by reviewing new hire or change of status records• Submit required filings to the CRD• Acknowledge electronic filings are on behalf of CIM Securities and its employees• Request and schedule examinations• Ensure employees who require registrations obtain them• Amend U4s or U5s when there are reportable events• Review the CRD Late Filing Fee Report to identify late filings and to take corrective action• Affirm that employees are registered as required for their responsibilities• For those with "permissive registration:"<ul style="list-style-type: none">○ Assign persons with permissive qualification to a registered supervisor (representative or principal to supervise a representative; principal to supervise a principal); the assigned registered person is responsible for periodically contacting the person's direct supervisor to confirm the person is not acting outside his/her assigned responsibilities
Record	<ul style="list-style-type: none">• Registration records including CRD notices, approvals, amendments, and other registration records are maintained in employee files<ul style="list-style-type: none">○ Where the registered person's signature is not required on U4 amendments, CIM Securities may rely on the CRD for recordkeeping• The CRD Late Filing Fee Report is retained in a CRD report file with initials of who reviewed and date reviewed and any action taken

	<ul style="list-style-type: none"> • Affirmation regarding appropriate registrations or activities
--	---

This section outlines the requirements for registration. All individuals engaged in activities (including selling or trading products such as stocks, bonds, options, insurance, *etc.*) or supervising such activities subject to registration requirements must complete the necessary registration and licensing prior to engaging in such activities (with the 120-day exception explained below). Employees may not conduct business with public customers or engage in other activities requiring registration until required registrations are effective.

Changes in registration requirements became effective October 1, 2018.

4.2.1 Persons Registered Prior To October 1, 2018

- Individuals registered prior to October 1, 2018 who maintain their registration on or after that date may continue conducting business requiring their registration status without further requirements.
- Individuals whose registration terminated between October 1, 2014, and September 30, 2018 are not required to take the Securities Industry Essentials (SIE) examination provided they re-register within four years from the date of their last registration.

4.2.2 Registered Representatives

Individuals registering as representatives after October 1, 2018 must satisfy the following requirements:

- Pass the SIE examination; and
- Pass a representative-level qualification examination (such as the Series 7 exam).

Accepting customer orders requires registration as a representative.

As of October 1, 2018, FINRA has eliminated the registration categories of Order Processing Assistant Representative, United Kingdom Securities Representative, Canada Securities Representative, Options Representative, Corporate Securities Representative, Government Securities Representative and Foreign Associate. These registrations may be maintained but will not be reinstated if registration is terminated.

4.2.3 Registered Principals

Firms are required to have at least two officers or partners (unless a one principal exemption has been granted by FINRA) who are registered as General Securities Principals; however, a firm limited in its activities may instead have two officers or partners who are registered in a principal category corresponding to the scope of the firm's activities.

Principals are required to pass the SIE, representative level, and principal-level qualification examinations.

Representatives who assume duties that require principal registration have 120 calendar days to pass the appropriate principal examination, provided that such person has at least 18 months of experience functioning as a registered representative within the five-year period immediately preceding the designation and has fulfilled all applicable prerequisite registration, fee and examination requirements prior to designation as a principal.

4.2.3.1 Financial And Operations Principal (FINOP) And Introducing Broker-Dealer Financial And Operations Principal

Every firm is required to designate a FINOP (which includes a FINOP for an introducing BD) unless exempt from the requirement. The FINOP is responsible for the BD's financial reports including approval and preparation; compliance with financial responsibility rules; supervision of those preparing reports, maintaining books and records, and engaged in back office operations; and any other matter involving the financial and operational management of the member.

4.2.3.2 Principal Financial Officer And Principal Operations Officer

CIM Securities will appoint a Principal Financial Officer and Principal Operations Officer subject to the following:

- The Principal Financial Officer is responsible for financial filings and related books and records.
- The Principal Operations Officer has primary responsibility for the day-to-day operations of the business, including overseeing the receipt and delivery of securities and funds, safeguarding customer and firm assets, calculation and collection of margin from customers and processing dividend receivables and payables and reorganization redemptions and those books and records related to such activities.
- Both must qualify through registration as a Financial and Operations Principal or Introducing Broker Financial and Operations Principal as well as an Operations Professional. No exam is required for these principals to qualify as an Operations Professional. The FINOP exam does not apply to BDs exempt from the FINOP requirement.
- Introducing vs. clearing firms:
 - If the firm neither self-clears nor clears for others, the same person may act in both roles as well as Financial and Operations Principal or introducing Broker-Dealer Financial and Operations Principal.
 - Firms that are clearing and self-clearing must designate separate persons to function as Principal Financial Officer and Principal Operations Officer, though such individuals may also carry out the responsibilities of a Financial and Operations Principal.
 - A clearing or self-clearing firm that is limited in size and resources may request a waiver of the requirement to designate separate persons to function as Principal Financial Officer and Principal Operations Officer.
- Firms may appoint multiple Principal Operations Officers (but not Principal Financial Officers), provided that the firm precisely defines and documents the areas of primary responsibility and makes specific provision for which of the officers has primary responsibility in areas that can reasonably be expected to overlap.
- A Principal Financial Officer or a Principal Operations Officer is permitted to delegate his or her day-to-day duties to other principals at the firm with the understanding that ultimate responsibility for the function rests with the Principal Financial Officer and the Principal Operations Officer.

4.2.3.3 Compliance Officer

CIM Securities will designate a Compliance Officer (unless it is engaged in limited investment banking or securities business). An individual designated as Chief Compliance Officer on Schedule A of Form BD may register in a principal category that corresponds to the limited scope of business. Individuals who have the prerequisite qualifications prior to October 1, 2018 may be designated as Compliance Officer without taking further examinations. Those qualifying on or after October 1 must qualify as a General Securities Representative including the SIE; General Securities Principal (Series 24); and Compliance Official (Series 14).

4.2.3.4 BDs Exempt From FINOP Requirement

BDs exempt under FINRA Rule 1220(a)(4) are not required to designate a FINOP. In addition, they may name the same person as Principal Financial Officer and Principal Operations Officer.

4.2.4 Expiration Of Registrations

When a registration is terminated, there are grace periods for re-registering before an individual must re-take examinations. These periods are:

- SIE registration: four years
- Representative or principal: two years

4.2.5 Persons Exempt From Registration

[FINRA Rule 1230]

The following persons are not required to be registered with FINRA:

- persons whose functions are solely and exclusively clerical or ministerial; and
- persons whose functions are related solely and exclusively to:
 - effecting transactions on the floor of a national securities exchange and who are appropriately registered with such exchange;
 - transactions in municipal securities;
 - transactions in commodities; or
 - transactions in security futures provided that any such person is registered with a registered futures association.

4.2.6 FSAWP Waivers

[FINRA Rule 9600]

As applicable, Individuals who go to work for a foreign or domestic financial services industry affiliate of CIM Securities and have previously received the Financial Services Affiliate Waiver Program (FSAWP) waiver have the option of continuing in the FSAWP. This waiver program is not available to new applicants. Participants are subject to annual Regulatory Element Continuing Education.

4.2.7 Other Registrations

- CIM Securities may permit any employee to become registered as a representative or a principal, including individuals working in a clerical or ministerial capacity ("permissive qualification"). If not required for the person's responsibilities, approval by the supervisor and Compliance is required. These individuals are subject to regulatory conduct rules such as outside business activities, private securities transactions, *etc.* All registered persons, including those who solely maintain a permissive qualification, are required to satisfy the annual Regulatory Element of continuing education. Permissively qualified persons will be assigned to a registered supervisor who is responsible for confirming that individual does not act outside the scope of his/her responsibilities or registration status.

- Anyone (whether employed by a member firm or not) may ask to take the SIE exam. That person cannot be registered with FINRA unless employed by a member firm and has completed an RR qualification examination.

4.2.8 Qualified Persons Serving In The Armed Forces

[FINRA Rule 1210.10]

FINRA provides exceptions for qualified persons who volunteer for or are called into active U.S. military service. The supplementary material should be consulted for details of the requirements.

4.2.9 CRD Electronic Filings

[FINRA Rule 1010]

CIM Securities has designated one or more employees with authority over registration functions, as named in CIM Securities's *Designation Of Supervisors* chart. Any supervisor of electronic filings is a registered principal or a corporate officer and is responsible for review and approval of electronic filings and acknowledging electronically that the forms are filed on behalf of CIM Securities and its associated persons.

4.2.10 State Registrations

RRs must be registered in the state from which they conduct business and may be required to be registered in other states where customers are domiciled. Most states require successful completion of the Series 63 Uniform State Agent Securities Law Examination. Successful completion of the exam does not automatically confer registered status on the examinee. Application must be made to the CRD to obtain each state registration.

The designated supervisor is responsible for identifying transactions in states where registration may be required.

4.2.11 Parking Registrations

[FINRA Rule 1210.11]

CIM Securities does not permit individuals to "park" licenses. Parking occurs when CIM Securities maintains a registration on behalf of an individual that does not work for CIM Securities or who does not need that registration for their job function. Registration status is retained only for those persons where it is required. CIM Securities may, however, maintain registration for legal, compliance, or other non-sales employees as permitted under regulators' rules.

4.2.12 Form U4

[FINRA Rule 1010 and 2263]

All applicants for registration are required to complete Form U4. It is the RR's responsibility to include accurate information and promptly notify CIM Securities of any updates that may require amendment to Form U4.

At the time a new or amended U4 is signed, the applicant will be provided the *Form U4 Disclosure To Associated Persons*, which discloses information about the predispute arbitration clause included in Form U4.

4.2.13 Amendments To Form U4 Or Form U5

CIM Securities will submit amendments to Form U4 when an RR advises of updates that require amendment. Compliance is responsible for determining whether reportable events or other matters require the filing of an amendment to an RR's Form U4. Compliance is also responsible for identifying disciplinary or complaint matters to be reported on Form U5 termination notices including amendments required after termination. Required reportable events include the receipt of an SEC Wells notice.

The FINOP is responsible for providing requested information.

4.2.14 Assignment Of RR Numbers (IF APPLICABLE)

RR numbers are assigned by Compliance. New numbers will not be assigned to individuals who are not yet registered with CIM Securities. An RR number may be assigned prior to registration approval when customer accounts are being transferred and the RR number is needed to transfer accounts. However, the number is not approved for conducting business until all registration approvals have been received.

4.2.15 Maintaining Terminated Persons' Registration

[FINRA Rule 1240(c); FINRA Regulatory Notice 21-31]

Individuals who terminate their RR or principal registration categories may maintain their qualification(s) for five years following termination of terminated registration categories subject to the following conditions:

- The person was registered for at least one year immediately preceding termination of the registration category, and the person was not subject to a statutory disqualification and is not during the term of the Maintaining Qualifications Program (MQP).
- The person must satisfy CE requirements as outlined in FINRA Rule 1240(c).

4.3 Statutorily Disqualified Persons

[FINRA Rule 9285; FINRA Regulatory Notice 21-09 and 09-19; SEC Securities Exchange Act of 1934 Rule 19h-1 and Section 3(a)(39); FINRA By-Laws Article III Section 3 and Section 4; FINRA FAQs for MCDC firms: <https://www.finra.org/rules-guidance/guidance/faqs/faq-eligibility-proceedings-firms-participating-mcdc-initiative>]

Responsibility	<ul style="list-style-type: none">• CCO, IB Supervisor
Resources	<ul style="list-style-type: none">• N/A
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Compliance will:<ul style="list-style-type: none">○ Complete the required regulatory forms○ Establish an interim plan of heightened supervision that would be in effect throughout the application review process

	<ul style="list-style-type: none"> ○ Establish procedures for conducting heightened supervision: <ul style="list-style-type: none"> ▪ during the pendency of an appeal from, or NAC review of, a disciplinary decision ▪ including specific supervisory policies or procedures to address violations ▪ considering the conditions or restrictions imposed by the Hearing Officer or Review Subcommittee, and ▪ designate the responsible principal, who must sign the heightened procedures and carry out supervision • The designated supervisor will: <ul style="list-style-type: none"> ○ Sign a copy of the heightened supervision plan ○ Conduct required supervision ○ Provide Compliance with certifications of supervision, if required
Record	<ul style="list-style-type: none"> • Regulatory applications/forms and related documents are retained in the RR's file in Compliance • Copy of the heightened supervision plan and records of supervision • Certification of supervision, if required

4.3.1 Introduction

Individuals may become subject to statutory disqualifications as a result of a felony conviction or regulatory suspension, revocation of registrations or injunctions (including actions by domestic regulators including the CFTC and actions by foreign regulators). The definition of statutory disqualification is included in Section 3(a)(39) of the Securities Exchange Act of 1934. FINRA Regulatory Notice 09-19 includes a chart, in Attachment B, that outlines statutory disqualifications under the Rule.

4.3.2 Hiring Or Retaining Employment Of A Statutorily Disqualified Person

All prospective employees (including those engaged solely in clerical and/or ministerial activities) are subject to background investigations that include identification of potential statutory disqualification. Prior to hiring an individual subject to a statutory disqualification, Compliance should be consulted to review the nature of the statutory disqualification and potential heightened supervision that may be required. When an existing employee becomes subject to a statutory disqualification, CIM Securities is required to submit an application to continue associating with a disqualified person and establish an interim plan of heightened supervision in effect throughout the application review process.

4.3.3 Regulatory Filings

[FINRA Rule 4517]

Compliance is responsible for completion and filing of the appropriate regulatory form or application, which will be signed by a senior officer or partner of CIM Securities. A hearing may be required prior to approval of a new employee or existing employee's continued association with CIM Securities.

4.3.4 Supervision

Compliance will establish procedures to carry out the supervision required under agreement with the SRO reviewing the disqualified person, including records of supervision to be conducted by the designated supervisor. The supervisor assigned to supervise the statutorily disqualified person will be provided a copy of the procedures which must be signed by the supervisor who is then responsible for carrying them out.

4.3.5 Reporting Statutory Disqualifications

When an employee becomes subject to a statutory disqualification, Compliance will file the necessary registration updates and, in addition, the required notification on the quarterly complaint report will be made to regulators consistent with those SRO's reporting requirements.

4.4 Broker-Dealer Registration

4.4.1 Form BD

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• Information regarding reportable items including civil and regulatory actions• Records regarding officers and directors to be included on Form BD• Other information as required by Form BD
Frequency	<ul style="list-style-type: none">• As required - updates• Quarterly - review for potential updates
Action	<ul style="list-style-type: none">• Prepare updates as required; consult with in-house or outside counsel, as required• File Form BD updates• At least quarterly review Form BD for potential updates
Record	<ul style="list-style-type: none">• File of BD amendments

Compliance is responsible for updating Form BD when necessary and filing with the required SROs and other regulatory agencies.

4.4.2 Member Application And Associated Person Registration (MAP Rules)

[FINRA Rule 1000 series; FINRA Regulatory Notice 21-09; FINRA web site re mergers, acquisitions, and business transfers: <http://www.finra.org/industry/checklist-organizational-change-important-steps-related-merger-acquisition-or-succession>; NASDAQ Rule 1017]

When CIM Securities anticipates a material change in its business, Compliance will file requests for approval by the appropriate SROs.

4.4.2.1 Events Requiring Approval

Events that require approval include merger with or acquisition of another broker-dealer or acquisition of 25% or more of the assets of another dealer; a change in ownership or control; and a material change in business operations. In addition, material changes include removing or modifying a membership agreement restriction; market making for the first time; adding business activities that require a higher level of minimum net capital; and engaging in activities beyond proprietary trading as defined in NASDAQ rules.

Certain types of expansions are presumed to not be a "material change in business operations" and do not require FINRA approval. However, this safe harbor is not available to firms that, among other things, have a "disciplinary history" as defined in IM-1011-1 or that seek to add a natural person who has, in the prior five years, one or more final criminal matters or two or more specified risk events and seeks to become an owner, control person, principal, or registered person of CIM Securities. The interpretation must be consulted to determine what changes are not material and what constitutes disciplinary history precluding use of the safe harbor.

If CIM Securities operates under a Restriction Letter, it will conduct business consistent with the Letter and Compliance will contact FINRA if a change is necessary.

4.4.2.2 Employment (New Or Continuing) Of A Natural Person Subject To Criminal Matters Or Risk Events

[FINRA Regulatory Notice 21-09]

CIM Securities must file a Continuing Membership Application (CMA) when a person who, during the past five years, becomes subject to one or more "final criminal matters" or two or more "specified risk events" and seeks to become an owner, control person, principal or registered person of CIM Securities. As an alternative, CIM Securities may submit a written request to FINRA for a materiality consultation for the contemplated activity. This does not apply to an existing RR or principal of CIM Securities who seeks to add an additional RR- or Principal-level registration, respectively.

4.4.3 Regulatory Contact Information

CIM Securities is obligated to maintain current contact information with regulators.

4.4.3.1 FINRA and NASDAQ Contact Information

[FINRA Rule 4517; FINRA Contact System web page: <http://www.finra.org/Industry/Compliance/RegulatoryFilings/FCS/>]

Updates to contact information will be made within 30 days following any change. In addition, by the 17th business day after the end of each calendar year, CIM Securities is required to verify contact information through the FINRA Contact System.

Compliance will update the following information through FINRA's Contact System when necessary and will conduct the mandatory annual verification:

- Executive Representative [FINRA By-Laws Article IV, Section 3, FINRA Rule 4517; NASDAQ Rule 1150]
- Regulatory Element Continuing Education Contact Person [FINRA Rule 1250]
- Emergency contact persons [FINRA Rule 4370]
- AML contact person(s) [FINRA Rule 3310.02]
- Other contacts mandated by FINRA rules

Contact information will be provided promptly to FINRA upon request, but no later than 15 days after the request.

4.4.4 FINRA Entitlement Program

[FINRA FAQs: <http://www.finra.org/industry/saa-faq>]

FINRA's Entitlement Program provides authorized Firm personnel with access to FINRA Web Applications. CIM Securities has designated a Super Account Administrator (SAA) who is responsible for creating, editing, or deleting accounts for Account Administrators and users at CIM Securities. The designating criteria for the SAA are as follows:

- Must be formally delegated the authority by CIM Securities and as authorized in the New Organization Super Account Administrator (SAA) Form (or Update/Replace Super Account Administrator (SAA) Form) to perform the SAA responsibilities on its behalf.
- The designation must be executed on the current version of FINRA's New Organization SAA Form (or Update/Replace SAA Form), as instructed, and be executed by an Authorized Signatory, as defined by FINRA. An SAA may serve in this role for multiple organizations (affiliated or non-affiliated); however, a separate user name and password is required for each organization. The individual does not need to have an existing FINRA Entitlement Account.

The SAA is responsible for the following:

- Designate Account Administrators and users
- Update authorized persons as required
- Certify annually to FINRA
- Retain information about authorized users, updates, and certifications

4.4.5 Regulatory Filings

[FINRA Rule 4517]

CIM Securities will submit regulatory filings electronically where required. Filing procedures are included in appropriate sections of this manual.

4.4.6 Reporting Requirements

[FINRA Rule 4530; FINRA Regulatory Notice 11-32; FINRA FAQs on Rule 4530: <https://www.finra.org/filing-reporting/regulatory-filing-systems/rule-4530/faq>]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • Criminal, civil, and arbitration actions against CIM Securities
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Determine whether information or events are reportable • File information [specified in Rule 4530(f)(1)] with FINRA; information will be filed within 30 calendar days after knowing of the event; copies of documents will be filed promptly
Record	<ul style="list-style-type: none"> • Record of filings

CIM Securities will file information with FINRA for reportable events involving CIM Securities under FINRA Rule 4530 within 30 calendar days of becoming aware of the reportable event. When CIM Securities concludes CIM Securities has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization, such reported violations will include only conduct that has widespread or potential widespread impact to CIM Securities, its customers or markets, or conduct that arises from a material failure of CIM Securities's systems, policies or practices involving numerous customers, multiple errors or significant dollar amounts.

Refer to the section *Reporting Possible Law Or Rule Violations* in the chapter *GENERAL EMPLOYEE POLICIES* for procedures addressing the identification of violations, escalation of internal reporting, and reporting of internal conclusions.

4.5 Heightened Supervision

[FINRA Regulatory Notice 18-15]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • Form U4 information • CRD • Customer complaints • Regulatory actions • Other activity that may warrant heightened supervision, at the discretion of Compliance
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Compliance: <ul style="list-style-type: none"> ○ Identify employees subject to heightened supervision ○ Determine the scope of heightened supervision ○ Notify the employee's supervisor of required supervision ○ Collect certifications from supervisor

	<ul style="list-style-type: none"> • Designated supervisor: <ul style="list-style-type: none"> ○ Conduct required heightened supervision ○ Prepare and send certifications to Compliance
Record	<ul style="list-style-type: none"> • Reviews of employees for potential heightened supervision are retained in a "Heightened Supervision" file in Compliance • Memos and certifications pertaining to a specific employee are retained in Compliance's file for the employee

4.5.1 Introduction

CIM Securities will institute heightened supervision for RRs or other employees when appropriate. The following sections describe CIM Securities's procedures for identifying those subject to heightened supervision and the types of supervision that may be conducted. Reference to "employees" also includes independent contractors affiliated with CIM Securities.

4.5.2 Identifying Employees For Heightened Supervision

It is the responsibility of Compliance to identify employees for potential heightened supervision. Employees will be identified at the time of hire or when an employee becomes subject to regulatory action and/or a pattern of customer complaints. Unregistered individuals who were previously registered and the subject of customer or regulatory complaints are also subject to consideration for heightened supervision.

4.5.3 Criteria For Identifying Candidates For Heightened Supervision

The following are criteria that will trigger a review by Compliance to determine whether an employee should be subject to heightened supervision. Pending as well as resolved matters will be considered. The criteria are subjective and the details of complaints and/or regulatory actions must be considered in determining whether heightened supervision is necessary.

- Three or more customer complaints alleging sales practice abuse within the past two years (complaints include written complaints, arbitrations, other civil actions)
- Complaint filed by a regulator
- Injunction in connection with an investment-related activity
- Termination for cause or permitted to resign from a former employer where the termination appears to involve a significant sales practice or regulatory violation
- Employment with three or more broker-dealers in the past five years
- Direct or indirect outside business activities associated with microcap and OTC companies (see the section *Low-Priced And Microcap Securities* in the chapter *ORDERS*)
- Traders involved in trading microcap and low-priced OTC securities (determined by Trading Supervisor)

4.5.4 Heightened Supervision Memorandum

When a candidate is identified for possible heightened supervision Compliance, in consultation with the RR's supervisor, will consider whether heightened supervision will be established. After the determination is made, Compliance will prepare a memorandum outlining action taken (or not taken).

Where it is determined that CIM Securities's existing supervision is adequate to address oversight of the candidate, Compliance will document in the memorandum the reasons why existing supervision is adequate. Where it is decided heightened supervision will be conducted, Compliance will outline the supervision to be conducted (including type, frequency, time period of heightened supervision, and how supervision should be documented) and provide copies of the memorandum to the subject RR and the RR's supervisor outlining the terms of the heightened supervision. The RR and the supervisor will sign and return copies of the memorandum to Compliance.

4.5.5 Scope Of Potential Heightened Supervision

Heightened supervision will be established after considering the specifics that apply to the RR. Heightened supervision may take many forms and may include some of the following, to be determined by Compliance. This list does not limit or prescribe how heightened supervision should be structured for any one RR, since each case must be reviewed individually.

- Limits on type of business (option, futures, *etc.*)
- Limits on types of accounts (discretionary, certain age groups or other demographics, *etc.*)
- Verification with customers of new account information when accounts are opened
- Pre-approval of some or all trades entered
- Pre-approval of certain types of accounts
- Contact with customers by the RR's designated supervisor
- Pre-approval of all written public communications originated by the RR
- Extra training or continuing education in areas subject to heightened supervision
- Assignment of the RR to a "mentor" or partner

4.5.6 Certification By RR's Supervisor

During the term of heightened supervision, the RR's supervisor will certify to Compliance, in writing, that the heightened supervision has been conducted. The form and frequency of certification will be determined by Compliance and will be explained in the Heightened Supervision Memorandum provided to the supervisor.

5 COMMUNICATIONS WITH THE PUBLIC

[FINRA Rule 2200 Series, 3110(b)(4), 3110.06, 3110.07, 3110.08 and 3110.09; FINRA Regulatory Notice 19-31; FINRA Rule 2210 Q & A: <https://www.finra.org/industry/finra-rule-2210-questions-and-answers>]

5.1 Introduction

[FINRA Rule 2200 Series; FINRA Regulatory Notice 12-29]

This chapter explains regulatory and policy requirements when dealing with the public through a wide range of media including electronic media. "Communications" consist of correspondence, retail communications and institutional communications.

In general,

- All communications must be truthful and balanced.
- Communications (incoming and outgoing) are subject to review by CIM Securities. Do not expect confidentiality for any communications that are received by you or that you send from CIM Securities.
- CIM Securities's facilities and systems (email, fax, etc.) should be used for business purposes only.
- Records of communications (incoming and outgoing) are retained by CIM Securities and are subject to review by regulators and subpoena in civil actions.

5.2 Definitions

[FINRA Rule 2210(a)]

There are three broad categories of communications as defined by rule. ***"Written communications" include electronic communications.***

Retail communication: includes **any** written communication (including advertising, telemarketing and other sales scripts and other written communications) that is published, distributed or made available to **more than** 25 retail investors within any 30 calendar-day period. *Requires pre-use approval except that the following do not require pre-use approval and may be supervised like correspondence:*

- *Communications excepted from the definition of "research report" **unless** the communication makes any financial or investment recommendation;*
- *Any retail communication that is posted on an online interactive electronic forum; and*
- *Any retail communication that does not make any financial or investment recommendation or otherwise promote a product or service of CIM Securities.*

Institutional communication: includes written communications that are distributed or made available only to institutional investors. *(Does not require pre-use approval, reviewed consistent with correspondence requirements.)*

Correspondence: Includes any written communication that is distributed or made available to **25 or fewer** retail investors within any 30 calendar-day period. *(Does not require pre-use approval unless indicated otherwise for specific products or services.)*

Additional definitions include:

Retail investor: includes any person other than an institutional investor, regardless of whether the person has an account with CIM Securities.

Institutional investor: includes a:

1. government entity or subdivision thereof;
2. employee benefit plan, or multiple employee benefit plans offered to employees of the same employer, that meet the requirements of Section 403(b) or Section 457 of the Internal Revenue Code and in the aggregate have at least 100 participants, but does not include any participant of such plans;
3. qualified plan, as defined in Section 3(a)(12)(C) of the Exchange Act, or multiple qualified plans offered to employees of the same employer, that in the aggregate have at least 100 participants, but does not include any participant of such plans;
4. FINRA member firm or registered person of such a member; and
5. person acting solely on behalf of any such institutional investor.

Institutional investor also includes [per FINRA Rule 4512(c)] an account for:

1. a bank, savings and loan association, insurance company or registered investment company;
2. an investment adviser registered either with the SEC under Section 203 of the Investment Advisers Act or with a state securities commission (or any agency or office performing like functions); or
3. any other person (whether a natural person, corporation, partnership, trust or otherwise) with total assets of at least \$50 million.

5.3 Retail Communications

Responsibility	<ul style="list-style-type: none">• IB Supervisor – CCO – File with FINRA as required• Compliance (approval of advertising, file retail communications with FINRA (if required))
Resources	<ul style="list-style-type: none">• Retail communications submitted for review
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Review proposed retail communications• Make revisions as needed• Provide requestor with approved copy or notify of disapproval• File communication with FINRA, if required; notify requestor of any required delay to receive FINRA approval
Record	<ul style="list-style-type: none">• Dates of first and (if applicable) last use• Copies of reviewed communications, including the reviewer's approval and date of approval• For communications not requiring pre-approval, the name of the person who prepared or distributed the communication• Information regarding the source of any statistical table, chart, graph or other illustration used in the communication• Copies of communications filed with FINRA (see section <i>FINRA Filing Requirements</i>) and FINRA response/approval (as applicable)• If the communication was prepared by another member firm and filed with FINRA, the name of the firm and a copy of FINRA's review letter

Retail communications, which include advertising, require the **prior approval** of the designated supervisor prior to use or distribution. Advertising also requires the **prior approval** of Compliance and may be filed with FINRA depending on the content. The person submitting the retail communication for review (and that person's supervisor, if applicable) will be notified of approval or the need to make changes prior to release.

5.3.1 FINRA Filing Requirements

[FINRA Rule 2210(c)]

Some retail communications must be filed with FINRA. The following chart outlines those requirements and the corresponding rule cite.

- Filings must be accompanied by FINRA's Advertising and Sales Literature Filing Cover Sheet.
- Filings should identify the reference number of any communication previously submitted by CIM Securities and already reviewed by FINRA that is similar to the current filing.
- All retail communications to be submitted to FINRA must be approved by the designated supervisor prior to submission to FINRA.
- The actual or expected date of first use or publication and the name and CRD number of the approving supervisor must be included with the FINRA filing. [FINRA Rule 2210(c)(5)]

It is not necessary to file any retail communication which has previously been filed and is used without any changes. FINRA rules should be consulted for specific requirements and some exclusions [Rule 2210(c)(7)] from the requirements.

Retail Communication Content Requiring Filing	When	FINRA Rule
New member firms only: certain broadly disseminated retail communications such as generally accessible websites, print media communications, and TV and radio commercials. Free writing prospectuses are also included other than those exempt from filing with the SEC. The rule also excludes research reports concerning only securities listed on a national securities exchange [other than those that must be filed under Section 24(b) of the Investment Company Act of 1940]	One-year requirement to file at least 10 business days prior to use starting on the date the firm's membership with FINRA becomes effective, per the CRD. Free writing prospectuses may be filed within 10 business days of first use.	2210(c)(1)(A)
Investment company communications that promote a specific registered investment company or family of registered investment companies. (Generic investment company communications are not required to be filed.)	Within 10 business days of first use or publication	2210(c)(30)(A)
Investment company using performance rankings or comparisons	10 business days prior to first use or publication	2210(c)(2)(A) 2212 2214
Security futures (with certain exceptions)	10 business days prior to first use or publication	2210(c)(2)(B) 2215

Bond mutual funds that include volatility ratings	10 business days prior to first use or publication	2210(c)(2)(A) 2213
Options communications used prior to the delivery of the Options Disclosure Document	10 calendar days prior to first use or publication	2220(c)
Public direct participation programs	Within 10 business days of first use or publication	2210(c)(3)(B)
Templates for written reports produced by or concerning an investment analysis tool <i>(Retail communications based on templates previously filed with FINRA where the only changes are to update statistical or other non-narrative information do not require re-filing. Also updated non-predictive narrative descriptions of market events during the period covered by the communication and factual descriptions of portfolio changes without having to re-file the template as well as updated information from a registered investment company's regulatory documents filed with the SEC. Filing exclusion includes updates supplied by third-party data providers if its information is from SEC filings; CIM Securities should obtain assurances from the data provider regarding the quality of the data and consistency with SEC source data.)</i>	No filing requirement; must provide access to investment analysis tools upon request	2214
Registered CMOs	Within 10 business days of first use or publication	2210(c)(3)(C) 2216
Registered securities that are derived from or based on a single security, a basket of securities, an index, a commodity, a debt issuance or a foreign currency	Within 10 business days of first use or publication	2210(c)(3)(D)
Television or video where CIM Securities has filed with FINRA a draft version of a "story board"	Within 10 business days of first use or broadcast	2210(c)(4)
Certain 529 Plans communications offering registered investment company products	Within 10 business days of first use or publication	2210(c)(2)(A)
Certain broker-prepared widely disseminated free-writing prospectuses that are required to be filed with the SEC under Securities Act 433(d)(1)(ii) [Excludes those exempt from filing with the SEC]	Within 10 business days of first use or publication	Regulatory Notice 10-52

5.4 Institutional Communications

[FINRA Rule 2210(b)(3)]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor; CCO – File with FINRA as required
Resources	<ul style="list-style-type: none"> • Communications sent to institutions
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Communications limited to institutions reviewed after sending: <ul style="list-style-type: none"> ◦ Review all; or ◦ Review on a sampling basis (see the section <i>Risk-Based Reviews</i> that follows) • Limit distribution to only institutions by: <ul style="list-style-type: none"> ◦ Advising the receiving institution that the material is for institutions only ◦ Adding a legend to material; ◦ Asking the receiving institution to affirm materials will be distributed to institutional investors only; or ◦ Taking other steps to limit distribution • If institutional communications will be distributed to retail customers or CIM Securities becomes aware they are going to retail customers: <ul style="list-style-type: none"> ◦ Subject the communication to reviews required for those sent to retail customers (see <i>Outgoing Communications</i>); or ◦ Cease providing material to the institution • Include institutional communications in training (approval requirements, requirements when institutions forward communications to retail customers, acceptable content, other subjects)
Record	<ul style="list-style-type: none"> • Institutional communications reviewed including record of who reviewed and date reviewed • Institutional affirmations limiting distribution • Action taken if an institution distributes institutional-only communications to retail investors • Training including subjects covered, who attended, date conducted

Institutional communications (including electronic communications) are subject to review and retention by CIM Securities. Communications sent only to institutions do not require approval prior to sending. Those sent to institutions that also will be sent to retail customers (whether by CIM Securities or forwarded by the institution) require approval described in *Outgoing Communications*, including prior approval for any communication provided to more than 25 retail investors in a 30-day period. Institutions may be asked to provide written affirmation that communications sent to them will NOT be provided to retail customers.

Institutional communications are subject to the general standards that appear below.

5.5 General Standards

[FINRA Rule 2210(d)(1)]

Communications must meet general standards which are summarized below. The rules should be consulted for details.

- Communications must be based on principles of fair dealing and good faith, must be fair and balanced, and must provide a sound basis for evaluating the facts and must not omit any material fact where its omission would make the communication misleading.
- Communications may not contain false or misleading statements or any statement CIM Securities knows to be untrue.
- Information may be placed in a legend or footnote only in the event that such placement would not inhibit an investor's understanding of the communication.
- Statements must be clear and not misleading within the context in which they are made and must provide balanced treatment of risks and potential benefits. Communications must be consistent with the risks of fluctuating prices and the uncertainty of dividends, rates of return and yield inherent to investments.
- The nature of the audience to which the communication will be directed must be considered providing appropriate details and explanations appropriate to the audience.
- Communications may not predict or project performance, imply that past performance will recur or make any exaggerated or unwarranted claim, opinion or forecast; provided. Exceptions include hypothetical illustrations of mathematical principals, investment analysis tools, or research reports subject to certain conditions.

5.5.1 Comparisons

Any comparison in retail communications between investments or services must disclose all material differences between them, including (as applicable) investment objectives, costs and expenses, liquidity, safety, guarantees or insurance, fluctuation of principal or return, and tax features.

5.5.2 Disclosure Of The Firm's Name

All retail communications (other than "blind" advertisements used to recruit personnel) and correspondence must:

- prominently disclose the name of the Firm, or the name under which business primarily is conducted (per CIM Securities's Form BD), and may also include a fictional name by which CIM Securities is commonly recognized or which is required by any state or jurisdiction;
- reflect any relationship between CIM Securities and any non-member or individual who is also named; and
- if it includes other names, reflect which products or services are being offered by CIM Securities.

5.5.3 Use Of Non-Member Or OBA Names (DBAs)

RRs may not use names of firms that are not FINRA members or that use DBAs ("doing business as") on customer communications except under the following requirements:

- Clear and prominent identification of CIM Securities as the entity through which securities are offered (including on websites, social media posts, seminars or emails that promote or discuss CIM Securities's securities business)
- Prior approval from Compliance
- Inclusion of a clear explanation of the identity of the other firm and its relationship with CIM Securities
- Communications are subject to review including content and disclosures
- Use only Firm-approved standardized templates which include approved content and disclosures (if available)
- Notify Compliance of any changes to approved communications

5.5.4 Tax Considerations

- References to tax-free income must indicate which income taxes apply, or which do not.
- Communications must not characterize income or investment return as tax-free or exempt when liability is merely postponed.
- A comparative illustration of the mathematical principles of tax-deferred versus taxable compounding must meet seven specified criteria.

5.5.5 Disclosure Of Fees, Expenses And Standardized Performance

[FINRA Regulatory Notice 13-23]

Communications about fees must be accurate and balanced. Representing that fees are not charged in connection with retail accounts and IRAs is inaccurate and a violation of rules when the account is subject to other charges or fees. Investment products have their own associated costs including commissions, management fees, and other product-level expenses. For example, stating that there are no fees charged or highlighting "no fees" and then providing separate, less-prominent disclosure of other fees is misleading. Footnotes do not meet the requirements for disclosure.

Claims regarding fees must be accompanied by clear disclosure of the types of fees that may be charged. A statement that "other account fees, fund expenses, brokerage commissions and service fees may apply" would be consistent with rule requirements. This statement could be hyperlinked to CIM Securities's web site where fees are explained.

Communications that present certain permitted investment company performance data must disclose performance information required by SEC Rule 482 and Investment Company Act Rule 34b-1, among other things. This information must be set forth prominently, and in any print advertisement, in a prominent text box that contains only the required information.

5.5.6 Recommendations

- If a communication includes a recommendation of securities, it must comply with Regulation Best Interest [see the chapter *REGULATION BEST INTEREST (BI)*], have a reasonable basis and disclose:
 - whether CIM Securities is making a market in the recommended security (or in the underlying security if the recommended security is an option or security future) or the security will be bought or sold on a principal basis;
 - if CIM Securities or any associated person directly and materially involved in the preparation of the content of the communication has a financial interest in the securities of the issuer; and
 - if CIM Securities was a manager or co-manager of a public offering of any securities of an issuer whose securities were recommended within the past 12 months.
- CIM Securities must provide, or offer to furnish upon request, available investment information supporting the recommendation (including, for corporate equity securities, the price at the time the recommendation is made).
- Generally, a communication may not refer to past specific recommendations of CIM Securities that were or would have been profitable; however, it may set out or offer to furnish a list of all recommendations as to the same type of securities made by CIM Securities within the past year if the communication meets certain conditions, including the condition that the communication contain a specified, prominently displayed cautionary legend.
- These requirements do not apply to any communications that meet the definition of "research report" and include required research disclosures.

- The general disclosure requirements for recommendations do not apply to any communication that recommends only registered investment companies or variable insurance products, if such communications have a reasonable basis for the recommendation.

5.5.7 Prospectuses Filed With The SEC

Prospectuses, preliminary prospectuses, fund profiles and similar documents that have been filed with the SEC are not subject to the content standards except for investment company prospectuses published pursuant to Rule 482 and broadly disseminated free writing prospectuses that are filed with the SEC pursuant to Securities Act Rule 433(d)(1)(ii).

5.5.8 Limitations On Use Of FINRA's Name And Any Other Corporate Name Owned By FINRA

[FINRA Rule 2210(e); FINRA email address for questions: trademarks@finra.org]

CIM Securities may indicate its FINRA membership in only three ways:

- In a communication that complies with the standards of FINRA Rule 2210 and neither states nor implies that FINRA or any other corporate name or facility owned by FINRA, or any other regulatory organization, endorses, indemnifies or guarantees CIM Securities's business practices, selling methods, the class or type of securities offered, or any specific security; references are limited to "Reviewed by FINRA" or "FINRA reviewed;"
- In a confirmation statement for an OTC transaction that includes a specified legend; or
- On CIM Securities's website (or any related firm website about securities business), as long as CIM Securities provides a hyperlink to the homepage of FINRA's website in close proximity to CIM Securities's indication of FINRA membership.

Member firms are prohibited from including FINRA's logo on web sites, business cards, stationery, or other marketing materials. The FINRA trademark or references to membership may not be included in any trademark of CIM Securities or associated person. CIM Securities may, however, include "FINRA Member Firm" or "Member of FINRA" on such materials.

5.6 Approval

[FINRA Rule 2210(b)]

Supervisory review and approval requirements are outlined in the following chart.

Type	Approval Required
Retail communications	<p>Must be approved by the designated supervisor before the earlier of its first use or filing with FINRA.</p> <p>Prior approval is not required for the following retail communications:</p> <ul style="list-style-type: none"> • Another FINRA member already filed it and received approval and the Firm does not materially alter it or use it inconsistent with FINRA's approval • Retail communications supervised as correspondence where: it is excepted from the definition of "research report" unless it makes any financial or investment recommendation; it is posted on an online interactive electronic forum; and it does not make any financial or investment recommendation or otherwise promote a product or service of the member.
Institutional communications	<ul style="list-style-type: none"> • Reviewed after sending
Correspondence	<ul style="list-style-type: none"> • Reviewed after sending
Seminar materials	Compliance prior approval
Advertising	Compliance prior approval
Pre-approved form letters, group e-mails, hedge clauses, other pre-approved communications	Require no additional approval if used without change

5.7 SIPC Membership

[Securities Investor Protection Act of 1970; United States Code Title 15 Chapter 2B-1; SIPC web site at www.sipc.org/how/sipclogo.aspx]

Advertising must include a notation that CIM Securities is a member of SIPC, e.g., "Member, SIPC." If an explanatory statement will be included in advertising explaining what SIPC is, one of the following two standardized phrases must be included:

- Member of SIPC, which protects securities customers of its members up to \$500,000 (including \$250,000 for claims for cash). Explanatory brochure available upon request or at <http://www.sipc.org>.

- Member of SIPC. Securities in your account protected up to \$500,000. For details, please see <http://www.sipc.org>.

The words "Member, SIPC" may be omitted if the official explanatory statement is used in conjunction with the official SIPC symbol.

When SIPC is referenced in CIM Securities's web site, the site will include a hyperlink to the SIPC web site.

"Advertising" is defined under SIPC rules as any promotional material used in or on any newspaper, magazine, or other periodical, radio, television, telephone or tape recording, videotape display, motion picture, slide presentation, telephone directory, sign or billboard, electronic or other public media.

5.8 Recordkeeping Requirements For Retail And Institutional Communications

[FINRA Rule 2210(b)(4)(A); SEC Securities Exchange Act of 1934 Rule 17a-4]

Records of retail and institutional communications must include:

- Originals of all communications received and copies of all communications sent
- While not "retail" or "institutional" communications, records of inter-office memoranda and communications relating to CIM Securities's business [SEC Rule 17a-4(b)(4)]
- The dates of first use and (if applicable) last use
- The name of the registered principal who approved the communication and the date of approval
- For communications not approved by a supervisor prior to first use, the name of the person who prepared or distributed the communication (where clerical staff prepares or distributes the communication, include the name of the person on whose behalf the communication was prepared or distributed)
- The source of statistical tables, charts, graphs and other illustrations
- For a retail communication prepared by another firm and submitted to FINRA, the name of the firm and a copy of FINRA's review letter
- A record that the item was filed with FINRA and when filed (if required)
- Changes recommended by FINRA and approval received from FINRA (if required)

5.9 Outgoing Communications

[FINRA Rule 3110(b)(4), 3110.07, 3110.08 and 3110.09]

This section outlines requirements for outgoing communications which includes written and electronic communications. Electronic communications are subject to specific procedures for review; see the section *Electronic Mail* in this chapter and the section *Electronic Communications Policy* in the chapter *GENERAL EMPLOYEE POLICIES*.

5.9.1 Sending Communications From Personal Computers And Other Non-Firm Facilities

Outgoing public communications must be sent or transmitted only through Firm-sponsored facilities or systems. Written and electronic communications must be sent through channels that permit review by the supervisor (CIM email address). Communications may only be sent through an RR's personal computer using CIM email address or if in the case of use of social media sites, communications must be captured by the Firm and reviewed by a principal..

5.9.2 Review And Approval

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • Outgoing customer communications
Frequency	<ul style="list-style-type: none"> • Daily
Action	<ul style="list-style-type: none"> • Review communications for appropriateness of language • Pre-approve retail communications that are sent to more than 25 persons in a 30-day period (other than those excluded; see <i>Retail Communications</i> under <i>Definitions</i> in this chapter) • Review other communications after sending • Identify outgoing communications that may constitute "research" under FINRA Rule 2241(a)(11) • Take corrective action, if necessary, which may include consultation with the RR and/or Compliance, sending corrected communications, added training for the RR, restrictions on communications, or other action considered appropriate for the circumstance
Record	<ul style="list-style-type: none"> • Communications including reviewer's initials or other record of review and action taken, if appropriate

Outgoing customer communications are subject to review and approval by the designated supervisor.

- Retail communications sent to more than 25 persons in a 30-day period require the supervisor's approval **before** sending.
- Other communications will be reviewed and approved after sending.
- Some communications (depending on type and other factors) require prior approval (see the section *Approvals*).

Pre-approved form letters and group e-mails **used without change** (other than customer name, address) may be sent to customers or prospective customers without additional approval. Records of to whom form letters and group e-mails are sent must be retained in CIM Securities's records.

5.9.2.1 Risk-Based Reviews

[FINRA Rule 3110.06]

Responsibility	<ul style="list-style-type: none"> • Compliance: Establish risk-based reviews • Designated supervisors: conduct risk-based reviews as required.
Resources	<ul style="list-style-type: none"> • Evaluation of CIM Securities's size, types of business, supervisory structure
Frequency	<ul style="list-style-type: none"> • At inception of risk-based procedures and ongoing
Action	<ul style="list-style-type: none"> • Compliance:

	<ul style="list-style-type: none"> ○ Determine scope of risk-based review (size, what is subject to review, who is subject to review) ○ Develop procedures and update as necessary ○ Provide procedures and education/training to communications reviewers ○ Include communications requirements in RR training ○ Include risk-based procedures in periodic reviews of branches, offices, and supervisory system, controls and procedures ○ Identify RRs with complaint/disciplinary history necessitating review of ALL communications and notify the RR's supervisor ("heightened supervision") • Designated supervisors: <ul style="list-style-type: none"> ○ Review communications for compliance with policies and securities rules/laws ○ Take corrective action, if necessary, including consulting with RR and/or Compliance, contacting the customer, issuing corrections, etc.
Record	<ul style="list-style-type: none"> • Procedures for risk-based reviews are included in the manual • Updates to procedures are retained by Compliance • Education and training are documented including how conducted, who attended, and dates of education/training including educational memoranda • Designated supervisors: records of reviews and action taken, if any

Supervisors may review written outgoing communications on a risk-based basis using the guidelines that follow, or, if risk-based review is not adopted, review all outgoing communications.

Risk-based guidelines include the following. "Pre-review" refers to review and approval of written communications **before** it is sent. Communications subject to "post-review" may be reviewed after sending. All RRs are subject to review of at least some of their communications on a regular basis. Risk-based review is permitted for the following type(s) of outgoing communications:

- E-mails
- Post-review:
 - At least 5% of other communications
- Refer to the section *Content Guidelines* that follows for guidance on acceptable content
- For communications that includes a recommendation, determine that the information presented balances the benefits and risks of the recommendation and, if the subject security is high-risk, determine the recommendation is appropriate for the customer by conferring with the RR and/or reviewing new account information
- If there are problems with an RR's communications that is being minimally sampled, increase the reviews and note the change in the RR's file, on a Daytimer, or on a supervisory log.

5.9.3 Content Guidelines

Items to consider when preparing and reviewing outgoing communications (and other forms of written or electronic communications) include:

- Truthfulness and good taste are required.

- Exaggerated, unwarranted, or misleading statements or claims are prohibited.
- Promises or guarantees: past performance may not be used to promise, guarantee, or imply future profits or income from securities.
- Projections and predictions are not permitted.
- Comparisons of personnel, facilities, or charges with those of other broker-dealers should not be made unless supported by the facts, and other firms' names should not be included.
- Communications regarding securities subject to pending distributions (underwritings) are generally not permitted.
- Communications regarding securities sold by prospectus (mutual funds, limited partnerships, *etc.*) must be approved by Compliance prior to sending (except for pre-approved communications where no changes are made).
- Only firm-approved hedge clauses may be used.
- Tax advice must not be provided; the customer should be referred to his or her tax adviser for such issues.
- Photocopying and distributing copyrighted material may violate copyright laws.
- Profit and loss or other portfolio analyses should include a disclaimer that the customer should rely on customer statements provided by CIM Securities and any analysis or calculation is provided for information purposes only.
- The use of firm letterhead should be restricted to firm-related matters.
- Communications regarding options is subject to specific requirements which are discussed in the chapter *OPTIONS*.

5.9.4 Letters And Notes

Copies of letters, notes, and similar communications must be provided to the designated supervisor on the day sent.

5.9.5 Research (Not applicable at Present)

Research published by CIM Securities must be distributed in accordance with the requirements and limitations communicated by Research or another issuing department/personnel. Failure to comply may subject CIM Securities and the RR to regulatory actions for violating rule requirements. For example:

- If CIM Securities issues debt research, some may be restricted to institutional customers only. Institutional investors are required to affirm they meet the definition of an institution and are able to meet certain conditions regarding their investment sophistication. Such research may NOT be provided to retail customers.
- Some research may qualify for distribution only to certain jurisdictions (states) where the subject securities are qualified for sale.

Questions regarding distribution of research should be referred to the appropriate research personnel or to Compliance.

5.9.6 Other Communications Defined As "Research"

[SEC Regulation AC; FINRA Rule 2241(a)(11)]

R Rs are **not** permitted to send communications that may be deemed "research" since there are complex requirements that apply to the issuance of research reports. Federal and SRO rule interpretations define "research" as any written communications (including electronic) that includes an analysis of equity securities of individual companies or industries (other than an open-end registered investment company that is not listed or

traded on an exchange), and that provides information reasonably sufficient upon which to make an investment decision and that is distributed to at least 15 persons. This applies even if the author does not hold the title of "research analyst" and does not work in a research department.

There are specific exceptions under SRO rules. Questions regarding whether a communication constitutes "research" should be referred to Compliance.

5.10 Incoming Correspondence

[FINRA Rule 3110(b)(4), 3110.07, 3110.08 and 3110.09]

In this section, "correspondence" means written and electronic communications received by CIM Securities.

5.10.1 Review Of Incoming Correspondence

Responsibility	<ul style="list-style-type: none">• IB Supervisor
Resources	<ul style="list-style-type: none">• Incoming correspondence, including correspondence marked "personal and confidential"
Frequency	<ul style="list-style-type: none">• Daily
Action	<ul style="list-style-type: none">• Review all incoming correspondence• Refer customer securities and checks directly to Operations• Refer customer complaints to Compliance• Refer audit letters to Operations
Record	<ul style="list-style-type: none">• Initial each piece of correspondence and maintain in branch/department incoming customer correspondence files.

All incoming written correspondence will be opened and reviewed by the designated supervisor or someone qualified and appointed by the department supervisor. This review includes letters, facsimiles, courier deliveries, and other forms of written communication. Electronic mail is subject to specific procedures for review; see the section *Electronic Mail* in this chapter and the section *Electronic Communications Policy* in the chapter *GENERAL EMPLOYEE POLICIES*.

The following guidelines for review apply:

- Correspondence identified as "Confidential" will be opened and reviewed.
- Obvious non-customer correspondence (bank statements, advertising, etc.) will not be opened and will be forwarded directly to the addressee.
- Audit letters (requests from customers' auditors for verification of account positions) will be forwarded directly to Operations for response.
- Complaints will be immediately forwarded to the RR's supervisor and to Compliance.

- Checks or securities will be immediately deposited with the appropriate operations personnel and the RR notified of receipt.
- Original customer correspondence will be retained for CIM Securities's files; the addressee will receive a copy.
- Original customer correspondence will be forwarded to the designated supervisor for review, initialing, and filing.

5.10.2 Offices Without Resident Supervisors

Responsibility	<ul style="list-style-type: none"> • Designated Supervisor
Resources	<ul style="list-style-type: none"> • Incoming customer correspondence
Frequency	<ul style="list-style-type: none"> • Daily
Action	<ul style="list-style-type: none"> • Supervisors: review incoming correspondence in accordance with CIM Securities's policy • Compliance: conduct branch reviews to verify procedures are being followed
Record	<ul style="list-style-type: none"> • Incoming correspondence retained by designated supervisor in accordance with CIM Securities's policy on incoming correspondence • Compliance retains records of branch reviews

For offices without a resident registered supervisor, copies of all incoming, written correspondence related to CIM Securities's securities business must be forwarded to the designated supervisor at the end of each week for review.

Compliance with this requirement will be audited during branch reviews.

5.10.3 Personal Mail

Employees should direct all personal mail to their home address. Personal mail is subject to incoming correspondence and electronic mail review policies.

5.10.4 Inter-Office Communications

[SEC Securities Exchange Act of 1934 Rule 17a-4(b)(4)]

You should presume that any inter-office communications may be subject to regulatory review, and therefore must comply with good business practice as well as CIM Securities's policies on communications and securities rules/laws. Inter-office memos and other communications are subject to review and retention requirements.

5.10.5 Internal Use Only

Printed or electronic information marked "internal use only" may not be sent or otherwise provided to individuals outside CIM Securities.

5.10.6 Squawk Box, Conference Calls, And Other Internal Communication Systems

If applicable, access to squawk box technology (phone squawk box, intranet system, *etc.*) or other internal systems that communicate confidential information about customer orders is limited to employees who have a bona fide reason for knowing, such as facilitating finding the contra-side of a broadcast customer order. Confidential information communicated to employees in such venues may not be shared with outsiders. For example, sharing information (either by allowing an outsider to listen to or participate in or by giving the information to an outsider) about proprietary trading, block orders, or other information intended for internal use only, could give an outsider an unfair advantage to act on the information and is prohibited.

Employees must request approval from their designated supervisors to obtain access to such internal systems and, if approved, sign a certification that they agree to abide by confidentiality requirements.

5.11 Complaints

[FINRA Rule 3110(b)(5), 4513 and 4530]

Responsibility	<ul style="list-style-type: none">• CCO
Resources	<ul style="list-style-type: none">• Customer communications• Customers' complaints (written or electronic)• FINRA reports (Report Center, Risk Monitoring Reports):<ul style="list-style-type: none">○ FINRA Sales Practice Complaint Report○ FINRA Customer Complaint Report
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Branch/Department Supervisor:<ul style="list-style-type: none">○ Identify potential complaints when reviewing customer communications○ Resolve complaints of an operational nature such as late dividends, delayed delivery of stock, <i>etc.</i> If written, forward a copy to Compliance with description of resolution○ Refer all other complaints (mishandling of account by RR, improper transactions, churning, <i>etc.</i>) to Compliance• Compliance:<ul style="list-style-type: none">○ Send initial acknowledgment of receipt of complaint○ Gather needed information and investigate the complaint○ Provide a response and resolution to the customer with a copy to the RR and RR's supervisor○ If necessary, amend the RR's U4 (or, in the case of a terminated RR, amend Form U5)○ File quarterly electronic complaint report with FINRA○ Maintain central record of complaints

	<ul style="list-style-type: none"> ○ For formal civil actions (lawsuits, arbitrations), refer the matter to CIM Securities's counsel for response ○ Review FINRA reports for trends in complaints ○ Include complaints in training
Record	<ul style="list-style-type: none"> • Copies of written complaints and related correspondence (including acknowledgment of receipt of complaint and resolution) are retained in: <ul style="list-style-type: none"> ○ Branch file for complaints (unless CIM Securities makes complaints promptly available to FINRA upon request at the office location) ○ Compliance central file of CIM Securities's complaints (retention for 4 years) • <i>Note:</i> options complaints are retained in separate files both by branches (where records are maintained at branches) and by Compliance • Central complaint log (MSRB requires electronic format under Rule G-8) • Record of electronic filings • Records of updates to Form U4 or U5 • Reviewed FINRA reports • FINRA record retention: 4 years (Rule 4513) • MSRB record retention: 6 years with 2 years in a readily-accessible location (MSRB Rule G-8) • Records of training

5.11.1 Complaint Defined

"Complaint" is defined as any grievance by a customer or any person authorized to act on behalf of the customer involving the activities of CIM Securities or someone associated with CIM Securities in connection with the solicitation or execution of any transaction or the disposition of securities or funds of that customer.

5.11.2 Handling Of Customer Complaints

When a written complaint is received, a copy should be forwarded immediately to Compliance for follow-up.

Oral complaints may be resolved by the designated supervisor if the nature of the complaint is operational such as late check, late dividend, or another type of nominal problem. Oral complaints alleging mishandling of the customer's account (unauthorized trading, improper investments, *etc.*) should be brought to the attention of Compliance for review and resolution.

5.11.3 Oral Complaints

Oral complaints should be reported immediately to the designated supervisor for sales practice issues, or to Operations for operational issues. Examples of sales practice issues include complaints regarding losses, improper trades, and other complaints involving the quality of investments or wrongdoing by the RR or CIM Securities. Examples of operational issues include late dividend checks, errors on monthly statements, *etc.* RRs should not make independent decisions regarding whether to report complaints; all oral complaints should be reported either to the designated supervisor or Operations.

5.11.4 Complaints Received By Clearing Firm (Not applicable at Present)

As required under SRO rules, whenever CIM Securities's clearing firm receives a customer complaint, the clearing firm will:

- Provide a copy of the complaint to CIM Securities's compliance officer.
- Provide a copy to CIM Securities's designated examining authority (DEA).
- Notify the customer directly that their complaint has been forwarded to CIM Securities for response and to the DEA.

When received by CIM Securities, the complaint will be handled in the same manner as other complaints received directly by CIM Securities.

5.11.5 Records Of Complaints

Compliance will maintain a central record of all customer complaints including the following MSRB rules require an electronic log.

- Complainant's name and address
- Account number or municipal advisory number or code, if any
- Date the complaint was received
- Name(s) of employee(s) identified in the complaint
- Description of the nature of the complaint including the date(s) of activity that resulted in the complaint
- Disposition of the complaint

5.11.5.1 Office Records Of Complaints

Each office of supervisory jurisdiction (OSJ) will maintain a separate file of all written customer complaints that relate to that office (including complaints that relate to activities supervised from that office) and action taken by CIM Securities, if any, or a separate record of complaints and a clear reference to the office files that contain correspondence regarding complaints. Alternatively, CIM Securities may make complaints promptly available at that office, upon request of FINRA.

5.11.6 Notice To Customers

Each customer is provided with notification of the address and telephone number of the department to which complaints may be directed. The FINOP is responsible for establishing procedures to provide this information to customers.

5.11.7 Reporting Of Customer Complaints

[FINRA Rule 4530]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • Complaints received from customers or referred by RRs, supervisors, or others • FINRA Disclosure Timeliness Report Card
Frequency	<ul style="list-style-type: none"> • Statistical Complaint Report: Quarterly • Form BD, U4s, and U5s (if applicable): Promptly after receipt of complaint
Action	<ul style="list-style-type: none"> • Identify reportable complaints and other reportable events • Report to FINRA the events specified in FINRA Rule 4530 within 30 calendar days of knowledge of the event • File electronically the quarterly statistical report by the 15th of the month following the calendar quarter
Record	<ul style="list-style-type: none"> • Quarterly complaint reports are maintained in a file for the reports • Copies of events reported

CIM Securities will file a quarterly statistical report of complaints with FINRA. Complaints reportable in CIM Securities's Form BD and/or an RR's Form U4 (or an amendment to Form U5, if the RR is terminated) will be promptly forwarded to FINRA.

5.12 Customer Privacy Policies And Procedures

[Gramm-Leach-Bliley Act Sections 501-503; SEC Regulation S-AM and S-P; Evolution of a Prototype Financial Privacy Notice: <http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf>; FINRA web site Customer Information Protection: <http://www.finra.org/industry/customer-information-protection>; Fair Credit Reporting Act; SEC Risk Alert on Regulation S-P: <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf>]

5.12.1 Introduction

CIM Securities has adopted a Privacy Policy which is provided to customers at the time a new account is opened. The Privacy Policy explains CIM Securities's policies regarding safeguarding of customer information and records and whether CIM Securities shares information with outside parties. CIM Securities also publishes its Privacy Policy on its web site. Customers will receive notice of revisions to the Privacy Policy when they occur.

SEC Regulation S-P ("Privacy Of Consumer Financial Information") applies only to accounts for individuals (*i.e.*, institutional accounts are not affected) and differentiates between "customers," where CIM Securities has an established relationship with the individual, and "consumers," where there is no pre-established relationship. For purposes of this section, any individual from whom information is obtained (and their legal representative acting on their behalf) to open an account or to obtain services or products from CIM Securities is considered a "customer." The term "consumer" will be considered synonymous with "customer" for purposes of this section.

The Privacy Policy applies to all individual customers of CIM Securities, whether U.S. residents or foreign residents.

5.12.2 "Public" vs. "Nonpublic" Personal Information About Customers

Generally, information provided to CIM Securities by a customer or potential customer in the normal course of CIM Securities offering a product or service is considered "nonpublic personal information." Identifying whether information is "public" or "nonpublic" is important as to CIM Securities's obligations if CIM Securities shares information with nonaffiliated third parties. Public information is information that CIM Securities reasonably believes may be obtained from three sources:

- federal state or local government records;
- widely distributed media; or,
- disclosures to the general public that are required to be made by federal, state, or local law.

Nonpublic personal information also includes any list, description, or other grouping of customers (and publicly available information about them) that is derived from financial information that is not publicly available.

5.12.3 Sharing Nonpublic Financial Information

In the normal course of business, CIM Securities may share customer nonpublic financial information with service providers such as clearing firms or service bureaus. Agreements with such third parties include assurances regarding the protection of customer records and information. Information sharing with affiliated companies may also occur, and if applicable, is disclosed in CIM Securities's Privacy Policy.

CIM Securities does not share customer nonpublic financial information with non-affiliated companies or non-exempt service providers.

5.12.4 Customer Notification

[12 CFR Federal Reserve System Regulation P; Federal Reserve Privacy of Consumer Financial Information (Regulation P): <http://www.federalreserve.gov/boarddocs/supmanual/cch/consumer.pdf>; Gramm-Leach-Bliley Act Title V Section 503]

CIM Securities will provide notice to customers about CIM Securities's Privacy Policy. The notice is provided as follows:

- At the time an account is opened.
- On CIM Securities's web site.
- Annually, unless CIM Securities meets the following two conditions:
 - CIM Securities does not disclose nonpublic information to third parties (*e.g.*, sharing in connection with marketing activities vs. sharing solely to service customer accounts), other than disclosure permitted under exemptions available under the Gramm-Leach-Bliley Act; and
 - There has been no change in policies regarding disclosing nonpublic personal information from the last notice sent to customers

5.12.5 Affiliate Marketing

[SEC Regulation S-AM; SEC Small Entity Compliance Guide regarding Regulation S-AM: <http://www.sec.gov/divisions/marketreg/tmcompliance/34-60423-secg.htm>; Fair Credit Reporting Act Section 624]

Regulation S-AM limits use of certain information received from CIM Securities's affiliates to solicit a consumer for marketing purposes. Consumers may block the use of certain financial information by affiliates of the person the consumer does business with. CIM Securities may use "eligibility information" (*i.e.*, certain financial information such as information regarding the consumer's transactions or experience with the affiliate) if:

- the potential market use of the information has been clearly, conspicuously, and concisely disclosed to the consumer;
- the consumer has been provided with reasonable opportunity to opt out; and
- the consumer has not opted out.

CIM Securities will only use information from affiliates if the above requirements are satisfied. Opt-out notices under Regulation S-AM may be included with Regulation S-P opt-out notices described above.

5.12.6 Introduction

CIM Securities and its employees are subject to restrictions that govern telephone solicitations as well as unsolicited facsimile advertisements to residences.

Key points include the following:

- Telephone and facsimile solicitations are allowed when the target individual has an "established business relationship" with CIM Securities.
- Calls may not be made to individuals included on a Do Not Call List which includes lists maintained by the federal government, state governments, and CIM Securities.
- "Telephone solicitation" is defined as a telephone call initiated for the purposes of encouraging the purchase of or investment in property, goods, or services. The definition exempts calls made by tax-exempt nonprofit organizations.
- "Established business relationship" includes someone who has had a transaction or security position, money balance, or account activity within 18 months preceding the call or fax or has contacted CIM Securities to inquire about a product or service within 3 months preceding the call or fax. CIM Securities has the burden to prove an established business relationship exists.
- Calls to businesses are exempt from telemarketing restrictions; however, solicitations may not be made to induce sales or contributions by individuals employed by a business.

5.12.7 Telephone Calls

General requirements include the following:

- The caller must provide the called party, at the beginning or in the introductory portion of the script, the name of the caller; the name of the person or entity on whose behalf the call is being made; a telephone number or address at which the caller may be contacted; and disclosure that the purpose of the call is to solicit the purchase of securities or related services.
- Telephone solicitations to residences may not be made before 8:00 a.m. or after 9:00 p.m. in the time zone of the called party's location.
- A "Do Not Call" list must be established that includes the names of individuals who have specifically requested they not be called for solicitations.
- Prerecorded calls to residences are prohibited unless the person has consented in writing to receive such calls and can opt out of future calls and CIM Securities complies with the requirements of FINRA Rule 3230(k).
- The telephone number of the sender may not be a 900 number or other number where the called party will incur a charge for notifying the sender of a desire not to be called. Consumers may not be charged to protect their privacy.
- Caller identification information must be transmitted; blocking caller identification information is prohibited.
- Outbound telemarketing calls may not be "abandoned" which means a person answers the call and the call is not connected to someone at CIM Securities within two seconds of the completed greeting. CIM Securities employs technology to avoid abandoned calls as included in FINRA Rule 3230(j).

The restrictions do not apply to calls to customers for whom CIM Securities carries accounts and where the account has had some activity in the last 18 months (trading, credit of interest earned, *etc.*). Calls to other broker-dealers also are not covered by these restrictions.

5.12.8 Wireless Communications

The rule also applies to outbound telephone calls to wireless telephone numbers.

5.12.9 Outsourcing Telemarketing

Compliance must review the use of third party telemarketers before they are engaged. CIM Securities is responsible for compliance with telemarketing requirements even if the function is outsourced to a third party. Outsource firms may require registration or licensing to conduct telemarketing for CIM Securities.

5.12.10 Unencrypted Consumer Account Numbers

CIM Securities and its associated persons are prohibited from disclosing or receiving, for consideration, unencrypted consumer account numbers for use in telemarketing. "Unencrypted" is defined as not only complete, visible account numbers, whether provided in lists or singly, but also encrypted information with a key to its decryption.

5.12.11 Submission Of Billing Information

For any telemarketing transaction, CIM Securities or its associated person must obtain the express informed consent of the person to be charged and to be charged using the identified account. If the telemarketing transaction involves pre-acquired account information and a free-to-pay conversion feature, CIM Securities or its associated person must: (1) obtain from the customer, at a minimum, the last four digits of the account number to be charged; (2) obtain from the customer an express agreement to be charged and to be charged using the identified account number; and (3) make and maintain an audio recording of the entire telemarketing transaction. For any other telemarketing transaction involving pre-acquired account information, CIM Securities or its associated person must: (1) identify the account to be charged with sufficient specificity for the customer to understand what account will be charged; and (2) obtain from the customer an express agreement to be charged and to be charged using the identified account number.

5.12.12 Abandoned Calls

CIM Securities and its associated persons are prohibited from abandoning any outbound telemarketing call. The abandoned calls prohibition is subject to a "safe harbor" which provides that a firm or its associated person will not be liable for violating the FINRA rule if:

1. CIM Securities or its associated person employs technology that ensures abandonment of no more than three percent of all calls answered by a person, measured over the duration of a single calling campaign, if less than 30 days, or separately over each successive 30-day period or portion thereof that the campaign continues;

2. CIM Securities or its associated person, for each telemarketing call placed, allows the telephone to ring for at least 15 seconds or four rings before disconnecting an unanswered call;
3. whenever an associated person is not available to speak with the person answering the telemarketing call within two seconds after the person's completed greeting, CIM Securities or its associated person promptly plays a recorded message stating the name and telephone number of CIM Securities or associated person on whose behalf the call was placed; and
4. CIM Securities retains records establishing compliance with the "safe harbor."

5.12.13 Credit Card Laundering

There is a prohibition against credit card laundering, the practice of depositing into the credit card system a sales draft that is not the result of a credit card transaction between the cardholder and CIM Securities. Except as expressly permitted by the applicable credit card system, the rule prohibits a firm or its associated person from:

1. presenting to or depositing into the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and CIM Securities;
2. employing, soliciting, or otherwise causing a merchant, or an employee, representative or agent of the merchant, to present to or to deposit into the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant; or
3. obtaining access to the credit card system through the use of a business relationship or an affiliation with a merchant, when the access is not authorized by the merchant agreement or the applicable credit card system.

5.12.14 Other Prohibited Activities

The following are prohibited when calling customers or prospective customers:

- threats, intimidation, and the use of profane or obscene language
- calling a person repeatedly with intent to annoy, abuse, or harass the called party
- using an alias

5.12.15 Do Not Call Lists

Phone solicitations may not be made to phone numbers that are included in federal, state, or CIM Securities's do not call list. **Because fines may be substantial for each call that violates a restriction, it is important to comply with these requirements.**

It is permissible to contact someone with whom CIM Securities has an "established business relationship" (described below); the person called has given express written permission to call outside the applicable time; or the person called is a broker or dealer.

If someone has asked to be included on CIM Securities's do not call list, that person may not be called regardless of whether they are a current customer or have an established business relationship. Individual states may impose stricter requirements limiting contact with persons on that state's do not call list.

- Lists are available for RRs to reference prior to making solicitation calls.

5.12.16 National Do-Not-Call Registry

The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) established requirements for sellers and telemarketers to participate in a National Do-Not-Call Registry of phone numbers that do not accept phone solicitations. CIM Securities and its employees must avoid solicitation calls to any number on the list unless the person has an "established business relationship" with CIM Securities. The list used must be no older than 31 days prior to the date any call is made.

In general, national do-not-call requirements apply to residential phone numbers. In addition, the FCC includes wireless subscribers in the national registry, presuming these are residential subscribers.

5.12.17 State Restrictions

Certain states have enacted restrictions on telephone solicitations to residences. Florida, for example, has a restrictive policy whereby individuals may ask to be included on a state-wide "do not call" list. It is the telephone solicitor's obligation to be aware of any individuals who are included on that list. Contact Compliance if you have questions regarding state restrictions.

5.12.18 Internal Do Not Call List

Employees are responsible for reporting to Compliance the names of individuals who do not wish to be called. Compliance maintains a Do Not Call List that is periodically distributed to employees with an explanation of CIM Securities's telemarketing policy. It is the RR's responsibility to ensure outgoing calls are not made to anyone appearing on CIM Securities's Do Not Call List.

5.12.19 Facsimile Transmissions

General requirements that apply to faxes include:

- A facsimile transmission must include, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and the identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of the sender.
- Unsolicited faxes may only be sent to individuals who have an established business relationship with CIM Securities.

5.12.20 Established Business Relationship

Calls and faxes to the following are not subject to do-not-call restrictions:

- a person having made a financial transaction or having a security position, a money balance, or account activity with CIM Securities (or its clearing firm if a clearing firm relationship exists) within 18 months immediately preceding a call or fax; or

- CIM Securities is the "broker-dealer of record" (identified on the customer's account application for accounts held directly at a mutual fund or variable insurance product issuer) for the account of the person within the previous 18 months immediately preceding the date of the call or fax; or
- the person has contacted CIM Securities to inquire about a product or service offered by CIM Securities within the previous 3 months immediately preceding the call or fax.

5.13 Public Appearances

[FINRA Rule 2210(f)]

Responsibility	<ul style="list-style-type: none"> • CCO, IB Supervisor
Resources	<ul style="list-style-type: none"> • Requests for public appearances • Outlines of subjects to be included • Charts or other visual aids to be used in conjunction with public speaking • Written materials to be provided to attendees
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Refer requests for contact with media to Compliance • Review outlines of information to be presented and revise, as needed • For product-specific presentations, request review by product manager, if necessary • For mutual fund presentations, materials provided by wholesalers also require the approval of Compliance • Review charts and written materials to be presented • Attend sales seminars periodically to confirm compliance with requirements • Ensure presentations involving securities being offered by prospectus include provision of prospectuses to attendees • Include public appearance requirements in training or provide training prior to appearances
Record	<ul style="list-style-type: none"> • Maintain approved outline, samples of visual aids, and written materials in a "Public Appearances" file • Initial and date all approved materials • Obtain and maintain in the Public Appearances file a list of attendees who received prospectuses (if applicable) • Compliance maintains records of approved wholesaler materials • Records of training including who participated, subjects covered

The following sections outline requirements when RRs engage in public appearances.

5.13.1 General Guidelines

The general concepts of truthfulness, good taste, and a fair presentation apply to employees engaging in public appearances. Public appearances include participation in a seminar, forum (including an interactive electronic forum), radio or television interview, or other public appearance or public speaking activity.

- The general standards explained earlier in this chapter apply to public appearances.
- If a security is recommended in the public appearance, the RR must have a reasonable basis for the recommendation **and** must disclose:
 - If the RR has a financial interest in the securities of the issuer; the nature of the interest (including derivatives such as options, warrants, *etc.*) and any material conflict of interest of the RR or CIM Securities known at the time of the appearance. (*This disclosure does not apply to investment company securities or variable insurance products.*)
- These requirements do not apply to public appearances by research analysts where the appearance complies with the requirements of FINRA Rule 2241(d).

5.13.2 Seminars

RRs should use pre-approved materials and advertisements for sales seminars. Materials and advertising must be submitted to Compliance for approval prior to use if it has not been pre-approved.

5.13.3 Approval

Prior to engaging in public speaking, the RR should prepare an outline and submit a Public Appearance/Seminar/Luncheon Request for approval by the designated supervisor and Compliance at least 3 weeks prior to the event to ensure timely review. The Request should also include a copy of any proposed advertising about the event if using materials that are not pre-approved by CIM Securities.

5.13.4 Radio, TV, And Other Extemporaneous Presentations

The general standards of communications with the public apply to all public appearances whether scripted or not. The following should be considered when participating in radio, TV, or other non-scripted public appearances. Also refer to the chapter *GENERAL EMPLOYEE POLICIES* and the section *Media Contact Is Limited To Certain Authorized Persons* that explains restrictions on dealing with the media. Most employees are restricted from such contact except with the specific approval of Compliance.

- Specific recommendations of securities must be avoided unless approved by Compliance or the speaker is authorized under CIM Securities's "Media Contact" policy. If a recommendation is made, the speaker is required to disclose material information such as when CIM Securities is a market maker in the stock. The current price and any special risks associated with the security also must be disclosed.
- The firm's name must be clearly disclosed in conjunction with any securities or services offered.
- The speaker cannot assume a specific level of audience knowledge, experience or suitability. High risk securities may not be appropriate for discussion in a broadcast format available to any listener.
- Media presentations should be clear and understandable. Avoid overly complex messages and technical terminology which may not be understood by the general audience.
- Include products only where the speaker is licensed to sell the product.

For RRs who are approved to engage in radio, TV, or other extemporaneous public speaking, Compliance is responsible for periodically reviewing the presentations, either on tape or concurrent with broadcast, contacting the RR if unacceptable material is included, and making a record of the review and any action taken.

5.13.5 Securities Sold By Prospectus

When presentations include discussion of securities sold by prospectus (mutual funds, variable annuities, *etc.*), participants should receive a copy of the prospectus. A list of participants should be prepared and an indication included that prospectuses were provided.

5.13.6 Options (NOT APPLICABLE AT PRESENT)

Any presentation that includes a discussion of options must be approved by Compliance prior to the presentation. Compliance will maintain a written record of any such approved presentations including an outline or description of the presentation.

5.13.7 Collateralized Mortgage Obligations (CMOs)

Because of the potential complexity of some CMO investments, review by the designated supervisor of the CMO area is required prior to public speaking on these investments. The chapter *COLLATERALIZED MORTGAGE OBLIGATIONS (CMOs)* should be reviewed for further information.

5.13.8 Mutual Funds

Refer to the section *Seminars And Other Public Presentations* in the chapter *MUTUAL FUNDS* for specifics regarding mutual fund seminars.

5.13.9 Cold Caller Requirements

All cold callers will be employees of CIM Securities and will be subject to the usual background investigations for all new employees. Cold callers are supervised by the designated supervisors of their respective departments.

Cold callers will be provided with a copy of CIM Securities's policy regarding cold callers and the Calling Restrictions policy as well as CIM Securities's Do Not Call list. Cold callers will be asked to acknowledge, in writing, receipt of the policies and the list.

5.13.10 Permissible Cold Caller Activities

Unregistered cold callers are restricted to the following:

- Inviting prospects to CIM Securities-sponsored events
- Asking whether a prospect would like to speak to an RR
- Asking whether a prospect would like to receive information about investments

When making a call, the cold caller must identify himself or herself as well as CIM Securities and the purpose of the call.

Prior to making calls, the caller must check CIM Securities's Do Not Call List.

5.13.11 Prohibited Cold Caller Activities

Unregistered individuals may NOT:

- Solicit prospects to open accounts
- Discuss general or specific products or services
- Pre-qualify prospects by inquiring about financial status or investment objectives
- Use an alias when identifying themselves
- Contact persons included on CIM Securities's Do Not Call List

5.13.12 Telemarketing Restrictions

Cold caller activities are subject to the Telephone Consumer Protection Act of 1991 issued by the Federal Communications Commission, as outlined in the section *Calling Restrictions* of this manual.

5.13.13 Scripts

Cold callers will be restricted to CIM Securities-approved scripts when making calls. Scripts are approved by the designated supervisor prior to use.

5.14 Electronic Communications

[FINRA Rule 3110(b)(4) and 3310.06]

The Electronic Communications Policy for all employees is included in the chapter *GENERAL EMPLOYEE POLICIES*. This section provides details of these requirements and oversight of electronic communications.

5.14.1 Electronic Communications Systems And Devices

Compliance will determine what systems and devices may be used for CIM Securities business communications. Approved systems and devices are included in the Electronic Communications Policy.

5.14.2 Education And Training

Employees are required to review and understand the electronic communications policies and procedures contained in this manual. Employees may also be subject to training as appropriate.

5.14.3 Commercial E-Mail Procedures

[CAN-SPAM Act of 2003]

E-mails that are "commercial electronic mail" are subject to the CAN-SPAM Act. Commercial electronic mail includes, under federal law, any electronic mail message primarily for the purpose of sending a commercial advertisement or promotion of a commercial product or service. It does not include electronic mail relating to transactions or where there is a relationship between the sender and the recipient. The Act applies to "persons" who include individuals, groups, unincorporated associations, limited or general partnerships, corporations, or other business entities.

CIM Securities's e-mail will comply with the following federal requirements.

- All e-mails will include clear identification of CIM Securities, its address and the sender's e-mail address.
- E-mails will be sent using CIM Securities's computers or other computers specifically authorized for transmission of CIM Securities e-mails.
- Recipients will be given the opportunity to "opt-out" from receiving future commercial electronic mail. The recipient cannot, as a condition of honoring an opt-out request, be charged a fee, be required to provide information other than the recipient's e-mail address and opt-out preferences and be required to take any steps other than sending a reply e-mail or visiting a single page on an Internet website. Opt-out requests will be effected within 10 business days of the request, as required by the Act.
- Where CIM Securities e-mails include other marketers (for example, a mutual fund management company), CIM Securities will be considered the "sender" responsible for compliance with the Act unless specifically agreed in advance that another entity included in the e-mail will act as "sender."
- CIM Securities will not use "address harvesting" or "dictionary attacks" to obtain e-mail addresses from the Internet.

5.14.4 Review Of Electronic Communications

This section outlines procedures for reviewing electronic communications.

5.14.4.1 Methods Of Review

All electronic communications are subject to review. Types of review include:

- Lexicon-based program that identifies words or phrases in communications selected for review
- Review of all or sampled communications depending on business area and/or criteria determined by Compliance for selective review

5.14.4.1.1 Delegation Of Review

The IB supervisor is responsible for reviewing electronic communications and taking necessary actions. The review may be delegated to a qualified reviewer; "qualified" means the individual has been trained in what to review and what items to refer to the supervisor and/or Compliance. Though reviews are delegated, the supervisor is ultimately responsible for compliance with review requirements. The delegated reviewer will refer the following communications:

- Questionable language to the designated supervisor or Compliance

- Objectionable language or content (profanity, *etc.*) to the supervisor or Compliance
- Complaints to the designated supervisor **and** Compliance
- Advertising not previously approved to Compliance
- Communications regarding errors or account designation changes in orders to the supervisor

5.14.4.2 Communications Review Before Or After Sending

The following communications require approval by a qualified supervisor **prior to** sending. Other types of communication are subject to post-sending review.

- Advertising (Compliance approval required)
- Form letters (approval of initial form required; subsequent communications may be sent without prior approval if there is no change in previously-approved content)
- Retail communications (communications sent to more than 25 retail investors)

5.14.4.3 Review Of Institutional Customer Communications

Incoming and outgoing customer electronic communications are reviewed, and complaints are referred to Compliance.

5.14.4.4 Review Of Institutional Communications

Incoming and outgoing customer electronic communications are reviewed, and complaints are referred to Compliance.

5.14.4.5 Review Of Investment Banking Communications

- All communications between Research (if applicable) and investment banking personnel must be routed through Compliance and may not be directly sent.
- Confidentiality of communications about confidential investment banking activities must be protected by limiting access to information (passwords, closing open pages when not in use, avoiding use of PDAs in public places, *etc.*).
- Communications are subject to review and retention.

5.14.4.6 Special Reviews

Compliance may impose different standards of review that may include review of all incoming and outgoing communications regardless of form; pre-approval; or other special reviews. See the section *Heightened Supervision* in the chapter *EMPLOYMENT, REGISTRATION AND LICENSING* for further information.

5.14.4.7 Use Of Non-Firm Systems Or Devices

CIM Securities may approve the use of non-Firm systems or devices by certain employees. When exceptions are approved, the employee will be required to submit a separate certification regarding the use of the external system/device and re-certify annually; usage will be monitored and periodically audited by Compliance.

5.14.5 Advertising

Electronic advertising is subject to pre-use review by Compliance and/or IB Supervisor. Refer to the section *Retail Communications* in this chapter.

5.14.6 Internet

This section outlines procedures for accessing communications systems on the web and posting information to the web, including a firm web site.

5.14.6.1 Social Networks, Bulletin Boards, Web Sites And Other Electronic Communication Systems

[FINRA Regulatory Notice 10-06]

The use of social networking sites (Facebook, LinkedIn, Twitter, *etc.*), bulletin boards, web sites, message boards, or other electronic communication systems on the Internet for the purposes of advertising, soliciting business, or in any way communicating about Firm business is prohibited, exceptions may be made on a limited basis, subject to review and recordkeeping.

5.14.6.2 Digital Channels

Digital channels are communication paths and platforms which may include promotion, marketing, or selling products and services and allowing customers to access information and communicate with CIM Securities. RRs and customers are advised of available features of Firm digital channels. This may include the use of mobile apps.

RRs may use only authorized digital channels (and tools and features); unauthorized channels, tools and features may be blocked. Activity and content on digital channels are subject to supervisory reviews and record retention requirements.

Video presentations are subject to prior approval including submission of scripts and details of contents. Video blogs must be approved prior to initiation and records retained of all video blog information.

5.14.6.3 Firm Web Site

[FINRA Rule 2210; FINRA Notice to Members 07-02; SIPC By-Laws Article 11 Section 4; SEC Guidance for public companies on the use of company web sites: <http://www.sec.gov/rules/interp/2008/34-58288.pdf>; FINRA BrokerCheck link requirements: <https://www.finra.org/compliance-tools/rule-2210-brokercheck>]

Responsibility	<ul style="list-style-type: none"> • CCO
Resources	<ul style="list-style-type: none"> • CIM Securities's web site • Requests to include information
Frequency	<ul style="list-style-type: none"> • Approvals - as required • Periodic (at least monthly) review of the web site
Action	<ul style="list-style-type: none"> • Review proposed materials to be included on the web site and approve or disapprove <ul style="list-style-type: none"> ◦ Determine whether filing with FINRA is required and make necessary filings • Review the web site to confirm that only previously approved materials are included • If SIPC is referenced on the site, provide a hyperlink to the SIPC web site • If FINRA is referenced on the site, provide a hyperlink to FINRA's home page • Contact supervisors of departments that have included unapproved materials and take corrective action • Confirm hyperlinks to BrokerCheck are included • Corrective action may include changing or deleting the material and/or reminding the supervisor of the pre-use approval requirement
Record	<ul style="list-style-type: none"> • Approved materials and (if applicable) copies of FINRA filings • Notations regarding periodic reviews and corrective action taken • Record of the appearance of the site over the past 3 years (including all changes)

CIM Securities has established a web site. Any information to be included on the web site requires the **prior approval** of Compliance.

If CIM Securities's site refers to its membership with FINRA, a hyperlink to the FINRA internet home page will be included. If SIPC membership is included on the site, a hyperlink to SIPC's web site will be shown.

The site also includes the required hyperlink to FINRA's BrokerCheck on the initial web page for viewing by retail investors and on any web page that includes a profile of one or more RRs who deal with retail investors. The hyperlink is not required for firms that do not conduct business with retail investors or to a directory or list of RRs limited to names and contact information.

5.14.6.4 RR Web Sites

RRs are permitted to establish web sites under the following conditions:

- RRs must obtain Compliance approval to publish a web site.
- Additions or changes to the site must receive the prior approval of Compliance.

5.14.6.5 Data Feeds

[FINRA Regulatory Notice 11-39]

Any third party data feeds tied to CIM Securities's or an RR's web site must be reviewed by Compliance prior to use. Reviews will identify the proficiency of the data provider to feed accurate and timely information. Compliance will regularly review the data feeds for red flags indicating the data may not be accurate and will take corrective action as necessary.

Compliance will advise the requestor whether the data provider is approved and will retain records of its review.

5.14.6.6 Third-Party Postings

Compliance must review and approve any requests to include third-party postings on CIM Securities's web site prior to inclusion of such postings on the site. If third-party postings (including customer postings) are permitted, the following requirements will apply:

- A disclaimer will be included on the web site stating that such posts are not those of CIM Securities; do not reflect the views of CIM Securities; and CIM Securities does not take responsibility for the content of such posts.
- Potential third-party posters must pre-register and will be screened by Compliance before being allowed to post content.
- The site is regularly reviewed and third-party posts will be monitored as part of that review to mitigate any perception that CIM Securities is adopting any post.
- Usage guidelines will be provided to customers or other third parties permitted to post on firm-sponsored sites.
- Compliance may develop standard responses that RRs will be authorized to use in response to third-party postings on social media web sites.

Compliance will retain records of registration and screening of third parties allowed to post.

5.14.7 Hyperlinks

[FINRA Interpretation Letter from Thomas M. Selman to the Investment Company Institute, November 11, 1997]

When hyperlinks to third-party sites are included in CIM Securities communications or on a CIM Securities web site, it is important the hyperlink meets the following conditions to avoid liability for the content or regulatory filing of information included in the third-party site:

- A hyperlink may not be established to a site known (or there is reason to know) to contain false or misleading information.
- The hyperlink must be continuously available to investors who visit the site.
- CIM Securities or its employees cannot have discretion to alter information on the third-party site.
- Investors have access to the hyperlinked site whether or not it contains material favorable to CIM Securities.
- The linked site can be updated or changed by the third party, following which investors would still be able to use the hyperlink.

5.14.8 Prohibition Against Automatic Erasing/Deleting

[FINRA Regulatory Notice 11-39]

CIM Securities and its employees are prohibited from sponsoring a social media site or using a communication device that includes technology which automatically erases or deletes content.

5.14.9 Policy Violations

Employees who violate CIM Securities's Electronic Communications Policy are subject to disciplinary action which may range from education, restricting electronic and/or Internet access, to suspension or termination depending on the nature and seriousness of the infraction. Compliance determines the appropriate action to be taken.

5.15 Identification Of Sources

When using communications not prepared under the direct supervision of CIM Securities, it is necessary to identify, on the communication, the person or entity that prepared the material. This includes research reports obtained from outside sources.

6 FINANCIAL AND OPERATIONS PROCEDURES

This chapter provides key policies and procedures affecting the financial and operations areas of CIM Securities. Detailed operations procedures are included in a separate operations manual maintained by CIM Securities or, if CIM Securities is an introducing firm, the clearing firm's operations manual.

CIM Securities has designated a Financial and Operations Principal who is responsible for general oversight of financial and operations areas of CIM Securities. Supervisors of specific financial or operations areas are responsible for day-to-day procedures.

6.1 Qualification Of Operations Personnel

[FINRA Rule 1230(b)(6)(A) and 1250; FINRA Regulatory Notice 11-33]

Certain operations personnel are considered "covered persons" under FINRA Rule 1230 because of their responsibilities for "covered functions" as defined in the Rule. These personnel are required to qualify as "Operations Professionals" by completing the Series 99 qualification examination or by qualifying for an exception because of the person's other registration qualifications. In general the requirements apply to senior management responsible for covered functions; persons designated by senior management to supervise, manage, or approve or authorize work relating to the covered functions; and persons with authority or discretion materially to commit CIM Securities's capital relating to covered functions. The Rule should be consulted for definitions of covered persons and covered functions.

In addition, covered persons are required to participate in Regulatory Element and Firm Element continuing education. Refer to the chapter *TRAINING AND EDUCATION* for procedures regarding continuing education.

CIM Securities has named a Principal Financial Officer and Principal Operations Officer (unless an exception applies). Refer to the section *Principal Financial Officer And Principal Operations Officer* in the chapter *EMPLOYMENT, REGISTRATION AND LICENSING* for detailed information about these designations.

The Principal Operations Officer is responsible for confirming that covered persons complete the necessary requirements for registration and continuing education and to restrict an employee's activities if either requirement is not completed within required timeframes.

6.2 Books And Records

[SEC Securities Exchange Act of 1934 Rule 17a-3 and Rule 17a-4; FINRA Rule 4510, 4511 and 4512; FINRA New And Amended Recordkeeping Checklist: <http://www.finra.org/industry/books-and-records>; MSRB Rule G-8 and G-9]

6.2.1 Introduction

SEC Rule 17a-3 identifies the types of books and records to be retained by CIM Securities and 17a-4 identifies the period these records are to be retained. SROs also specify certain record requirements. Designated supervisors are responsible for retaining required records for areas under their supervision. The FINOP is responsible for establishing and maintaining CIM Securities's record retention schedule.

For accounts and other business introduced to a clearing firm, the clearing firm is responsible for retaining certain records as outlined in the clearing agreement.

6.2.2 Electronic Storage Of Records

[SEC Securities Exchange Act of 1934 Rule 17a-4(f); FINRA Regulatory Notice 18-31]

CIM Securities utilizes electronic storage media and/or micrographic media for certain records.

6.2.2.1 Notification To Examining Authority

[SEC Securities Exchange Act of 1934 Rule 17a-4(f)(2)(i)]

CIM Securities has provided the required notification to its designated examining authority (DEA) prior to employing electronic storage media. The independent third party with download access is also required to submit an undertaking indicating it agrees to promptly furnish information to regulators.

6.2.2.2 Conditions

[SEC Securities Exchange Act of 1934 Rule 17a-4(f)(2)(ii)]

As required by rule, CIM Securities's electronic storage media meets the following conditions:

- non-rewritable, non-erasable format
- automatic verification of the quality and accuracy of the process
- serialize original (and duplicate units) and time-date for required retention period
- capacity to readily download indexes and records

6.2.2.3 Ability To Retrieve And Reproduce

[SEC Securities Exchange Act of 1934 Rule 17a-4(f)(3)]

CIM Securities's electronic or micrographic storage will also meet the following requirements:

- facilities for immediate, easily readable production of records
- ability to provide facsimile enlargements
- duplicate copies stored separately from the originals
- organized and indexed accurately
- current information necessary to access records and indexes
- independent third party who has access and the ability to download records

6.2.2.4 Audit System

The third party that provides electronic storage services has an audit system to test, on an ongoing basis, the integrity of the Firm's records retained in electronic storage media. Anomalies reported by the third party will be reviewed by the FINOP or another designated person on the FINOP's behalf to ensure corrective action has been taken and records are retained as required.

6.2.2.5 Confidentiality Of Electronic Records

CIM Securities (in conjunction with any vendor) protects against unauthorized access to or use of customer records by use of a password system. Passwords will be changed periodically and disabled for terminated employees or employees no longer requiring access.

6.2.3 Availability Of Records In Offices

Required records under Rules 17a-3 and 17a-4 are available in office locations. The FINOP is responsible for establishing a method for producing required records at office locations upon the request of a regulator. The section *Office Records* in the chapter *OFFICES* discusses this subject in more detail.

6.3 Calculation And Reporting Of Net Capital

[SEC Securities Exchange Act of 1934 Rule 15c3-1, Rule 17a-5 and Rule 17a-11; FINRA Rule 4110, 4120, 4130, 4140, 4521 and 4524]

The calculation and monitoring of net capital is the responsibility of the FINOP who also is responsible for ensuring the accurate and timely reporting of periodic net capital reports. Some of the FINOP's specific responsibilities include:

- Review and filing of CIM Securities's financial reports and periodic review of accounting records
- Periodic consideration of whether CIM Securities's minimum net capital requirements have changed because of changes in CIM Securities's business
- Supervising additions to, and withdrawals from, the equity capital of CIM Securities
- Reporting borrowings and subordinated loans for capital purposes
- Establishing procedures for retention of required financial books and records

If CIM Securities becomes deficient in its net capital position, the FINOP is responsible for making the necessary reports to regulators and communicating any restrictions in business that may result.

6.4 Reports

Responsibility	<ul style="list-style-type: none">• FINOP
Resources	<ul style="list-style-type: none">• Data regarding capital, sending of statements, compliance with protection of customer assets
Frequency	<ul style="list-style-type: none">• Monthly: Risk reports (if applicable)• Quarterly: Custody Report• Annually: Audit Report; Exemption or Compliance Report (whichever applies)
Action	<ul style="list-style-type: none">• File required reports
Record	<ul style="list-style-type: none">• Records of reports and when filed

CIM Securities is obligated to file certain reports with regulators.

6.4.1 Annual Audit Report

[Exchange Act Rule 17a-5(d); FINRA Regulatory Notice 16-05 and 11-46]

The FINOP is responsible for filing of CIM Securities's annual audited financial statements with regulators, not more than 60 days after the date of the statements, including the oath and affirmation page. Filing is made electronically with FINRA and the SEC. The FINOP will retain records of the filings including the filings themselves, names of regulators, and date of filing.

Reports will be as of the same fixed or determinable date each year, unless a change is approved in writing by FINRA. A copy of FINRA's written approval will be sent to CIM Securities's SEC regional office.

6.4.2 Risk Reports

If CIM Securities computes capital charges under 15c3-1e (limitations on the withdrawal of equity capital) it is required to file additional reports with the SEC. Reports are required within 17 business days after the end of each month that is not a quarter and within 17 business days after the end of each quarter. Refer to Rule 17a-5(a)(6) for details of what must be reported.

6.4.3 Custody Report And Requirements

[SEC Securities Exchange Act of 1934 Section 17(b); FINRA web page: <https://www.finra.org/media/document/8365>]

CIM Securities is required to file a quarterly Form Custody report that contains information about whether and how CIM Securities maintains custody of customer assets.

CIM Securities is also required to allow staff of the SEC and SROs to review working papers of CIM Securities's PCAOB-registered independent public accounting firm if requested in writing as part of an examination and allow regulators to discuss the findings of CIM Securities's accounting firm with the accounting firm's representatives. The FINOP is responsible for facilitating regulators' access.

6.4.4 Exemption Report

[SEC Securities Exchange Act of 1934 Rule 17a-5]

CIM Securities will annually file with the SEC the Exemption Report (within 60 calendar days after the fiscal year-end as part of CIM Securities's annual compliance audit).

6.5 Reconciliations And Bank Records

Responsibility	FINOP
Resources	<ul style="list-style-type: none">• Bank records
Frequency	<ul style="list-style-type: none">• Monthly
Action	<ul style="list-style-type: none">• Reconcile bank accounts against CIM Securities's records
Record	<ul style="list-style-type: none">• Bank statements and other bank records, retained by FINOP

The FINOP is responsible for establishing procedures for the periodic reconciliation of bank statements, clearing and depository accounts, and other accounting and business records. Records of bank accounts and other reconciled accounts will be maintained in accordance with regulatory requirements.

6.6 Designation Of Accountant

[SEC Securities Exchange Act of 1934 Rule 17a-5(f)]

The FINOP is responsible for filing notice of the designation of its accountant by December 10 of each year with FINRA, the SEC's principal office, and CIM Securities's SEC regional office. If the agreement with the accountant is continuous providing for successive annual audits, notice is not required annually. The following additional requirements apply:

- An agreement must exist with an independent public accountant by December 1 covering a contractual commitment to conduct CIM Securities's annual audit during the following calendar year.
- If the agreement is for a single audit or if the continuing agreement is terminated or amended, a filing is required by December 10.
- If CIM Securities is exempt from filing an annual audited financial statement, notice must still be filed indicating the date as of which an unaudited report will be prepared.
- Notice must be filed with FINRA and the two SEC offices within 15 days after:
 - CIM Securities notifies the accountant that its services will be terminated;
 - the accountant notifies CIM Securities it will not continue its engagement; or
 - a new accountant has been engaged without notice to or by CIM Securities's current accountant.

The FINOP is responsible for maintaining a record of filing the required notices.

6.7 Guarantees By, Or Flow Through Benefits For, Members

[FINRA Rule 4150]

Whenever CIM Securities guarantees, endorses, or assumes, directly or indirectly, the obligations or liabilities of another person (including an entity), a written request will be made to FINRA. Prior written approval from FINRA is required whenever CIM Securities receives flow-through capital benefits in accordance with Appendix C of SEC Rule 15c3-1. The FINOP is responsible for filing necessary requests for such arrangements; responding to

subsequent FINRA requests for information; complying with FINRA rule requirements; and maintaining records regarding such arrangements.

The requirements when entering into such an arrangement include the following:

- CIM Securities must have the authority to make available to FINRA the books and records of the other person or entity for inspection in the U.S. The other person's books and records must be kept separately from those of CIM Securities.
- CIM Securities is required to provide FINRA with the person's FOCUS reports simultaneous with their being filed with the person's designated examining authority (DEA), unless the person's DEA is FINRA. If the person is not a registered broker-dealer, CIM Securities will submit financial and operational statements in a format and for time periods required by FINRA.
- Guarantees executed in the normal course of business (trade guarantees, signature guarantees, endorsement of securities and the writing of options) are not subject to these requirements. Guarantees regarding the writing of options are not subject if appropriately recorded in CIM Securities's books and records and reflected in net capital computations.

6.8 General Ledger And Suspense Accounts

[FINRA Rule 4523]

Responsibility	FINOP
Resources	<ul style="list-style-type: none">• Ledger and suspense accounts
Frequency	<ul style="list-style-type: none">• Ongoing - oversee entries• Monthly or more frequently - review of accounts
Action	<ul style="list-style-type: none">• Oversee entries• Determine accounts are current and accurate• Review accounts to determine they are accurate and any aged or unresolved are promptly identified for research and possible transfer to suspense account(s)
Record	<ul style="list-style-type: none">• General and suspense accounts• Resolution of aged or unresolved items• Record of reviews including reviewers initials, date reviewed, notes of action taken, if any

The designated supervisor (or supervisors, if accounts are assigned to multiple persons) is responsible for oversight of general ledger and suspense accounts. Suspense accounts must be clearly identified as such and record money charges or credits and receipts or deliveries of securities whose ultimate disposition is pending determination. The record must include all information known for each item recorded.

6.9 Financial Reporting

[SEC Securities Exchange Act of 1934 Rule 17a-5 and Rule 17a-11; SEC FAQs regarding financial responsibility rules: <http://www.sec.gov/divisions/marketreg/amendments-to-broker-dealer-financial-responsibility-rule-faq.htm>; FINRA Rule 4520 Series]

6.9.1 Part-Time, Off-Site Or Multiply Registered FINOP

[FINRA Notice to Members 06-23]

Responsibility	FINOP
Resources	<ul style="list-style-type: none">• Background and capabilities of the FINOP• References from other firms• FINOP's CRD record• Reports prepared by the FINOP• Observation of performance
Frequency	<ul style="list-style-type: none">• At time of hire: background check• Ongoing: evaluate FINOP's work
Action	<ul style="list-style-type: none">• Conduct background check before hiring FINOP:<ul style="list-style-type: none">○ Review qualifications○ Check references○ Review CRD record○ Conduct other reviews such as credit review○ Obtain contract outlining FINOP's responsibilities including the obligation to remain current on rules and regulations affecting FINOP responsibilities• Review FINOP's work including timely completion and filing of FOCUS reports, other reports prepared by the FINOP
Record	<ul style="list-style-type: none">• Background check information• Contract with FINOP• Review of FOCUS and other reports

CIM Securities employs a FINOP who is part-time, off-site, or registered with multiple firms. The FINOP's responsibilities are outlined in CIM Securities's contract with the FINOP and include the following:

- Prepare and file FOCUS reports
- Review items that may impact net capital

6.9.2 Financial Statements

[SEC Securities Exchange Act of 1934 Rule 17a-5(c)]

The FINOP will determine CIM Securities's obligation to provide financial statements to customers. This section discusses exemptions and requirements. Rule 17a-5 should be consulted for details regarding the requirements.

Broker-dealers are required to provide financial statements to their customers unless they qualify for an exemption, which includes: (1) an introducing broker or dealer; (2) a BD that promptly forwards subscriptions for

securities to the issuer, underwriter, or other distributor and does not hold funds or securities; (3) a BD dealing with subscriptions of mutual funds, sale/redemption of savings and loan associations, or offering credit for loans to purchase insurance related to the sale of mutual funds; or (4) a BD that conducts business that is exempt under Rule 17a-3(a). These exemptions have further conditions and Rule 17a-5 should be consulted.

For firms that do not qualify for an exemption, audited statements must be provided to customers within 105 days after the end of the BD's fiscal year or within 30 days of that date if sent with the next mailing of quarterly customer statements. Unaudited statements dated 6 months from the date of the audited statements must be provided to customers within 65 days after the date of the unaudited statement or 70 days after that time if sent with the next mailing of customer quarterly statements.

Statements are not required to be sent if posted on the BD's web site not later than 90 days after the date of audited statements or 75 days after the date of unaudited statements. Statements must be accessible by hyperlinks in either textual or button format, separate prominent links that are clearly visible, and are placed in **each** of the following locations:

- On the BD's website home page; and
- On each page where a customer can enter or log in to the website; and
- If the home page website is for two or more BDs, on the home page of the website of each BD.

In addition, the BD must maintain a toll-free number that customers may call to request statements and must send statements promptly after request at no cost to the customer. The BD also must not have been required, during the year prior to the date of the statement, to give notice and transmit a report to the SEC under 17a-11(e).

6.9.3 Disclosure Of Financial Condition

[FINRA Rule 2261]

Upon request, information about CIM Securities's financial condition in its most recent balance sheet will be made available to customers and to any member firm that is party to an open transaction or has on deposit cash or securities with CIM Securities. The information may be provided in paper or electronic form (if for a customer, the customer must consent to electronic delivery).

6.9.4 Notification Rule ("Early Warning Rule")

[SEC Securities Exchange Act of 1934 Rule 17a-11]

The FINOP is responsible for notifying (within 24 hours) the SEC and other securities regulators upon the occurrence of certain events (insolvency, decrease of net capital below required minimum, or CIM Securities's repurchase and securities lending activities exceed 25 times its tentative net capital). As an alternative to notification regarding repurchase and securities lending activities, CIM Securities may report monthly as to its stock loan and repurchase activities to its DEA. The FINOP is responsible for maintaining records of any early warning notifications (or monthly reports).

6.10 Regulation T And Extension Of Credit To Customers – NOT APPLICABLE AT PRESENT

[FINRA Rule 4210; NYSE Rule 430-434; Federal Reserve Regulation T]

Responsibility	NOT APPLIBALE AT PRESENT
Resources	<ul style="list-style-type: none"> • Various • FINRA Customer Debits Report
Frequency	<ul style="list-style-type: none"> • Ongoing
Action	<ul style="list-style-type: none"> • Monitor accounts for compliance with Regulation T requirements • Request extensions, issue margin calls, <i>etc.</i> • Discontinue margin trading for accounts missing required signed margin agreements • Review FINRA report for unsecured debits and take corrective action as necessary which may include consultation with RR and RR's supervisor, closing the account, or other appropriate action
Record	<ul style="list-style-type: none"> • Various records maintained by Operations • FINRA report including notes of action taken

6.10.1 Compliance With Regulation T – If applicable

It is the responsibility of the FINOP to establish operating procedures to ensure compliance with Regulation T regarding the settlement of customer transactions.

6.10.2 Customer Margin Balance Report – If applicable

[FINRA Rule 4521(d)]

If CIM Securities carries customer margin accounts, the FINOP is responsible for filing the Customer Margin Balance Form on a settlement date basis, as of the last business day of the month. For any month where there is no information to submit, a report will be filed indicating such. The report is due as promptly as possible after the last business day of the month, but in no event later than the sixth business day of the following month and is filed through the FINRA Firm Gateway.

The FINOP is responsible for retaining records of filings.

6.11 Fees And Service Charges

[FINRA Rule 2122; NASD Notice to Members 92-11]

Broker-dealers are obligated to disclose fees and service charges to customers. In general, fees and charges are required to be reasonable and not unfairly discriminatory between customers.

If a fee or commission will be charged to redeem a mutual fund and the fund could be sold through the fund company itself without cost, the customer should be notified that the fund could be redeemed without cost by liquidating directly through the mutual fund.

6.11.1 Notification Of Customers

Customers will be notified of fees and changes to fees and service charges as follows:

- At the time an account is opened.
- When there is an increase in fees, at least 30 days prior to the increase to the last known address of every customer whose account is subject to the fees.
- If notification is by a method other than a letter (*i.e.*, statement stuffers, newsletters, *etc.*) notification of a fee increase will be clear and conspicuous and in plain English.
- Where a website is used to communicate or interact with customers, all fees will be posted (and kept current) including changes and the projected date of changes.
- For extensive fee changes, a letter may be sent to customers referring them to a website where complete information may be obtained.

6.12 Fidelity Bonding

[FINRA Rule 4360]

As required, CIM Securities is a member of SIPC and maintains required blanket fidelity bonding coverage based on CIM Securities's net capital requirement. The FINOP is responsible for obtaining and maintaining fidelity bonding as required by rule and verifying the adequacy of coverage and making necessary adjustments on at least an annual basis on the anniversary date of the issuance of the fidelity bond.

6.13 Independent Verification Of Assets

[FINRA Rule 4160]

If applicable, CIM Securities may custody assets (customer or proprietary) at financial institutions that are not members of FINRA. FINRA may request written verification of Firm assets held by that institution. If FINRA notifies CIM Securities that the institution has failed to respond to FINRA, CIM Securities will withdraw its assets promptly and transfer them to another financial institution. This requirement does not apply to:

- proprietary assets that are treated as non-allowable assets under Exchange Act Rule 15c3-1; or
- instances where FINRA determines there is no independent custody or record ownership of assets

The FINOP is responsible for withdrawing affected assets when notified by FINRA. Contracts with non-member financial institutions may include the obligation that the financial institution comply with FINRA requests for verification of assets. The FINOP controls records of custody arrangements and contracts.

6.14 Cash Deposits Not Accepted

CIM Securities does not accept cash or currency from customers. If a customer attempts to deposit cash or currency, the employee receiving the deposit is responsible for refusing the deposit and advising the customer CIM Securities will only accept checks.

In the event cash is inadvertently accepted, the following steps must be followed:

- Immediately provide the cash to the cashier or other authorized Operations personnel.

- The cashier or Operations is responsible for counting the cash (2 people must be present to verify the amount) and entering the amount into CIM Securities's customer account system for credit to the customer's account.
- Immediately thereafter the cash must be walked to CIM Securities's bank for credit to the account maintained for the benefit of customers or, if no account exists, obtain a cashier's check or money order made payable to CIM Securities (or its clearing firm if applicable) and then deposit or send the check/money order to the bank account for customers the same day.
- The Operations Manager is responsible for filing Form 104 (Currency Transaction Report) with the IRS by the 15th calendar day after receipt for cash in excess of \$10,000 for one person on any one day.
- The designated supervisor of Operations is responsible for retaining a file of forms filed with the IRS.

6.15 Cash Equivalents

CIM Securities also does not accept deposits of cash equivalents such as travelers checks, money orders, or cashiers checks. Customers attempting to deposit cash equivalents should be advised to instead provide a personal check for deposit to their account.

6.16 Risk Management

[FINRA Notice to Members 99-92; SEC Securities Exchange Act of 1934 Rule 17a-3(a)(23), Rule 17h-1T and Rule 17h-2T]

Risk management is the identification, management, measurement and oversight of various business risks (such as proprietary trading, credit, liquidity and new products) and is part of CIM Securities's internal control structure.

6.16.1 Risk Practices Regarding Employment And Employees

CIM Securities has established procedures regarding the hiring of personnel; conduct and review of employee accounts; granting of authority to act in various capacities on behalf of CIM Securities; and the integrity of CIM Securities's systems and financial reporting.

6.16.1.1 Background Checks

One of CIM Securities's first lines of defense is the hiring of qualified people who do not bring high-risk behavior to their positions. CIM Securities conducts background checks on all applicants for employment with CIM Securities. All offers of employment are considered conditional pending the outcome of the background checks. These background checks include contact with the applicant's prior employers for at least the past three years or use of third party vendor. Any adverse information is referred to the supervisor/management for consideration prior to finalization of employment.

Also refer to the section *Hiring Procedures* in the chapter *EMPLOYMENT, REGISTRATION AND LICENSING* for more information about hiring procedures.

6.16.1.2 Employee Accounts

Employees are subject to policies governing the conduct of their personal securities accounts. Refer to the section *Employee And Employee Related Accounts* in the chapter *GENERAL EMPLOYEE POLICIES* as well as the chapter on *INSIDER TRADING*.

6.16.1.3 Authority

Employees may only act on behalf of CIM Securities within the boundaries of authority granted them by CIM Securities. The following generally outlines the authority of certain employees or committees and their respective responsibilities.

6.16.1.3.1 Chief Financial Officer (or FINOP as applicable)

The Chief Financial Officer (or his/her designee - FINOP) is responsible for the following on behalf of CIM Securities:

- Establishing accounting procedures in accordance with generally accepted accounting principles
- Ensuring the accurate and timely filing of CIM Securities financial reports with regulators and others where financial reports are required
- Establishing bank accounts and designating employees authorized to sign checks and transfer funds on behalf of CIM Securities
- Interacting with CIM Securities's public accounting firm and coordinating the providing of information requested during CIM Securities's annual audit
- Follow up regarding exceptions or recommendations referred by the outside public accounting firm

6.16.1.3.2 Department/Business Unit Managers – Not Applicable At Present

Department and business unit managers are responsible for oversight of the activities within their respective department or business unit, with the interests of customers and CIM Securities as foremost considerations. The general scope of responsibility includes, among other responsibilities, the following:

- Hiring and termination of department/business unit personnel
- Supervision of department/business unit personnel including periodic reviews and salary administration
- Creating a safe and positive work environment for personnel
- Establishing and administering a budget to conduct the activities of the department/business unit
- Ensuring only authorized personnel act on behalf of CIM Securities (check signing, purchasing supplies, etc.)

6.16.2 New Accounts

In addition to review and approval by the designated principal/IB Supervisor new accounts are subject to CIM Securities's Customer Identification Program (described in the Anti-Money Laundering Program) and verification against a vendor database of potential "problem" accounts.

6.16.3 Technology Management

Oversight of CIM Securities's technology systems is the responsibility of the Chief Technology Officer or a management person with similar responsibilities working with outside IT vendors. Oversight includes:

- Review and approval of new systems or programs
- Review and approval of vendors that provide systems or programs and those that service CIM Securities's systems
- Review and approval of back office and vendor system changes, revisions to new systems or programs
- Development and oversight of security for systems (see *Cybersecurity* that follows)
- Oversight of the plan to adopt changes or new systems
- Periodic testing of systems and algorithms
- Documentation of systems
- Delegation of responsibility to those responsible for technology systems
- Training regarding systems and programs
- Oversight of algorithms including both proprietary and order-routing algorithms

6.16.4 Protection Of Customer Information And Records

CIM Securities has adopted procedures to protect customer information, including the following:

- Computerized customer information is accessed by password protection or other established controls within the Firm's (or clearing firm's) system to ensure only authorized persons gain access. For example, sales personnel may access information regarding accounts assigned to them but not the accounts assigned to others.

6.16.4.1 Social Security Numbers (SSNs)

SSNs are part of the information subject to protection of customer records. SSNs are obtained when accounts are opened, as required by federal law. SSNs are retained with account records and used for federally-required year-end reporting of transactions and/or income. Access is limited to authorized employees (operations personnel, RRs, managers, *etc.*) and are provided to outsiders only when required by law or court/arbitration action or other authorized authority.

6.16.4.2 Access To Customer Information Via Wi-Fi

Because of risk of unauthorized access by outside parties and the difficulty of ensuring the security of wireless connections to the Internet, employees are not permitted to use wireless fidelity (Wi-Fi) to access customer account information, unless:

- the employee is working on Firm premises; or
- the employee has installed Firm-required firewalls or other protections and has prior approval from CIM Securities's designated information officer to use Wi-Fi for Firm business.

6.16.4.3 Remote Access To Customer Accounts

Some employees may be authorized to work at home or while traveling during which time CIM Securities's network will be accessed. Authorization must be requested from the designated principal who will assign passwords and retain a record of authorized employees. Firewalls and other protections are in place to prevent intrusion by outsiders and breaches of confidentiality.

6.16.4.4 Disposal Of Consumer Report And Customer Information And Records

[SEC Regulation S-P Rule 30(b); SEC Release No. 34-50781; Fair and Accurate Credit Transactions Act of 2003 Section 216]

Consumer report and customer information and records will be disposed of in a manner to prevent unauthorized access or use while preserving firm books and records.

6.16.4.5 Compromised Accounts

If CIM Securities identifies unauthorized access to customer accounts, Compliance will be immediately notified and the following actions will be taken, as appropriate:

- Monitor, limit or temporarily suspend activity in the account
- Investigate the source of the intrusion and whether it is limited to an account or certain accounts
- Notify the clearing firm, if applicable
- Contact the SEC and the FINRA coordinator
- If appropriate, contact law enforcement such as the FBI or the U.S. Postal Inspector if mail is involved
- Contact relevant state regulatory authorities
- Determine whether specific notice to the customer is required under state law if personally identifiable information has been compromised
- Contact the customer and change access passwords and/or account numbers
- Determine whether CIM Securities should file a Suspicious Activity Report (SAR)

If firm data is compromised not involving customer accounts, Compliance and/or Legal (or outside counsel) must determine action to be taken which may include some of the actions listed above.

6.16.5 Credit Risk Management

[FINRA 2022 Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

CIM Securities conducts risk management reviews, as applicable or necessary to identify its exposure to credit risk.

6.16.6 Liquidity Risk Management

[FINRA Regulatory Notice 21-31, 21-12, 15-33, 10-57 and 99-92; FINRA 2022 Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

If applicable or as necessary given its business line, The Firm's management will be responsible for establishing a program to evaluate and monitor CIM Securities's liquidity risk. Liquidity risk can contribute to a firm's failure and customer inability to have prompt access to their assets, even in times of stress. Broker-dealers have an obligation to develop and maintain robust funding and liquidity risk management practices to prepare for adverse circumstances including extraordinary credit events, at the broker-dealer level and also at the holding-company level. FINRA Regulatory Notice 10-57 provides liquidity management practices and red flags for identifying problems.

6.16.7 New Products

[FINRA Notice to Members 05-26]

All new products require review and approval prior to offering new products to customers. A "new product" may include a product that:

- is new to the marketplace or CIM Securities.
- was previously sold only to a limited segment of CIM Securities's customers, such as only to institutional customers and now will be offered to retail customers.
- will be offered by a category of RRs who did not previously offer the product, such as a product new to retail RRs.
- involves material modifications to an existing product including risk, product structure, or fees and costs.
- requires material operational or system changes.
- involves a new or significant change in sales practices.
- raises conflicts that have not been previously identified and addressed.

If there is a question whether a product may be a "new" product, it should be submitted for the new product review.

6.16.7.1 New Product Committee

If applicable, the Firm will establish a New Product Committee or have designated principals (CCO/IB Supervisor) responsible for review of new products. The Committee or designated principals will be responsible for maintaining copies of documents related to the new product being reviewed.

6.16.7.2 Fiduciary Rule Considerations

This section is replaced by SEC Regulation BI. See Reg BI procedures in this manual.

Products and some services sold to retirement accounts are subject to the DOL Fiduciary Rule. See the section *Fiduciary Requirements* in the chapter *ACCOUNTS*. When reviewing a new product/service that is subject to the Fiduciary Rule the following considerations will be made:

- What compensation will be paid and does the compensation comply with the "best interests" requirement of the Fiduciary Rule?
- Does the product/service fall under the BIC or another exemption?
- What notification should be made to RRs and supervisors regarding requirements specific to the product/service (BIC, *etc.*)?

6.16.7.3 Anti-Money Laundering Considerations

New products and/or business lines may represent anti-money laundering risks. Such issues will be referred to the AML Compliance Officer for review.

6.16.7.4 New Product Review Checklist

RRs wanting to offer new products are required to prepare information for the review of the New Product Committee or designated principals by completing a New Product Review Checklist or by providing all pertinent information to the supervising principal and CCO. Information to be provided includes a description of the product, to whom the product would be offered, and economic justification of the product. The Committee or designated principals will notify the requestor regarding approval/disapproval or the need for modifications or additional information.

6.16.7.5 Training

A determination will be made by the committee or supervisor/CCO reviewing the new product regarding the need for training before the product is made available for sale. Considerations include:

- Whether RRs are already knowledgeable about the product including pre-existing training
- Sophistication of targeted investors
- Complexity of the product

6.17 Business Continuity Plan

[FINRA Rule 4370; FINRA Regulatory Notice 13-25; FINRA Notice to Members 06-74 and 04-37; NASDAQ Rule 3510; FINRA Small Firm Business Continuity Plan Template: <https://www.finra.org/compliance-tools/small-firm-business-continuity-plan-template/>; SIFMA Business Continuity Planning website: <https://www.sifma.org/resources/general/bcp/>]

CIM Securities has developed a Business Continuity Plan to provide procedures for response and recovery in the event of a significant business disruption. The purpose of the Plan is to identify responsible personnel in the event of a disaster; safeguard employees' lives and firm property; evaluate the situation and initiate appropriate action; recover and resume operations to allow continuation of business; provide customers with access to their funds and securities; and protect books and records. The Plan was developed considering the types of business conducted, systems critical to support business, and geographic dispersion of offices and personnel.

6.17.1 Designation Of Responsibilities

The following is a list of those responsible for CIM Securities's Business Continuity Plan.

Responsibility	Titles
Maintain and update Plan	CEO or equivalent/CCO
Approve Plan and Plan revisions; conduct annual review	CEO or equivalent

Annual testing of Plan	CCO
Implementation of Plan when a disruption occurs	CEO or equivalent/CCO
Provide Plan information to customers: <ul style="list-style-type: none"> • At time of account opening • Upon request 	RRs – at account opening CCO – Upon request
Post Plan disclosure on CIM Securities's web site and update, as required	CCO
Review critical third party assurances or disaster plans or plan summaries: <ul style="list-style-type: none"> • At initial engagement of third party • Annually when CIM Securities's Plan is reviewed 	CCO
Contact FINRA to provide information about: <ul style="list-style-type: none"> • the activation or implementation of the BCP • if possible, written notification of emergency office locations • emergency contacts • requests for extension of deadlines to open inquiries, investigations, or upcoming filings and qualifications examinations or continuing education 	CCO

6.17.2 Retention And Location Of The Plan

Copies of the current and prior versions of the Business Continuity Plan are retained as follows. Copies are dated as of the effective date of the version of the Plan.

- Prior versions (including approvals) are retained by Compliance.

6.17.3 Implementation Of The Plan

The Plan has been designed to be implemented in the event of a disaster that results in a significant business disruption. Whether all or only parts of the Plan are implemented depends on the nature of the disruption. Generally, a significant business disruption would include:

- Destruction of one of CIM Securities's offices or facilities, whether by natural causes or by other means
- Loss of life or major injuries to personnel in an office location that disables that office's ability to conduct business
- Disruption of service from a critical service provider
- Disruption of service due to wide-ranging regional outages such as a power outage
- Disruption of service due to a pandemic

6.17.4 Emergency Response Team

CIM Securities has designated an Emergency Response Team (CEO or equivalent and CCO) that are responsible for implementing necessary procedures included in this Plan. The Response Team's action will depend on the nature and scope of the disruption. The "first responder" has the primary responsibility for taking action, and the "secondary responder" acts as a back-up in the event the first responder is unable to act. Where feasible, the two responders are located in different office locations.

6.17.5 Emergency Contact List

CIM Securities has established an Emergency Contact List that includes the names, phone numbers (cell and land lines), e-mail addresses, and other contact information for individuals critical to CIM Securities's business including key employees, key vendors or service providers, regulators, insurance carriers, banks, attorneys, and other key contacts. A copy of the List is provided to each member of the Response Team and other key personnel. This list will be reviewed and updated on at least an annual basis.

6.17.6 Alternative Business Locations

In the event employees can no longer conduct business at one of CIM Securities's office locations, the following actions may be taken:

- Transfer employees to the closest unaffected office location and notify personnel
- Transfer critical systems to another office or a back-up firm or system
- Transfer business operations to another CIM Securities office unaffected by the disruption
- Transfer business operations to a different broker-dealer or other entity

Considerations that will be made include:

- Geographic diversity in the event of regional service outages
- Accessibility of alternative sites and the ability of employees to travel to the site and methods of relocating employees and living arrangements, if needed
- Number and composition of staff needed and supervisors for alternative sites
- Generator and other back-up sources at alternative sites
- Resources needed at alternative sites (desks, chairs, telephones, equipment, and supplies, *etc.*)
- Moving staff in advance of a significant BCP event, if it can be anticipated
- Whether employees should work from home and what resources they would need

6.17.7 Data Back-Up And Recovery

CIM Securities maintains its books and records in both hard copy and electronic format. The BCP indicates whether records are maintained in hard copy or electronic form; location of primary records; and back-up site for records.

In the event of an internal or external significant business disruption that causes the loss of CIM Securities's records (whether hard copy or electronic records), back-up records will be recovered from the back-up site.

6.17.7.1 Clearing Firm Back-Up And Recovery (Not applicable at Present)

If applicable, the clearing firm maintains records for CIM Securities under the terms of the clearing agreement. The clearing firm has developed a disaster and recovery plan to recover and retrieve records lost in a disaster affecting CIM Securities and/or the clearing firm. Records retained by the clearing firm are included on CIM Securities's Books and Records chart.

CIM Securities has received assurance from the clearing firm that its plan is consistent with SRO rule requirements and provides adequate protection of customer funds and securities held on behalf of CIM Securities customers and back-up and recovery systems for records retained by the clearing firm. Compliance (or another person designated to review critical third party plans) will review the clearing firm plan or a summary of the plan at least annually when CIM Securities's Plan is reviewed.

6.17.8 Mission Critical Systems

Mission critical systems are systems that are necessary to ensure prompt and accurate processing of securities transactions including order taking, entry, execution, comparison, allocation, clearance and settlement, maintaining customer accounts, and providing access to customer funds and securities.

The Mission Critical Systems identifies systems (or generally describes procedures) that are critical to the operation of CIM Securities's business; identifies third parties that provide those systems; and potential alternate procedures or systems for handling these critical functions in the case of a disruption.

6.17.9 Financial And Operational Assessments

The following describes procedures for assessing changes in operational, financial, and credit risk exposures in the event of a significant business disruption.

6.17.9.1 Operational Risk

In the event of a significant business disruption, alternative systems will be implemented to communicate with customers, employees, critical business constituents (banks, counter-parties, *etc.*), regulators, and other key parties depending on the nature and impact of the disruption

6.17.9.2 Financial And Credit Risk

In the event of a significant business disruption, CIM Securities's financial status will be evaluated to determine the need for additional financing or identify capital deficiencies including the following:

- Review the impact of the disruption on CIM Securities's ability to conduct business
- Identify inability to satisfy obligations with counter-parties
- Contact banks or other counter-parties to secure needed additional financing
- Notify regulators of capital deficiencies
- Reduce or cease business as may be required due to capital deficiencies or inability to conduct business
- Transfer business to other financial institutions until CIM Securities may resume conducting business

6.17.10 Alternative Market Entry

CIM Securities may use its clearing firm (if applicable) or other broker-dealers as alternative market entry points when CIM Securities cannot access markets through its own systems.

6.17.11 Alternative Communications

CIM Securities may use a wide range of communication systems to communicate with its customers, employees, counter-parties, and regulators including telephone; mail; fax; e-mail; vendor systems (such as Bloomberg); and personal meetings. CIM Securities may establish contracts with multiple telecommunications carriers to provide redundant systems and devices and to provide key employees with technology at remote locations, including home locations. Procedures for instituting alternative communications in the event of a significant business disruption include the following, depending on the nature of the disruption:

- Identify the most expedient remaining means of communication
- Notify employees if an off-site command center has been activated
- Notify employees of alternative communication systems to be used
- Transfer communications to another firm

Determination of what communication system will be used depends on the nature of the disruption and which communication systems (electronic mail, telephone calls, etc.) are functional and the availability of personnel in the event telephone contact is necessary.

6.17.11.1 Between Customers And The Firm

In the event of a significant business disruption that disables communications systems, alternative system procedures will be implemented, including the following:

- Identify the most expedient remaining means of communication
- Notify employees regarding how to contact customers
- Contact customers about how to enter orders, how to access accounts and account assets, and other alternative business operations

6.17.11.2 Between The Firm And Its Employees

In addition to the above, CIM Securities has developed a system to enable senior management to contact employees in the event of an emergency. The system may include, depending on geographic dispersion of employees:

- "Call trees" that provide contact initiated at senior management level and pyramiding down to reach affected personnel

6.17.11.3 Between The Firm And Trading Counterparties

Communications between CIM Securities and its trading counterparties regarding conduct of business will be implemented by alternative systems which may include:

- Via a clearing or other alternative business partner
- Phone
- Electronic communications
- Web site postings
- Other alternative means of communicating

6.17.11.4 Firm's Web Site

CIM Securities has established an alternative means of maintaining its web site in the event servers and other systems regularly used are unavailable. The web site will be used to communicate information to customers, counterparties, and others needing access to CIM Securities. It will include information about operations and contact information, including contact information at a clearing firm or other alternative business partner.

6.17.11.5 Between The Firm And Regulators

Communications with regulators will be conducted using the most expedient available communication system. The designated Response Team person will contact regulators regarding any major business disruption and plans for continuing business.

6.17.12 Regulatory Reporting

In the event of a significant business disruption affecting offices responsible for regulatory reporting, regulators will be contacted to determine which means of filing are available under the circumstances to meet filing requirements. In the event CIM Securities cannot contact regulators, required reports will be filed using communications means available.

6.17.13 Business Constituent, Bank, And Counter-Party Impact

This section describes business continuity procedures regarding third parties that are critical to the conduct of CIM Securities's business. In most instances, contracts with critical third parties will include assurances regarding the third party's disaster recovery plans. A disruption impacting CIM Securities's ability to conduct business may occur either at CIM Securities itself or at the third party.

6.17.13.1 Business Constituents

- Determine whether the third party is able to continue providing critical services.
- If not, identify and contact an alternate third party to provide services.

6.17.13.2 Banks And Other Financial Institutions

- Determine whether the bank/financial institution is able to continue providing financing.
- If not, identify and secure alternative financing.

6.17.13.3 Critical Counter-Parties

- Determine whether transactions may be completed with counter-parties.
- If not, contact counter-parties directly (or CIM Securities's clearing firm, if business is introduced) to make alternative arrangements to complete transactions.

6.17.14 Other Obligations To Customers

6.17.14.1 Accepting Customer Orders

In the event CIM Securities's systems for accepting customer orders are disrupted, alternative systems will be communicated to customers and to employees including, where appropriate:

- Accepting orders by telephone or other alternative means
- Communicating orders to trading desks (internal or external) or order execution systems by telephone or other alternative means

6.17.14.2 Prompt Access To Funds And Securities

When customer access to funds and securities is impacted by a significant business disruption, customers will be notified by whatever expedient means is available (telephone, e-mail, *etc.*) regarding who may be contacted to request funds or securities. If CIM Securities is unable to continue business operations, customers will be notified of an alternative financial institution where they may conduct business and access their funds and securities.

6.17.14.2.1 SIPC Liquidation

In the event SIPC liquidation of CIM Securities's business is required, designated personnel will work with the SIPC-appointed trustee to wind down CIM Securities's operations and transfer customer funds and securities.

6.17.14.3 Disclosure Of Business Continuity Plan

[FINRA Rule 4370(e)]

Information about CIM Securities's Business Continuity Plan is provided to customers as follows:

- At the time of account opening
- On CIM Securities's web site
- Upon request, by mail

6.17.15 Emergency Contact Information

[FINRA Rule 4370 and 4517]

CIM Securities has provided FINRA with the names of two emergency contact persons, one who must be a registered principal and member of senior management and a second who may be unregistered (such as CIM Securities's attorney, accountant, or a clearing firm contact) and who has knowledge of CIM Securities's business.

Emergency contact information will be promptly updated, when necessary. Contact information will be reviewed by Compliance (or someone else designated) within 17 business days of the end of each calendar year and a written record of the review will be retained.

6.17.16 Widespread Health Emergencies

[Federal government Business Pandemic Influenza Planning Checklist: <http://www.pandemicflu.gov/plan/pdf/businesschecklist.pdf>; FINRA Regulatory Notice 20-16, 20-08 and 09-59; FINRA Information Notice 3/26/20 Cybersecurity Alert]

A widespread pandemic or any biologically based threat could have significant impact on the ability of CIM Securities to continue conducting business. This section outlines the steps CIM Securities has taken and will take in the event of a widespread pandemic.

6.17.16.1 Preparatory Steps

- Document government resources for information about a pending pandemic
- Engage cybersecurity procedures (see the chapter: *CYBERSECURITY*)
- Identify and document an alternative firm or firms to handle CIM Securities's business for extended periods of time
- Identify and document medical resources to assist employees, including administering vaccinations or other medications
- Stock antibacterial and other hygiene products for use by employees
- Identify alternative work sites
- Identify employees who can telecommute and establish a list of those employees and what computers and technology will be necessary
- Establish supervisory procedures to oversee employees who will telecommute or are relocated to an alternative site

6.17.16.2 Action If A Pandemic Occurs

The following procedures will be followed in the event of a threatened health emergency.

1. The Emergency Response Team will meet to determine the potential seriousness of the threat and what action to be taken as the threat escalates.
2. Determine whether employees should work remotely (see the following section).
3. Notify employees of:
 - available vaccinations or other medication and whether they are mandated
 - necessary conduct such as avoiding personal contact such as handshaking
 - access to antibacterial or other hygiene products to reduce infections and transmission of communicable diseases
 - requirement to stay home and telecommute

- transfer of business/functions to other firms
- contact list of key personnel
- 4. Restrict access to CIM Securities by outsiders (customers, vendors, *etc.*).
- 5. The Emergency Response Team will meet or communicate regularly to determine steps to be taken.

6.17.16.3 Remote Work

If CIM Securities decides that employees will work remotely, procedures include the following:

- Provide back-up contact information and redirect phone lines to facilitate customer communications
- Ask remote staff to report their location to their supervisors, requiring approval prior to making changes to location
- Provide additional support and communication to staff which may include firm-wide calls and video conferences to provide updates; virtual training; communicating clear guidance about firm expectations; provide additional technology tools, if necessary, for remote workers; provide digital collaboration platforms and applications; and disseminate additional guidance and training regarding technology, tools and services in a remote work environment
- Reminding staff about confidentiality of firm and customer information and cybersecurity and fraud risks

6.17.17 Education Of Employees

The Business Continuity Plan is communicated to employees as follows:

- A summary is included in the chapter *GENERAL EMPLOYEE POLICIES* in the section *Emergency Business Recovery Procedures* and is provided to all employees.
- A current copy of the Plan is provided to the Emergency Response Team and key employees with responsibilities for aspects of the Plan. When changes are made to the Plan, new copies will be distributed to these employees.
- The most recent Emergency Contact List is provided to key employees.
- The BCP is included in training of employees.

6.17.18 Updating, Annual Review, And Testing

The Plan will be reviewed on at least an annual basis and revised as needed. Each revision will be approved by the designated senior manager and copies of the revised Plan distributed to the Emergency Response Team and key employees. Some material events require updating the Plan when they occur, including:

- Material changes to CIM Securities's business
- A change in CIM Securities's main office location
- Added office locations
- A change in a major service provider

When the Plan is reviewed, the procedures and accompanying lists and charts will be reviewed and updated as needed including the:

- Plan itself
- Emergency Response Team list
- Emergency Contact List
- Books and Records

- Mission Critical Systems
- Business Constituent, Bank, and Counter-Party
- *Designation Of Offices* section of the chapter *DESIGNATION OF SUPERVISORS AND OFFICES*
- Any other information related to the Plan

When appropriate, CIM Securities will participate in industry-wide testing programs. A written record of the annual review including the date reviewed and name and signature of the reviewer will be retained by Compliance.

6.18 Industry Testing

[Exchange Act Regulation SCI; FINRA Rule 4380; MSRB Rule A-18]

Regulators designate certain firms to participate in industry-wide business continuity/disaster recovery testing. Testing is conducted once a year; firms are notified that they are required to participate. Firms may also participate on a voluntary basis by submitting a request to FINRA.

The CEO or equivalent (or other designated supervisor) is responsible for complying with mandatory testing or designating someone to oversee the testing within the timeframes established by FINRA. Firms are expected to fulfill certain testing requirements which could include, for example, bringing up systems on the designated testing day and processing test scripts to simulate trading activity. Firms may also have to report test results or provide other reports to FINRA.

Records of testing conducted and information provided to FINRA will be retained by the CEO or equivalent. Anomalies identified during testing will be reviewed and corrected and records retained, if applicable.

6.19 Customer Payments For Purchases

When an order to purchase securities is accepted from a customer, payment from the customer's bank account or other depository must be authorized in writing by the customer. Payment is not acceptable based only on the customer's oral authorization to withdraw funds. Examples of acceptable payment include:

- a check signed by the customer
- written authorization by the customer to draft funds from the customer's bank checking or savings account

Questions regarding proper payments should be referred to Operations or Compliance.

6.19.1 Checks Payable To Clearing Firm

If applicable, all checks provided by customers must be made payable to CIM Securities's clearing firm only. Questions regarding check requirements should be referred to supervising principals.

6.19.2 Guaranteed Accounts – Not applicable at present

A customer (the "guarantor") may provide a written guarantee to cover the margin calls in another account (the "guaranteed" account) using the equity in the guarantor's account. Written agreements for such guarantees must be provided to Operations.

RRs are prohibited from guaranteeing payment in another customer's account (unless the other customer is an employee-related account and approval has been obtained from Operations).

6.20 Transmittals Of Customer Funds And Securities

If applicable, this section describes CIM Securities's procedures for transmitting funds or securities from customer accounts.

The following summarizes requirements:

- All transfers require written letters of authorization (LOAs) when funds and/or securities will be transmitted to a third party. LOAs may be received by mail, fax, delivery, or other means including electronic transmission that provides for written authorization with the customer's verifiable signature.
- LOAs will be forwarded to the clearing firm.
- Copies of LOAs are retained in the Firm's records.
- Suspicious or questionable activity must be brought to the attention of the AML Compliance Officer who is responsible for determining whether a Suspicious Activity Report must be filed.

6.20.1 Checking Account Safeguards

The following procedures must be followed to safeguard the use of checks, as applicable:

- Blank checks and check registers must be kept in a secured operations area or locked location with access limited only to authorized personnel.
- At the end of the business day, all blank checks must be locked in a safe or similarly secured area.
- If using a clearing firm's account:
 - Approval must be obtained from the clearing firm prior to writing a check, and approval noted in records retained for checks issued.
 - Transmit to the clearing firm, by the end of the business day, information regarding checks issued that day
- If a clearing firm issues all checks, promptly transmit the customer's request for issuance of a check or sending of securities
- Checks must be used in numerical sequence.
- CIM Securities maintains a list of authorized check signers. Each business location that issues customer checks must have at least 2 designated check signers.
- Checks **must not** be signed in blank, in anticipation of a check signer's absence. The manager of Operations must be contacted if alternate arrangements are necessary in the absence of an authorized check signer.
- When an employee will personally deliver a customer check, the procedures outlined in the section *Transmittals Between Customers And Registered Representatives* must be followed.

6.20.2 Prepayments And Extensions

Prepayments (customer requests payment prior to settlement date on a sale) or extensions of time to make payment must be approved by the designated supervisor.

6.20.3 Employees Authorized To Transmit Customer Assets From Accounts

As applicable, employees who are authorized to release customer funds and/or securities include:

- Authorized senior principals who transmit instructions to a clearing firm (if applicable)
- Authorized senior principals who issue checks (if applicable)

6.20.4 Issuing Checks To Customers

If applicable, checks to be paid to customers from their accounts will be paid to the order of the account as it is carried on CIM Securities's books and sent to the address appearing on the account. Exceptions require written authorization by the customer. When checks are to be issued to a third party or funds are transferred to a third party, the following procedures apply.

6.20.5 Persons Receiving Assets In Person

When someone appears in person to receive assets, a photo ID will be required before the assets are released. The person releasing assets is required to note on CIM Securities's records the type of ID presented and the number (driver's license, passport, *etc.*). If an authorized third party under an LOA is receiving assets, the LOA will be verified before assets are released.

6.20.6 Transmittals To Third Parties

When a customer wishes funds or securities to be paid to a third party in the third party's name, the customer will be required to provide a signed LOA that specifies to whom the funds are to be paid.

When funds are disbursed, CIM Securities (or its clearing firm, if applicable) will send a notice to the customer confirming that funds were sent to a third party from the customer's account.

6.20.6.1 Letters Of Authorization

A Letter of Authorization (LOA) is an important required document whenever a customer asks that funds or securities are to be sent to a third party out of the customer's account. LOAs are an important record for CIM Securities, both to ensure the customer's instructions are followed and to ensure CIM Securities has a written record in the event there is a question in the future about disbursements from an account.

6.20.6.1.1 LOA Instructions

RRs or their assistants are responsible for obtaining completed LOAs, when necessary.

- A completed LOA is required **prior to** disbursements to third parties.
- All blanks must be completed on the LOA.
- The customer's original signature is required. In the case of a joint account, all joint owners must sign the LOA. For corporations, trust accounts, and other accounts, the authorized person must sign the LOA.
- Completed LOAs are submitted to Operations and should accompany the request to disburse funds or send securities to a third party.

6.20.6.2 Email Instructions

[FINRA Regulatory Notice 12-05]

Email and other electronic communications can be subject to intrusion and compromised by a third party. There have been instances of third parties sending fraudulent requests to broker-dealers to transfer customer funds to an account for the benefit of the third party. To prevent theft from customer accounts, the following apply to email or other electronic requests to transfer funds to a third party:

- The customer will be contacted by phone, mail, or another means independent of the email account to verify the accuracy of the instructions.
- The RR, assistant, or operations person receiving instructions should be aware of "red flags" (e.g., funds to be transferred to an unfamiliar third party, particularly in a foreign country; transfers that appear to be out of the ordinary for the customer; and requests that indicate urgency or otherwise appear designed to deter verification of transfer instructions).
- If CIM Securities processes its transactions through a clearing firm, the clearing firm will have its own procedures to prevent unauthorized third party transmittals.
- The Operations Manager or Compliance should be contacted with any questions about questionable transfer instructions.

6.20.7 Authorization Records For Negotiable Instruments Drawn From A Customers Account – If Applicable

[FINRA Rule 4514]

The customer's written signature is required whenever CIM Securities obtains or submits for payment a check, draft, or other form of negotiable paper drawn on a customer's checking, savings, share or similar account; this may include the customer's signature on the negotiable instrument. Written authorization separate from the instrument must be retained for 3 years following the date the authorization expires. No record is required when the customer signs the instrument (*i.e.*, a check).

6.20.8 Transmittals To An Alternate Address

Funds and securities will be sent to the customer's address of record, unless the customer provides **written** authorization to use an alternative address.

6.20.9 Transmittals To Outside Entities

Customers sometimes request the transfer of funds or securities in their accounts to a bank or other entity on their behalf. A signed LOA must be obtained to effect such a transfer including the customer's account number at the receiving bank or other entity.

6.20.10 Transmittals Between Customers And Registered Representatives

If applicable, on occasion, a customer may request that the RR or other CIM Securities employee personally deliver a check to the customer. This is permitted under the following conditions:

- The designated supervisor must approve the check delivery. The designated supervisor should initial a record maintained by Operations.

- A same-day confirmation (letter) will be sent to the customer confirming that a check was delivered and inviting the customer to call if there are any questions.

6.20.11 Suspicious Or Questionable Activities

Employees are responsible for referring suspicious or questionable activities to their designated supervisor. If the activity involves the designated supervisor, the employee should bring the activity to the attention of the Compliance Officer. If the Compliance Officer is involved, the activity should be brought to the attention of someone else in senior management. Such activities may include transfers without required authorizations; failure to obtain secondary approvals where required; a pattern of transfers that have no reasonable business basis, or any other activity the employee considers suspicious.

6.21 Customer Protection

[SEC Securities Exchange Act of 1934 Rule 8c-1, Rule 15c2-1, Rule 15c3-3 and Rule 17a-13; SEC FAQs re customer financial responsibility rules: <https://www.sec.gov/divisions/marketreg/amendments-to-broker-dealer-financial-responsibility-rule-faq.htm>; FINRA Rule 1020; FINRA Rules and Guidance re FAQs re Rule 15c3-3 exemptions; NYSE Rule 402]

The procedures in this section generally outline some key requirements under Rule 15c3-3 and related regulations. The FINOP (or the clearing firm, if applicable) is responsible for developing detailed procedures for complying with SEC and SRO requirements.

6.21.1 Introduction

SEC Rule 15c3-3 specifies requirements for broker-dealers to protect customers' funds and securities. Two significant elements of the Rule are:

1. a formula for a cash reserve which restricts a broker-dealer from using customer funds and securities in their own business; and,
2. a requirement that brokers or dealers maintain and obtain physical possession or control, as defined in the Rule, of fully paid and excess margin securities.

6.21.2 Exemptions

Because of the nature of CIM Securities's business, CIM Securities qualifies for an exemption under Rule 15c3-3(k) or is a "Non-Covered Firm." The FINOP is responsible for determining that CIM Securities qualifies for one of the following exemptions.

6.21.2.1 Exemption Under (k)(1)

[Exchange Act Rule 15c3-3(k)(1)]

- i. CIM Securities' transactions as dealer (as principal for its own account) are limited to the purchase, sale, and redemption of redeemable securities of registered investment companies or of interests or participations in an insurance company separate account, whether or not registered as an investment company; except that where CIM Securities is transacting business as a sole proprietor may also effect

occasional transactions in other securities for its own account with or through another registered broker or dealer;

- ii. CIM Securities' transactions as broker (agent) are limited to:
 - a. The sale and redemption of redeemable securities of registered investment companies or of interests or participations in an insurance company separate account, whether or not registered as an investment company;
 - b. the solicitation of share accounts for savings and loan associations insured by an instrumentality of the United States; **and**
 - c. the sale of securities for the account of a customer to obtain funds for immediate reinvestment in redeemable securities of registered investment companies; and
- iii. CIM Securities promptly transmits all funds and delivers all securities received in connection with its activities as a broker or dealer, and does not otherwise hold funds or securities for, or owe money or securities to, customers.

6.21.2.2 Exemption Under (k)(2)(i) - Not at present

[SEC Securities Exchange Act of 1934 Rule 15c3-3(k)(2)(i)]

CIM Securities carries no margin accounts and promptly transmits customer funds and securities to its clearing firm. CIM Securities does not hold funds or securities from, or owe money or securities to, customers and effects all financial transactions between CIM Securities and its customers through one or more bank accounts, each designated as "Special Account for the Exclusive Benefit of Customers of the Firm."

6.21.2.3 Exemption Under (k)(2)(ii) – Not at present

[SEC Securities Exchange Act of 1934 Rule 15c3-3(k)(2)(ii)]

CIM Securities clears all transactions with and for customers on a fully disclosed basis with its clearing firm which carries all of CIM Securities's customer accounts and maintains books and records related to carrying the accounts. CIM Securities promptly transmits customer funds or securities to its clearing firm.

6.21.2.4 Exemption As A Non-Covered Firm

[<https://www.sec.gov/divisions/marketreg/amendments-to-broker-dealer-financial-responsibility-rule-faq.htm>]

As a "Non-Covered Firm" CIM Securities is not required to make a daily possession or control determination because the requirement applies only to broker-dealers that carry accounts of or for customers. CIM Securities is also not required to make the customer reserve or PAB reserve computations because CIM Securities is only required to make these computations to the extent it has amounts required to be deposited in the customer reserve account or the PAB reserve account.

CIM Securities will update its FINRA membership agreement when it adopts the Non-Covered Firm exemption. When filing its FOCUS Report CIM Securities may include a statement that "The firm has no possession or control obligations under SEA Rule 15c3-3(b) or reserve deposit obligations under SEA Rule 15c3-3(e) because its business is limited to [*list of activities*]."

6.21.2.5 Prompt Transmission Of Customer Funds And Securities – If applicable

[SEC No-Action Letter dated March 12, 2015 to NYLIFE Securities: <http://www.sec.gov/divisions/marketreg/mr-noaction/2015/nylife-securities-031215-15c3.pdf>]

One of the requirements for an exemption under 15c3-3(k) is the prompt transmission of funds and securities. The following outlines the requirements as they apply to different securities.

1. For checks payable to an insurance company for the purchase of a deferred variable annuity product, prompt transmission is no later than 7 business days after an OSJ receives a complete and correct application package for review by the principal. (Refer to the chapter *INSURANCE PRODUCTS* for more requirements regarding variable annuities.)
2. When an RR recommends the sale of a security on a subscription-way basis:
 - a. Promptly prepare and forward a complete and correct application package to an OSJ;
 - b. Perform a suitability review and approval (or disapproval) by a registered principal within 7 business days after receipt of a complete and correct package at the OSJ;
 - c. Transmit the check to the issuer no later than noon of the business day following the date the registered principal reviews and approves;
 - d. Return the package and the check to the RR if the transaction is disapproved;
 - e. Maintain a record of the check, when received, date transmitted to the issuer if approved, or date returned to the customer if disapproved;
 - f. Customers will be notified of CIM Securities's process for handling customer checks payable to issuers for subscription-way securities transactions before such transactions. Notice may be included in customer statements or another form of notice.
3. For all other securities, prompt transmission of a check to the clearing firm is defined as no later than noon of the next business day after received.

6.21.2.6 Inadvertent Receipt Of Customer Funds Or Securities

CIM Securities does not hold funds or securities for, or owe money or securities to, its customers. In the event that funds or securities are inadvertently received by CIM Securities, an entry will be made in a log maintained for that purpose recording the date, the amount, and, in the case of securities, a description of the securities received, and the action taken to return such funds or securities to their rightful owner.

No later than the next business day, CIM Securities will return the funds or securities to the sender. If the sender cannot be immediately determined, CIM Securities will open a separate bank account, to be designated as "Special Account for the Exclusive Benefit of the Owner of Funds and Securities," into which the funds or securities will be deposited and held until the rightful owner has been identified.

6.22 Customer Confirmations And Statements - Not applicable at Present

[FINRA Rule 2231 and 2232]

This section describes requirements regarding confirmations and statements.

6.22.1 Confirmations – Not applicable at Present

[Exchange Act Rule 10b-10 and 15g-3; FINRA Rule 2231 and 2232; MSRB Rule G-15]

Confirmations are issued for every trade executed for a customer and include required information, some of which is listed below. This section does not duplicate applicable rules which should be referenced for details.

- SEC Rule 10b-10 and 15g-3, FINRA Rule 2132, and MSRB Rule G-15 include details of required disclosures on customer confirmations

- Transaction information includes (among other information) the name of the security; quantity; price; markups/markdowns the time of execution (in minutes and seconds); the firm's role (agent, principal, riskless principal)
- Other types of disclosures (among others) include:
 - non-rated taxable debt securities (other than U.S. government securities) including a statement that rating information is based on a good faith inquiry of selected sources
 - control relationship with the issuer
 - call features
 - for principal transactions, the reported trade price, the net price to the customer, and the difference between the reported price and the price to the customer, the difference between the reported price and the customer's price (markup/markdown)
 - for municipal securities call features, primary revenue source for revenue bonds, securities sold as "original issue discount" (OID) bonds, yield information
 - for penny stocks bid or offer, compensation, and other disclosures (see Rule 15g-3 and the section *Penny Stocks* in the chapter *ORDERS*)
 - payment for order flow
 - Markups/markdowns in municipal securities for non-institutional customers (MSRB Rule G-15) (See the section *Mark-ups And Mark-Downs* in the chapter *MUNICIPAL SECURITIES*)

6.22.2 Customer Statements Only Are Provided To Customers – Not applicable at Present

[FINRA Regulatory Notice 10-19]

RRs are not permitted to create supplemental customer statements or reports for the purpose of consolidating investments not shown on customer monthly statements issued by CIM Securities. The customer monthly statement provided by CIM Securities is the only record to be provided to customers.

6.22.3 Control Of Blank Confirmations And Statements – Not applicable at Present

Blank confirmations and statements are to be retained in a secured location. Only authorized employees are permitted access to blank documents. The FINOP will establish procedures for control of these documents.

6.22.4 Undeliverable Mail

As applicable, if customer mail is returned to CIM Securities as undeliverable, A supervising principal will contact the RR's supervisor to obtain an updated address. When a new address is provided, the customer will be sent a letter at the new address asking for signed confirmation that the new address is correct. When the letter is returned, the customer's signature will be compared to other account documents on file. Signature anomalies will be referred to Compliance for follow up. If the customer fails to return the form, a second letter will be sent notifying the customer his or her account will be frozen unless an affirmation is received.

If a corrected address is not provided, the account will be frozen to preclude securities or money transactions (other than expiration of options or similar passive transactions) until a correct address is provided.

6.22.5 Holding Customer Mail Prohibited

CIM Securities will not hold mail on a customer's behalf, even for a short duration. RRs are **not** permitted to hold customer mail. A customer, who cannot receive mail at the address established on the account, must be instructed to provide a third party mailing address that is not related to CIM Securities or any associate of CIM Securities.

6.23 Lost Securityholders And Unresponsive Payees – Not applicable at Present

[SEC Securities Exchange Act of 1934 Rule 17Ad-17]

CIM Securities (and/or its clearing firm, if applicable) is required to search for holders of securities with whom it has lost contact and to provide notifications to persons who have not negotiated checks that have been sent to them. "Lost securityholders" are customers to whom any correspondence was sent and returned as undeliverable and for whom an updated address has not been received or is not obtainable from the customer. **The requirement does not apply when the securityholder is not a natural person.**

6.23.1 Searches For Lost Securityholders

Searches will be conducted through an information database service that contains addresses for the entire U.S. including the names of at least 50% of the U.S. adult population, is indexed by taxpayer ID number or name and is updated at least four times a year. The search will be conducted by taxpayer ID number or, if that search is not likely to locate the person, by name. Securityholders will not be charged for searches.

Searches will be conducted between three and twelve months from the later of:

- the date upon which correspondence is returned as undeliverable or
- if returned correspondence is re-sent within one month from the date it was returned and is again returned as undeliverable, the date on which the re-sent item is returned as undeliverable.

A second search will be conducted between six and twelve months after the first search.

Searches will not be conducted when (i) CIM Securities receives documentation the securityholder is deceased or (ii) the total value of assets in the account is less than \$25.

6.23.2 Unnegotiated Checks

Written notice will be provided to customers who do not negotiate checks sent to them within 6 months of sending. This does not apply to checks worth less than \$25.

6.24 Subordination Agreements With Investors

[SEC Securities Exchange Act of 1934 Appendix D to Rule 15c3-1; FINRA Notice to Members 02-32 and 02-04; FINRA web site: <https://www.finra.org/filing-reporting/regulatory-filing-systems/subordination-agreements>]

If CIM Securities enters into a subordination agreement with an investor, it will provide the investor with a copy of FINRA Subordination Agreement Investor Disclosure Document and obtain the investor's signature on a copy of

the Document. A copy of the signed Disclosure Document will be submitted to FINRA with the subordination agreement, for approval.

The FINOP is responsible for obtaining and submitting the required documents for subordination agreements.

6.25 Expense-Sharing Agreements

[SEC Letter July 11, 2003 to FINRA and NYSE Regarding Recording Certain Broker-Dealer Expenses And Liabilities; FINRA Notice to Members 03-63]

The SEC specifies requirements for incorporating an expense-sharing agreement into a broker-dealer's operations and how these agreements are recorded in the broker-dealer's financial records. The FINOP is responsible for ensuring CIM Securities complies with the SEC's guidelines if it enters into any such agreements.

In addition, the FINOP is responsible for notifying CIM Securities's Designated Examining Authority (DEA) if it enters into an expense-sharing agreement and does not record each of the expenses it incurs relating to its business on the reports it is required to file with the SEC or with the DEA. The notice will include the date of the agreement and the names of the parties to the agreement; a copy of the agreement will be provided to the DEA upon request.

6.26 Electronic Delivery And Signatures

[Electronic Records and Signatures in Global and National Commerce Act; SEC Release No. 34-42728; SEC Interpretive Release No. 33-7233, 33-7856 and 33-36345; NASD Notice to Members 98-3; NASD Regulatory and Compliance Alert March 1998; SIA Legal Alert 00-12]

Federal securities law through the Electronic Signatures in Global and National Commerce Act of 2000 regulates the use of electronic media for transmitting documents and the recording and accepting of electronic signatures. This section outlines requirements when CIM Securities uses electronic methods of delivery between CIM Securities and its customers and the use of electronic signatures for internal purposes such as approval of new accounts.

6.26.1 Electronic Delivery To Customers

[SEC Release No. 34-42728]

If CIM Securities electronically transmits documents to customers and/or accepts electronic signatures from customers, the following requirements will apply:

- The customer's consent will be obtained.
- Notice will be provided to customers that the information is available electronically.
- Customers who are provided electronic delivery have access to the information substantially equivalent to the access that would be provided if the information were delivered in paper form (*i.e.*, the electronically transmitted document will convey all material and required information). Customers will have ready access to the electronic document either through downloading or ongoing access online.
- CIM Securities will evidence satisfactory delivery through the customer's informed consent agreeing to delivery of certain documents or obtaining actual confirmation the customer received the information.
- Electronic delivery is subject to CIM Securities's policies and procedures to protect confidential customer information and ongoing review of CIM Securities's security systems.

6.26.2 Electronic Signatures

[SEC Release No. 34-42728]

Electronic signatures may be used by designated supervisors to indicate approval/review of new accounts, orders, and other ongoing supervisory reviews. Supervisors will be assigned passwords which will be changed periodically to protect the security of the system.

6.26.3 FINRA Access

[SEC Release No. 34-42728]

As required by FINRA, FINRA and its staff will have access to downloading and printing of documents which will have appropriate references and cross-references for ready access. If batch process approval is used (as opposed to opening individual files for review/approval), the batch process will:

- Give regulators immediate access to required books and records
- Permit the examining staff to download and print hard copies of required books and records
- Be subject to CIM Securities's policies and procedures regarding protection of customer information
- Be accessible only to authorized principals with password-based security access

Only authorized personnel will have access to the e-signature system which is password protected with periodic updating of passwords. Any branch offices that access the e-signature system will be provided CIM Securities's policy on safeguarding electronic signatures.

6.27 Transfer Of Accounts – Not applicable at Present

For accounts introduced to a clearing firm, the clearing firm is responsible for timely transfer. For accounts held by CIM Securities where CIM Securities self-clears, the FINOP will establish procedures in CIM Securities's operations manual for the timely transfer of customer accounts to another broker-dealer.

6.28 Solicitation Of Proxies

[SEC Securities Exchange Act of 1934 Section 14]

RRs are not permitted to solicit proxies from customers. Federal securities rules prohibit solicitation of proxies except in very limited situations. Questions should be referred to Compliance.

6.29 Customer Requests For References

Customers or prospective customers sometimes request letters of reference from broker-dealers regarding their accounts or future business to be done. Some of these requests in the past have been scams by unscrupulous individuals seeking to capitalize on a broker-dealer's good name. Any such requests should be referred to Compliance for handling.

6.30 Audit Letters

Auditors sometimes send letters asking CIM Securities to verify funds and securities on behalf of their customers who also have accounts with CIM Securities.

All requests should be forwarded to a supervising principal. In no instance should an RR or other branch personnel respond to these requests.

6.31 Annual Disclosure Of FINRA BrokerCheck

[FINRA Rule 2267]

As required by FINRA rule, at least annually customers will be provided with the following information in writing about FINRA BrokerCheck (formerly known as FINRA Public Disclosure Program):

- the hotline number
- the Web Site address
- a statement regarding the availability of an investor brochure regarding FINRA BrokerCheck

6.32 Carrying Agreements – Not applicable at Present

[FINRA Rule 4311; NASDAQ Rule 3230]

CIM Securities introduces its accounts and customer transactions to its carrying firm. CIM Securities has executed a carrying agreement consistent with regulators' requirements and will amend its carrying agreement when necessary. Any new carrying agreement or amendment will be submitted to its designated SRO for review and approval. A carrying agreement where accounts are carried on a fully disclosed basis will include the responsibilities of each party to the agreement as required by rule. Accounts introduced on a fully disclosed basis will be notified in writing at the opening of the account of the existence of the carrying agreement and the responsibilities allocated to the respective parties.

If CIM Securities has an agreement to act as an intermediary for another introducing firm ("piggybacking" arrangement), it will notify the carrying firm of the existence of the arrangement with the other introducing firm and disclose the identity of the firm. The carrying agreement will identify and bind every direct and indirect recipient of clearing services as a party to the agreement.

The FINOP is responsible for executing required carrying agreements; providing required notices; and retaining records.

6.33 Clearing Firm Exception Reports – Not applicable at Present

[FINRA Rule 4311(h); FINRA web site: <http://www.finra.org/Industry/Compliance/RegulatoryFilings/ClearingNotifications/index.htm>; NYSE Rule 382]

In compliance with SRO rules, CIM Securities's clearing firm is required to provide annual notice, by July 31 of each year, as follows:

- Notice to CIM Securities of:
 - exception reports available, and,
 - exception reports currently supplied to CIM Securities.

- A copy of this notice is forwarded to CIM Securities's designated examining authority or other appropriate regulator by the clearing firm.

When the list of available reports is received, Compliance will review the list and contact the clearing firm regarding changes to the list of reports currently received.

6.34 Short Interest Report

[FINRA Rule 4560; FINRA Regulatory Notice 16-32 and 12-38]

CIM Securities's clearing firm. If applicable, is responsible for filing required short interest reports.

6.35 Electronic Blue Sheets

[SEC Securities Exchange Act of 1934 Rule 17a-25; FINRA Regulatory Notice 12-47; FINRA Notice to Members 06-33 and 05-58; FINRA Electronic Blue Sheet FAQs: <https://www.finra.org/filing-reporting/electronic-blue-sheets-ebs/faq/>]

Regulators may request information regarding customer or CIM Securities transactions as part of their ongoing market surveillance activities. Information is transmitted electronically through FINRA's Regulatory Filings Application (RFA) Platform or the NYSE's Datatrak platform.

The FINOP is responsible for designating a person responsible for filing responses and retaining records of responses (or promptly forwarding requests to CIM Securities's clearing firm, if applicable, and retaining a record of forwarding).

6.36 Regulatory Fees And Assessments

[SEC Securities Exchange Act of 1934 Section 31; FINRA By-Laws Schedule A; FINRA Notice to Members 05-11 and 04-63]

The FINOP is responsible for paying fees and assessments required by regulators. A record of information reported and fees or assessments paid are retained in the FINOP's files.

6.37 Regulatory Requests

[FINRA Rule 8210]

Responsibility	<ul style="list-style-type: none"> • Compliance
Resources	<ul style="list-style-type: none"> • Regulatory requests received from regulators
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Process the inquiry including the following: <ul style="list-style-type: none"> ○ Record date of receipt ○ Flag due date in a log or other record ○ Assemble and review response ○ Encrypt responses prior to sending where required ○ Request and record any extension of due date, if necessary

	<ul style="list-style-type: none"> ○ Forward response, retaining a copy
Record	<ul style="list-style-type: none"> • Copy of request, response, and notations of when received, extensions, and when response was sent

Responses to regulatory requests may only be provided by authorized employees or departments such as Operations or Compliance. Requests received by employees other than those authorized must be referred to Compliance.

6.37.1 Information Provided Via Portable Media Device

[FINRA Regulatory Notice 10-59]

Information provided to FINRA by portable media device in response to requests under FINRA 8210 (Provision of Information and Testimony and Inspection and Copying of Books) will be encrypted using a method that meets industry standards for strong encryption. FINRA staff will be provided with the confidential process or key regarding the encryption in a communication separate from the encrypted information itself (separate email, fax, letter, *etc.*).

6.38 Outsourcing

[FINRA Regulatory Notice 21-29; FINRA Notice to Members 05-48]

Some services may be outsourced to third parties (vendors). While third parties are responsible for providing agreed-upon services in an accurate manner, regulators have stated that firms remain responsible for ultimate compliance with rules governing the outsourced activity ("covered activities") that, if performed by a firm, would be required to be the subject of a supervisory system and written supervisory procedures.

When choosing an outside vendor, a number of factors will be considered depending on the type of service provided. Factors that may be considered when engaging a third party include:

- Length of time in business
- Financial stability
- Prior knowledge of the vendor
- Other users of the vendor's services
- Technology and ability to deliver services
- Security of customer or other financial information, if applicable
- Vendor's cybersecurity controls
- Vendor's ability to retain firm records in accordance with regulatory requirements
- Who at CIM Securities is responsible for oversight and monitoring the vendor's services

6.38.1 Cybersecurity

CIM Securities will confirm that a vendor that will have access to customer and firm records has a viable cybersecurity program to protect such information and take corrective action when there are cybersecurity breaches. Cybersecurity considerations include:

- Review of a vendor's cybersecurity program and confirmation of continuing controls and technology changes to critical systems
- Testing of system changes and capacity to detect underlying malfunctions or capacity constraints
- Encryption of confidential firm and customer data stored at the vendor or in transit between CIM Securities and vendors
- Disposal of customer non-public information
- Retention or transfer of data upon termination of vendor agreement

6.38.2 Books And Records

CIM Securities's records are a critical part of any outsourced vendor agreement.

- Affirm the vendor will maintain books and records in accordance with Exchange Act Rules 17a-3, 17a-4, FINRA Rule 3110(b)(4), and FINRA Rule 4510.
- Confirm records will not be deleted upon termination of the vendor's contract with CIM Securities.
- Review vendor's recordkeeping in audit programs for compliance with regulatory requirements.

7 ANTI-MONEY LAUNDERING (AML) PROGRAM

[The Anti-Money Laundering Act of 2020: <https://www.fincen.gov/anti-money-laundering-act-2020>; FinCEN First National AML/CFT Priorities: <https://www.fincen.gov/news/releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements>; FINRA Rule 3310; FINRA Regulatory Notice 21-36; NASD Notice to Members 02-21; FINRA web site AML page <http://www.finra.org/RulesRegulation/IssueCenter/Anti-MoneyLaundering/index.htm>; FINRA 2022 Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>; Bank Secrecy Act; Office of Foreign Assets Control (OFAC) web site <http://www.treas.gov/offices/enforcement/ofac>; SEC web site AML page <http://www.sec.gov/spotlight/moneylaundering.htm>; SEC Anti-Money Laundering (AML) Source Tool: <http://www.sec.gov/about/offices/ocie/amlsourcetool.htm>; NASDAQ Rule 3011; SIFMA Anti-Money Laundering Resource Center: <http://www.sifma.org/issues/legal-compliance-and-administration/anti-money-laundering-compliance/resources/>; Regulatory Joint Statement on Digital Assets: <https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets>]

Note: Refer also to the Firm's AML Manual.

7.1 Introduction

This chapter explains CIM Securities's Anti-Money Laundering (AML) Program. An explanation of money laundering and guidance for all employees to detect money laundering is included in the chapter *GENERAL EMPLOYEE POLICIES* in the section *Money Laundering*.

Money laundering laws and rules include digital assets regardless of whether they meet the definition of a security or commodity. These policies will be updated and appropriate procedures and action effected when new rules are adopted.

7.1.1 Definitions

[Bank Secrecy Act 31 CFR Chapter X Part 1023.100 Subpart A]

Monetary instruments:

1. Currency;
2. Traveler's checks in any form;
3. All negotiable instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee (for the purposes of Section 103.23), or otherwise in such form that title thereto passes upon delivery;
4. Incomplete instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders) signed but with the payee's name omitted; and
5. Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.
6. Monetary instruments do not include warehouse receipts or bills of lading.

Digital assets: Instruments that may qualify under applicable U.S. laws as securities, commodities, or security- or commodity-based instruments such as futures contracts or swaps. There is no uniform legal definition, and digital assets have different labels such as cryptocurrencies, digital tokens, digital currencies, virtual assets, and initial coin offerings.

7.2 AML Compliance Officer

[FINRA Rule 3310(d) and 3310.02]

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer
Resources	<ul style="list-style-type: none"> • Computer reports and other programs developed for the Program • Internal audits or outside audits of the Program • Regulations and rules for broker-dealer anti-money laundering programs • OFAC web site • Other sites and resources available
Frequency	<ul style="list-style-type: none"> • Annual - review policies and procedures and business lines • Annual and more frequently, as needed - develop and schedule AML education for employees • As needed - update program and provide revisions to senior management for review and approval • As required: revise delegation of AML responsibilities • Annually - review AML contact information on file with FINRA • Ongoing - review new regulations • Ongoing - monitor activity including: <ul style="list-style-type: none"> ○ activity in micro-cap and penny stocks, particularly when transacted through omnibus accounts maintained for foreign financial institutions ○ accounts for foreign customers that appear to have been opened solely to trade in IPOs and post-IPO trading in shares issued by companies based in restricted markets such as China ○ due diligence with respect to SPAC sponsors and the appropriateness of disclosures in SPAC IPOs
Action	<ul style="list-style-type: none"> • Develop and update CIM Securities's anti-money laundering program • Obtain senior management approval for the program and any changes to the program • Identify delegation of AML responsibilities among persons/departments and escalation of red flags to those persons • Monitor (or designate monitoring) the activity of CIM Securities, its associated persons, and customers to reasonably detect and prevent money laundering activities • Consider AML implications of new business lines and products • Develop AML education program for employees and schedule training • File required reports • Retain required records • Provide contact information to FINRA and update contact information if necessary • Review policies and procedures and new areas of business and update AML Program as needed
Record	<ul style="list-style-type: none"> • Designation of AML Compliance Officer • Delegation of AML responsibilities and escalation procedures • Current and past copies of anti-money laundering program with senior management approval • Records of AML education including who attended, date of training, and material covered • Reports filed • Reviews of the AML Program • Other records to be retained, as listed in the Program

CIM Securities has designated an AML Compliance Officer who is responsible for developing policies, procedures, and internal controls reasonably designed to achieve compliance with AML rules and regulations.

7.3 Independent Testing

[FINRA Rule 3310.01]

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer
Resources	<ul style="list-style-type: none"> • Policies and procedures • Independent testing results
Frequency	<ul style="list-style-type: none"> • Annual or every two years - schedule, conduct, and follow up testing (unless the firm qualifies for testing every two years)
Action	<ul style="list-style-type: none"> • Identify person(s) to conduct testing • Conduct testing • Report results to CEO in annual compliance report • Revise policies and procedures as necessary • Conduct follow-up to determine corrective action has been taken
Record	<ul style="list-style-type: none"> • Independent testing results including who conducted and dates of review • Report to CEO • Record of changes to policies and procedures resulting from testing • Record of follow-up actions

The AML Compliance Officer will arrange for annually or every two years (on a calendar-year basis) independent testing of CIM Securities's policies and procedures regarding money laundering and the effectiveness of the program. The review is conducted by member personnel or a qualified outside party. More frequent reviews will be conducted, if necessary, as determined by the AML Compliance Officer.

Independent testing must be conducted by someone with a working knowledge of the Bank Secrecy Act and implementing regulation requirements. Independent testing may not be conducted by:

- A person who performs the functions being tested;
- The designated AML Compliance Officer; or
- A person who reports to a person described in the above two items.

7.4 Training Program

All employees are provided with CIM Securities's Money Laundering policy when they are hired. The policy is included in the chapter *GENERAL EMPLOYEE POLICIES*.

In addition, ongoing education will include the firm element continuing education program, periodic circulation of CIM Securities's policy, and other educational programs directed at specific employees such as operations personnel. Training will be delivered at least annually by video, intranet systems, in-person lectures, and other methods including third parties who deliver AML training.

Training will include the following, as well as other subjects identified by the AML Compliance Officer:

- How to identify red flags and signs of money laundering
- What to do once the risk is identified (how, when and to whom to escalate unusual customer activity or other red flags)
- Employees' roles in CIM Securities's compliance efforts and how to perform them
- CIM Securities's record retention policy
- Disciplinary consequences (including civil and criminal penalties) for non-compliance

The AML Compliance Officer is responsible for retaining records of employees trained, the dates of training, and the subjects included in training.

7.5 Bank Secrecy Act (BSA) Filings

[BSA E-Filing System: <http://bsaefiling.fincen.treas.gov/main.html>; FinCEN web site for Adobe forms: <https://www.fincen.gov/legal-reference-bank-secrecy-act-forms-and-filing-requirements>]

The BSA E-Filing System web site provides a list of forms supported for electronic filing, and include the following (refer to the web site for the most current list of forms):

- Currency Transaction Report (FinCEN Form 112)
- Designation of Exempt Person (FinCEN Form 110)
- Suspicious Activity Report by the Securities and Futures Industries (FinCEN Form 111)
- Report of Foreign Bank and Financial Accounts (Form 114)

7.6 OFAC List And Blocked Property

[Dept. of Treasury, various statutes; OFAC web site <http://www.treas.gov/offices/enforcement/ofac/>; Foreign Assets Control Regulations For The Securities Industry: <https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf>]

The property of sanctioned persons or entities will be blocked and transfer of assets prevented for persons or entities included on the OFAC list of blocked persons or entities. In addition, securities issued by sanctioned countries and other sanctioned issuers will be blocked. OFAC (the Office of Foreign Assets Control of the U.S. Treasury Department) enforces the sanctions and publishes, on its web site (www.treas.gov/ofac), information about sanctions. The information is divided into several categories including:

- Persons and entities subject to sanctions, *Special Designated Nationals and Blocked Persons* (SDN list)
- Persons and entities engaged in drug trafficking, *Specially Designated Narcotics Traffickers* (SDNTKs)
- Terrorists and terrorist organizations, *Specially Designated Terrorists* (SDTs)
- Countries, governments, and other entities subject to sanctions

OFAC requirements apply to all persons and entities under U.S. jurisdiction, including foreign branches of U.S. institutions. This also includes foreign institutions that operate in the U.S.

The term "OFAC list" in this section includes all sanctions published by OFAC even though the information may appear in multiple lists. CIM Securities relies on its clearing firm to monitor OFAC lists and block accounts and securities where appropriate and to file necessary reports.

7.6.1 Prohibited Transactions

CIM Securities is prohibited from conducting transactions in any account on behalf of a sanctioned party or in certain blocked securities. Securities and funds may not be released and securities transactions may not be executed. Securities and funds may be deposited to a blocked account, but no securities or funds will be released until the account is no longer subject to sanctions. Funds or securities may not be transferred to sanctioned parties.

Because transactions are prohibited, all open orders for a blocked account will be cancelled.

7.6.2 Risk Factors

[\[https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf\]](https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf)

Following are risk factors identified by OFAC that may warrant a heightened level of scrutiny.

International transactions, including wire transfers:

- a) High number of international transactions, cross-border transactions, or investments in a foreign investment fund or on a foreign exchange;
- b) Presence of overseas branches or multiple correspondent accounts with foreign financial institutions, including correspondent accounts subject to enhanced due diligence under Section 312 of the USA PATRIOT Act.

Foreign customers/accounts:

- a) A large, fluctuating client base across a number of foreign jurisdictions involving a large number of security transactions;
- b) Customers located in or having accounts in high-risk jurisdictions, such as countries found to be of "primary money laundering concern" pursuant to Section 311 of the USA PATRIOT Act;
- c) Customers located in or having accounts in countries that are havens for money laundering or are inadequately regulated, including countries identified by the Financial Action Task Force as maintaining an inadequate AML/CFT regime;
- d) Customers located in or having accounts in countries where local laws, regulations, or provisions (such as privacy laws) prevent or limit the collection of client identification information;
- e) Customers located in an offshore financial center as identified by the U.S. Department of State;
- f) Accounts for senior political or government officials ("politically exposed persons") of a foreign government;
- g) Accounts of closely held corporations;
- h) Accounts for unregistered or unregulated investment vehicles;
- i) Accounts for non-resident aliens;
- j) Accounts maintained at an offshore bank.

Foreign broker-dealers who are not subject to OFAC regulations:

- a) Lack of information regarding beneficial owners of securities; and
- b) Foreign broker-dealers that act as introducing brokers.

Risks of Investments in Foreign Securities:

Practical exposure increases when investing in a foreign investment fund or foreign exchange, because of the risk that the securities are issued by a sanctioned country or party or otherwise in violation of OFAC sanctions, e.g., securities of an issuer that provides financing for a sanctions target. Other risk factors include:

- a) Cross-border settlements involving the interaction of different settlement systems and laws in different countries;
- b) Foreign securities that may be more prone to misidentification in the course of a trade, e.g., similar names between two foreign issuers;
- c) Foreign companies that issue shares in bearer form.

Personal Investment Corporations or Personal Holding Companies:

Beneficial ownership by a non-U.S. person that maintains a private banking account with a U.S. financial institution.

Very High Net Worth Institutional Accounts, Hedge Funds, Funds of Hedge Funds and Other Alternative Investment Funds (Private Equity, Venture Capital Funds) and Intermediary Relationships:

- a) Lack of transparency regarding securities/investments and beneficial owners;
- b) U.S. hedge fund with an offshore related fund where beneficial owners are offshore investors; and
- c) Subscription funds that originate from or are routed through an account maintained at an offshore bank, or a bank organized or chartered in an inadequately supervised and poorly regulated jurisdiction, or a foreign shell bank.

Omnibus Accounts/Use of Intermediaries:

- a) Potential for the use of code names to invest funds in the United States on behalf of sanctions targets, concealing the identities of the beneficial owners;
- b) Accounts for intermediaries held in street name that trade on behalf of third parties, such as other broker-dealers, banks, and mutual funds; and
- c) Cross-border trades executed for unregulated investment vehicles, e.g., hedge funds, private equity funds, and other private pools of capital.

Third-Party Introduced Business:

Business introduced by an overseas bank, affiliate, or other investor based in high risk or inadequately regulated countries.

Confidential Accounts:

Private banking accounts established or maintained for non-U.S. persons or services, including financial and related services, to wealthy clients who use offshore accounts for tax avoidance purposes.

7.6.3 Blocking Requirements

Blocking requirements are generally triggered under the following circumstances:

- An account is opened for someone included on an OFAC list.
- The owner of an existing account is added to an OFAC list.
- A security is identified in a customer account where the issuer is the subject of sanctions.
- A request is made by a customer to pay or transfer funds or securities to a blocked person or entity.

While title to blocked property remains with the blocked person or entity, transactions affecting the property (including transfer of the assets) cannot be made without authorization from OFAC. Debits to blocked accounts are prohibited, but credits may be accepted. Cash balances in blocked accounts must earn interest at commercially reasonable rates. Blocked securities may not be paid, withdrawn, transferred (even in book transfer), endorsed, guaranteed, or otherwise dealt in.

It is not a violation to open an account for a blocked person. The violation occurs when the account is not frozen and assets are allowed to transfer out of the account. In addition, OFAC restrictions may vary depending on the blocked person or entity; details of blocking requirements are explained on the OFAC web site.

7.6.4 Monitoring Procedures

Monitoring is to be conducted as follows:

- Operations personnel should be aware of the countries included on the OFAC list, to watch for new accounts to be opened for or requests to transfer funds or securities to residents of those countries.
- CIM Securities (or a clearing firm or other third party) has procedures to monitor new accounts, existing accounts, security positions, and potential disbursements of funds or securities.

7.6.5 Other Requests To Monitor Accounts

Regulators or law enforcement agencies may ask the industry's cooperation in identifying accounts for individuals or entities under investigation or suspected of criminal activities.

The AML Compliance Officer is responsible for responding to such requests; providing the necessary information; and retaining records of requests, reviews conducted pursuant to requests, and information provided to authorities.

7.6.6 Blocking Property And Disbursements

Any blocked account will not be permitted to engage in transactions other than the acceptance of deposits of funds or securities. Open orders of blocked accounts will be cancelled.

Disbursements of funds or securities may not be made to sanctioned parties. CIM Securities (or a clearing firm) is responsible for monitoring requests for disbursements.

7.6.7 Reporting Blocked Property And Legal Actions

When an account or disbursement is blocked or a blocked security is identified, OFAC will be notified within 10 days of blocking. If CIM Securities blocks an account or security, it will file the necessary report with OFAC. Reports filed by CIM Securities will be retained in a file of blocked accounts or securities. Information to be reported includes:

- Owner or account party
- Property and property location
- Existing or new account number
- Actual or estimated value
- Date property was blocked
- Copy of the payment or transfer instructions
- Confirmation that funds have been deposited in a blocked account that is identified as blocked
- Name and phone number of contact person at CIM Securities

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of contact person at CIM Securities

7.6.7.1 Annual Report Of Blocked Property

On an annual basis by September 30th, Form TDF 90-22.50 will be filed with OFAC for any blocked property held as of June 30.

7.6.7.2 Legal Actions Involving Blocked Property

U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must provide notice to OFAC. Copies of all documents associated with the proceedings will be submitted by Compliance to the OFAC Chief Counsel at the U.S. Treasury Department within 10 days of their filing. In addition, information about the scheduling of any hearing or status conference will be faxed to the Chief Counsel.

7.6.8 Role Of Operations Personnel

Operations personnel are an important first line of defense in preventing transactions with sanctioned parties. The following guidance is provided to assist Operations personnel in identifying blocked parties. Any questioned accounts or transactions should be referred to Compliance.

- Be familiar with countries included on the OFAC list. These are countries considered potential havens for money laundering, drug trafficking, or terrorist activities. Information is included on the OFAC web site at www.treas.gov/ofac.
- When processing the opening of accounts, question accounts for residents of countries included on the OFAC list.
- Question requests to transfer funds or securities to residents or entities domiciled in any country included on the OFAC list.

7.7 Currency Reporting Requirements

[SEC Securities Exchange Act of 1934 Rule 17a-8; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart C]

The following summarizes the reporting requirements under the Bank Secrecy Act. CIM Securities's designated supervisor of Operations is responsible for maintaining records of any currency reports required to be filed by CIM Securities and retaining them for five years.

7.7.1 Transactions Involving Currency Over \$10,000

If CIM Securities accepts a currency deposit exceeding \$10,000, it is required to electronically file a Currency Transaction Report (CTR, Form 112) with the Financial Crimes Enforcement Network (FinCEN). Multiple transactions by the same person equaling over \$10,000 in any one day must also be reported.

"Currency" is defined as the coin and paper money of the U.S. or legal tender of other countries. Currency also includes U.S. silver certificates, U.S. notes, federal reserve notes, and official foreign bank notes customarily used and accepted as a medium of exchange in a foreign country. CTRs must be filed by the 15th calendar day after the day of the transaction and kept for 5 years.

7.7.2 Transactions Involving Currency Or Bearer Instruments Over \$10,000 Transferred Into Or Outside The U.S.

Broker-dealers are required to file a Currency and Monetary Instrument Transportation Report (CMIR, Form 105) with the U.S. Customs Service to report transactions in currency and/or bearer instruments which alone or in combination exceed \$10,000 and which are shipped or transported into or outside the U.S. This filing is not required for currency or other monetary instruments mailed or shipped through the postal service or by common carrier. CIM Securities (or clearing firm or other third party) is responsible for filing these reports and maintaining records of them. CMIRs must be filed within 15 days after the receipt of the currency or monetary instruments.

7.7.3 State Reporting Requirements

States have adopted various currency and suspicious activity reporting requirements. Most states have entered into an agreement with FinCEN to provide them with duplicate copies of forms filed by broker-dealers. Some states, however, require duplicate filing with the states themselves at the time the broker-dealer files with a federal agency. CIM Securities will file reports as required under state requirements.

7.8 Foreign Financial Account Reporting Requirements And Recordkeeping (FBAR)

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart C; FinCEN Notice 2012-1]

Certain "United States persons" that maintain accounts (including any account where the person has a financial interest in, or signature or other authority over) in foreign jurisdictions and with aggregate balances exceeding \$10,000 are required to electronically file the Foreign Bank Account Report Form 114 with FinCEN on or before June 30th of each calendar year for accounts maintained during the previous calendar year. The FINOP is responsible for filing the annual report if it is required for CIM Securities.

The filing requirement applies to:

- Non-resident aliens and foreign entities "in and doing business" in the U.S.

- All forms of U.S. business entities, trusts, estates with foreign accounts.
- U.S. citizens and residents with signature or other authority over a foreign account.
- Trust beneficiaries with a greater than 50% beneficial interest in a trust with a foreign account.
- U.S. citizens and resident stockholders with greater than 50% of the value or vote of the shares of a corporation with foreign accounts.
- Entities that are disregarded for tax purposes, such as limited liability companies.

The filing requirement does not apply to certain entities or situations. The regulation should be consulted for specific exemptions or conditions of exemptions.

- If the account is maintained in the United States, it is not considered a foreign account even if it holds foreign assets.
- An omnibus account held by a custody bank that holds assets both in the U.S. and outside the U.S. is not considered a foreign account unless the customer has direct access to its foreign holdings maintained at the foreign institution.
- Certain entities are excluded including: foreign hedge funds, venture capital funds, or private equity funds; tax-exempt investors that own offshore "blocker corporations;" government pension funds; pension plan participants and IRA owners (provided the trustee files a FBAR); investment advisers and employees of such advisers that provide advice to SEC-registered entities; remainder interests in trusts and beneficiaries of discretionary trusts; employees of a U.S. or foreign entity that issued a class of foreign equity (including ADRs) registered with the SEC.

There also are exemptions for officers or employees with signature or other authority over certain foreign financial accounts but no financial interest in the reportable account. The regulation should be consulted for details regarding who is not required to notify FinCEN regarding signature or other authority over such an account.

7.9 Recordkeeping Requirements (Joint Rule and Travel Rule)

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D]

In addition to maintaining records of reports filed with the IRS or other authorities, broker-dealers are obligated to maintain records of certain transactions, for potential inspection by regulators and other authorities. These records must be retained for five years.

7.9.1 Fund Transfers And Transmittals

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart D; FINRA Notice to Members 97-13, 96-67 and 95-69; SEC Q&As: <http://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf>; SEC Q&As: <http://www.sec.gov/about/offices/ocie/aml2007/fincen-advssiii.pdf>]

Broker-dealers are required to collect and retain information (such as name, address, account number of customer, date and amount of wire, payment instructions, name of recipient institution, and name and account information of wire payment recipient) and maintain records for domestic and international funds transfers (including wire fund transfers) of \$3,000 or more, with certain exceptions.

CIM Securities (and its clearing firm or other third party, if applicable) is responsible for complying with the requirements to record information regarding fund transfers and, when required, verifying information regarding transmitters and recipients who are not established customers. Examples of verification information include:

- Name and address
- ID reviewed (type and number on the ID)
- Taxpayer ID number (or alien ID or passport number including country of issuance)
- Copy or record of method of payment (e.g., credit card, check)

7.9.2 Other Recordkeeping Requirements

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D 1023.410]

The Bank Secrecy Act incorporates other records requirements that include records covered by *Books And Records* in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*. CIM Securities will retain all of the following required records:

1. Trading authorizations which are addressed in the chapter *ACCOUNTS*
2. Records under 17a-3 which are addressed in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*
3. A record of each receipt of currency, other monetary instruments, checks, or investment securities and of each transfer of funds or credit, of more than \$10,000 received on any one occasion directly and not through a domestic financial institution, for any person, account or place outside the United States.

7.10 DVP/RVP Accounts

DVP/RVP accounts that use brokers to liquidate large volumes of low-priced securities may be a red flag for AML concerns. Such accounts should be the subject of reasonable inquiry to determine the source of the securities and to identify potential money laundering and registration issues. CIM Securities is responsible for AML inquiries unless there is a formal undertaking by the customer's prime broker.

7.11 Omnibus Accounts And Transactions In Low-Priced Securities

[SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities; FINRA Regulatory Notice 21-03; FINRA's 2022 Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

There may be risks of illicit activities associated with transactions in low-priced securities through omnibus accounts maintained by foreign financial institutions (FFIs), particularly where the customer or beneficial owner is unknown. Such accounts may "nest" within omnibus accounts of financial institutions based in jurisdictions that are generally considered to be lower risk such as Canada or the UK. Such accounts may be subjected to added review and restrictions or a determination to not open or to close the account. Signs of potentially illicit trading activity in low-priced securities include:

- trading that coincides with a sudden increase in share price or trading volume, in the absence of legitimate news surrounding the company;
- investors depositing large blocks of shares of low-priced securities originating from convertible debt acquired from the issuer or a third party, immediately selling the shares and then transferring the proceeds out of the account;
- transactions in securities of issuers making questionable claims regarding their products or services related to a recent, major event (e.g., the COVID-19 pandemic) or a new trend (e.g., cryptocurrency or non-fungible tokens (NFTs)) or both; and
- increased trading that overlaps with a surge in relevant promotional activity on social media, investor chat rooms and message boards. Firms can find additional resources concerning potential warning signs of fraudulent activity.

7.12 Detecting Potential Money Laundering

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer • Other designated supervisor for review of AML Compliance Officer accounts • Reviewer of systems/procedures (<i>i.e.</i>, Internal Audit, Compliance)
Resources	<ul style="list-style-type: none"> • Internal reports of transactions, available exception reports
Frequency	<ul style="list-style-type: none"> • Daily and ongoing: review of transactions • Annual: test systems and data
Action	<ul style="list-style-type: none"> • For accounts that provide "banking-like services" (<i>i.e.</i>, wire transfers, check writing, ATM withdrawals) review for large movements of money with little or no securities trading • Monitor foreign currency-denominated wire transfers • Monitor customers' deposits and trades in penny stocks for potential suspicious activity • Review for red flags for IPOs in emerging markets • Monitor correspondent accounts maintained for foreign financial institutions • Supervisor(s): <ul style="list-style-type: none"> ○ Review reports of transactions (cash and security transactions) to identify potential money laundering (including employee accounts) ○ Another designated supervisor will review the AML Compliance Officer's accounts ○ Report suspicious activity (see the policy in this chapter) ○ Notify RRs, supervisors, and close accounts when necessary • Reviewer(s): Conduct reviews of systems and data sources to confirm potential suspicious activity will be identified and reported
Record	<ul style="list-style-type: none"> • Reviews including manual/electronic record of reviews of: <ul style="list-style-type: none"> ○ banking-like services ○ reports ○ foreign currency wire transfers ○ IPOs in emerging markets ○ Correspondent accounts for foreign financial institutions • Action taken, when necessary • Suspicious activity reports • Reviews of systems and data and corrective action taken, if applicable

CIM Securities has an ongoing program to identify potential money laundering. Monitoring will be conducted using available exception reports or review of a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or involve "red flags" (indicators of potential money laundering) which are included in the *Money Laundering* policy in the chapter *GENERAL EMPLOYEE POLICIES*. Items reviewed include trading and wire transfer transactions in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Among the information used to determine whether to file a suspicious activity report are exception or transaction reports that include transaction size, location, type, number, and nature of the activity.

Trading accounts will be identified and monitored where a series of financial transactions may help obscure the origins of the funds. This may include effecting securities transactions, closing the account, and transferring funds to a bank or other account, particularly to an offshore location. Trading penny stocks (which may involve unregistered distributions) or engaging in retail forex trading will, in particular, be monitored when they occur.

CIM Securities has included an educational policy (*Money Laundering*) in the chapter *GENERAL EMPLOYEE POLICIES* to educate employees on money laundering and guidelines for detecting money laundering activities. Periodically detection of money laundering and the obligation to report suspicious activities will be included in continuing education and other educational programs for employees.

7.12.1 Clearing Firm AML Procedures – Not applicable at Present

CIM Securities will work with the clearing firm to exchange information, records, data and exception reports as necessary to comply with AML laws. Required certifications for information sharing are on file. As a general matter, the clearing firm will monitor CIM Securities's customer activity on CIM Securities's behalf, and the clearing firm will be provided with proper customer identification information as required to successfully monitor customer transactions. CIM Securities's and the clearing firm's responsibilities are included in the clearing agreement and each firm is responsible for its own independent compliance with AML laws. CIM Securities and the clearing firm cannot disclaim their respective responsibilities to comply with AML requirements.

7.12.2 Foreign Currency Transactions

Foreign financial institutions may purchase U.S.-denominated bonds, generally issued by foreign governments, with the local currency, which are then transferred to a U.S. broker-dealer and sold, with proceeds then transferred offshore. U.S. broker-dealers act as intermediaries in these transactions and may receive foreign bonds or other securities worth millions of U. S. dollars without knowing who or how many underlying customers may be involved. RRs and CIM Securities must be diligent about such transactions which may involve money laundering.

7.12.3 IPOs In Emerging Markets

[FINRA 2022 Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>; SEC statement on emerging market investments: <https://www.sec.gov/news/public-statement/emerging-market-investments-disclosure-reporting>]

Emerging markets may pose an added risk of money laundering. Investors in IPOs in this market may be serving as nominees for an undisclosed control person or persons. These IPOs are typically smaller in size (*i.e.*, less than \$100 million) and listed on the lower qualification tiers of U.S. stock exchanges. Red flags of potentially manipulative trading associated with how these investors open new accounts and trade these securities, after the IPO is completed, include:

- numerous unrelated accounts being opened at the same time, including with similar banking information, physical addresses, email address domains and current employer (which is often associated with the IPO issuer);
- documents investors provide in order to open an account or verify source of funds that may have been altered or could be fictitious;
- wire transfers received into these accounts that exceed the financial wherewithal of the investor as indicated on their new account documents, exceed the value of the shares purchased in the IPO and are either sent from similar banks, or bank accounts that share certain identifying information (*e.g.*, employer of account holder, email domain);
- investor accounts being accessed by a different Internet Protocol (IP) or Media Access Control (MAC) address than is known for the customer, granting login and trading capabilities to a third party or both;

- multiple orders with substantially similar terms being placed at or around the same time by seemingly unrelated investors in the same security that is indicative of "spoofing" or "layering"; and
- investors engaging in trading activity that does not make economic sense.

7.13 Information Sharing Between Financial Institutions

[USA PATRIOT Act Section 314(b); Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; Section 314(b) Fact Sheet: Section 314(b) Fact Sheet (fincen.gov)]

CIM Securities may share information with other financial institutions regarding accounts and account activity in accordance with Patriot Act and regulatory requirements.

7.14 Suspicious Activities

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; USA PATRIOT Act Section 356; FINRA Notice to Members 02-47; FinCEN Guidance FIN-2008-G005; FinCEN FAQs: Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations <https://www.fincen.gov/resources/statutes-regulations/guidance/answers-frequently-asked-questions-regarding-suspicious>; 2022 FINRA Report: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer
Resources	<ul style="list-style-type: none"> • Reports from employees of crimes or suspected crimes • Suspicious activities detected through ongoing reviews • Exception and other reports (internal and/or provided by a clearing firm) • FinCEN advisories • Other available information
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Maintain the confidentiality of SAR reviews and filings: <ul style="list-style-type: none"> ○ Limit the sharing of information to those authorized and need to know ○ Electronic files should be password-protected and use a file name that does not identify files as SARs-related ○ Use a header on documents: CONFIDENTIAL ○ In redaction markings or privilege logs, identify the redacted or privileged information as "nonpublic supervisory information" ○ For production of documents, produce SAR documents separately from other documents and identify as confidential SAR information ○ Destroy copies of SARs when retention periods have passed ○ Confer with counsel or other outside expert regarding confidentiality questions • Include FinCEN red flags in suspicious activity identification • Review and investigate suspicious transactions referred by employees or identified in review of surveillance reports • Review and investigate suspicious transactions referred by a clearing firm, if applicable • Periodically review reports to confirm integrity of captured data and adjust reports as necessary • Determine whether CIM Securities (or its clearing firm, if applicable) will file a SAR • If appropriate, file Form SAR with FinCEN and state authorities

	<ul style="list-style-type: none"> • Notify senior management, as appropriate, of forms filed • Provide copy to parent company, if applicable • File SARs jointly with other financial institutions, if applicable
Record	<ul style="list-style-type: none"> • Notes and other documented reviews including record of manual/electronic review and actions taken, if applicable • Review of reports for integrity and adjustments made • Copies of SARs filed by CIM Securities are retained in the SAR file with notation of when and to whom sent

CIM Securities has an obligation to identify suspicious activities and file Suspicious Activity Reports (SARs) for transactions that may be indicative of money laundering activity. Suspicious activities include a wide range of questionable activities; examples include trading that constitutes a substantial portion of all trading for the day in a particular security; trading or journaling between/among accounts, particularly between related owners; late day trading; heavy trading in low-priced securities; unexplained wire transfers, including those to known tax havens; unusually large deposits of funds or securities. For business introduced to a clearing firm, if applicable, CIM Securities will rely on the clearing firm to make filings on its behalf and to provide copies to CIM Securities.

7.14.1 Identifying Potential Suspicious Activity

CIM Securities uses a number of tools to identify potential suspicious activity including:

- Transaction information including disbursement of funds or securities
- Education of firm personnel, particularly supervisors in Operations areas
- Employee reports of potential suspicious activity forwarded to the AML Compliance Officer
- Internal reports or reports provided by a clearing firm, if applicable

7.14.2 When A Report Must Be Filed

A SAR must be filed for any transaction that, alone or in aggregate, involves at least \$5,000 in funds or other assets, if CIM Securities knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is part) falls into one of the following categories:

- Transactions involving funds derived from illegal activity or intended or conducted to hide or disguise funds or assets derived from illegal activity.
- Transactions designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act (BSA).
- Transactions that appear to serve no business or apparent lawful purpose or are not the sort of transactions in which a particular customer would be expected to engage, and for which CIM Securities knows of no reasonable explanation after examining the available facts.
- Transactions that involve the use of CIM Securities to facilitate criminal activity.

Excluded from the filing requirement are violations otherwise reported to law enforcement authorities such as:

- a robbery or burglary that is reported to law enforcement authorities
- lost, missing, counterfeit, or stolen securities reported pursuant to 17f-1
- a violation of federal securities laws or SRO rules by CIM Securities, its officers, directors, employees, or RRs that are reported to the SEC or SRO, except for violations of Rule 17a-8 (filing of Currency and Transaction Reports) which must be reported on a SAR

7.14.3 Filing A Report And Emergency Notification

If CIM Securities determines to file a SAR with FinCEN, the AML Compliance Officer will file:

- within 30 days of becoming aware of the suspicious transaction; or
- if no suspect has been identified within 30 calendar days of detection, reporting may be delayed an additional 30 calendar days or until a suspect has been identified, but no later than 60 days from date of initial detection.

In situations involving violations that require immediate attention (such as terrorist financing or ongoing money laundering schemes), the AML Compliance Officer will immediately notify by telephone an appropriate law enforcement agency. Suspicious transactions that may relate to terrorist activity may also be reported to FinCEN's Financial Institutions Hotline. In either event, a SAR will be filed.

7.14.3.1 Emergency Notification

[FINRA Notice to Members 02-21]

When conducting due diligence or opening an account, Federal authorities will be notified immediately by the AML Compliance Officer, when necessary, in the following situations:

- A legal or beneficial account holder or person is engaged in a transaction listed on or located in a country or region listed on the OFAC list.
- An account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list.
- A customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity.
- There is reason to believe a customer is trying to move illicit cash out of the government's reach.
- There is reason to believe the customer is about to use funds to further an act of terrorism.

Emergency contacts include:

- OFAC Hotline (1-800-540-6322)
- Financial Institutions Hotline (1-866-556-3974)
- Local U.S. Attorney's office
- Local FBI office
- Local SEC office

7.14.4 Retention Of Records

The AML Compliance Officer maintains a file of copies of SARs filed with FinCEN and all related documents for a period of 5 years from the filing date.

7.14.5 Providing SARs Information To SROs

[SEC letter to CEOs: <http://www.sec.gov/about/offices/ocie/brokerdealerletter.htm>]

While SARs are to be treated as confidential, CIM Securities will provide SARs and supporting documentation available to any self-regulatory organization (SRO) that examines CIM Securities for compliance with the SAR

Rule, upon request of the SEC. The request may be part of a routine examination, an investigation, or part of the SRO's risk assessment effort within its examination program.

7.14.6 Prohibition Against Disclosure

By statute and regulation, CIM Securities may not inform customers or third parties that a transaction has been reported as suspicious. U.S. Treasury and Federal Reserve Board regulations also require CIM Securities to decline to produce SARs in response to subpoenas and to report to FinCEN and the Federal Reserve Board the receipt of such requests and CIM Securities's response. Failure to maintain the confidentiality of SARs may subject an employee to civil and criminal penalties under Federal law. Violations may be enforced through civil penalties of up to \$100,000 for each violation and criminal penalties of up to \$250,000 and/or imprisonment not to exceed five years. CIM Securities may also be liable for civil money penalties resulting from AML deficiencies that led to improper SAR disclosure up to \$25,000 per day for each day the violation continues.

Procedures to protect the confidentiality of SARs include the following:

- Access to SARs is limited to employees on a "need-to-know" basis
- SARs will be maintained in locked physical or electronic files
- SARs may not be left on desks or on open computer files and must be viewed without access by unauthorized persons
- SARs shared with others will be clearly marked "Confidential"

Compliance (or CIM Securities's counsel) is responsible for responding to subpoena requests and Compliance will notify FinCEN and the Federal Reserve Bank of any subpoenas for SARs.

7.14.7 Politically Exposed Persons (PEP)

[FinCEN Advisory FIN-2018-A003]

FinCEN has highlighted how corrupt foreign PEPs' activity may trigger suspicious activities requiring reporting. FinCEN's advisory lists red flags which are incorporated into CIM Securities's suspicious activity identification and reporting process.

7.15 Requests And Written Notices From Regulators, Enforcement Agencies, And Other Authorized Persons

Under the Bank Secrecy Act, financial institutions are required to respond to federal banking agency requests for information relating to anti-money laundering compliance. The Rule requires provision of information and account documentation for any account opened, maintained, administered or managed in the U.S. The AML Compliance Officer maintains records of information provided in response to regulators' requests including the request, date of response, and information provided.

7.15.1 Federal Banking Agency Requests -- 120-Hour Rule

[USA PATRIOT Act Section 319(b)]

Upon receiving a request from a Federal banking agency, the AML Compliance Officer will provide the requested information within 5 days (120 hours) of receiving the request or will make available the information for inspection by the banking agency.

7.15.2 Information Sharing With Enforcement Agencies

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; USA PATRIOT Act Section 314]

Responsibility	<ul style="list-style-type: none">• AML Compliance Officer
Resources	<ul style="list-style-type: none">• Deposit records, purchase/sale records, account records, other records as required, FinCEN Secure Information Sharing System (SSIS)
Frequency	<ul style="list-style-type: none">• Upon request• Bi-weekly: review SSIS
Action	<ul style="list-style-type: none">• Conduct bi-weekly review of SSIS and print confirmation page• If a match is found, submit the information as required
Record	<ul style="list-style-type: none">• Documentation of reviews including a confirmation page from SSIS and records of positive search results

Enforcement agencies (FinCEN, state, local, and certain foreign law enforcement agencies eligible to make requests) send requests to FinCEN's Secure Information Sharing System (SSIS). CIM Securities is required to review the SSIS bi-weekly to identify requests for information and to send required information within required timeframes.

Enforcement agency requests are confidential and may not be disclosed to the subject of the request. CIM Securities will not use information provided to enforcement agencies for any purpose other than (1) to report to an agency as required under Section 314; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist CIM Securities in complying with any requirement of Section 314.

7.15.3 National Security Letters

[FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005)]

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. **NSLs are highly confidential. CIM Securities and its employees are barred from disclosing to any person that a government authority or the FBI has sought or obtained access to records.**

The AML Compliance Officer is responsible for responding to an NSL and maintaining the confidentiality of the letter and the response. If an SAR-SF is filed after receiving an NSL, the SAR-SF cannot make reference to the receipt or existence of an NSL. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

7.15.4 Grand Jury Subpoenas

[FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006)]

The receipt of a grand jury subpoena concerning a customer does not in itself require the filing of a Suspicious Activity Report (SAR-SF). When a grand jury subpoena is received, the AML Compliance Officer will:

- Conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity.
- If suspicious activity is identified during the risk assessment and review, the risk assessment will be elevated and an SAR-SF will be filed. The SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

The existence of a subpoena and any response are confidential and may not be disclosed directly or indirectly to the person who is the subject of the subpoena. The AML Compliance Officer will maintain the subpoena and any response in a confidential file and will only share information with those authorized.

7.15.5 Foreign Bank Correspondent Accounts

[USA PATRIOT Act Section 313]

Upon receipt of a written request from a Federal law enforcement officer for information about a foreign bank correspondent account, the AML Compliance Officer will provide the requested information no later than 7 days after receipt of the request.

Compliance will terminate any correspondent relationship with a foreign bank within 10 business days of receiving a notice from the Treasury Dept. or the U.S. Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in a U.S. court.

7.15.6 Requests By Law Enforcement To Maintain Accounts

Law enforcement agencies may have an interest in having accounts remain open in spite of suspicious or potential criminal activity in connection with the account. The AML Compliance Officer will consider such requests and, if the account will remain open, require the federal law enforcement agency to provide a written request issued by a supervisory agent or by an attorney within the U.S. Attorney's Office or another office of the Department of Justice. If requested by a state or local law enforcement agency, the letter must be issued by a supervisor or local prosecutor's office.

The written request must include:

- the agency's request that the account remain open;
- the purpose of the request; and
- the duration of the request (not to exceed 6 months).

The request will be retained for 5 years.

If CIM Securities is aware the account is under investigation (because of a subpoena, 314[a] request, National Security Letter, or similar communication), the requesting law enforcement agency will be advised before making a decision about the status of the account.

7.16 Accounts Requiring Approval By The AML Compliance Officer

The following accounts require review and approval by the AML Compliance Officer at the time of opening. The AML Compliance Officer may require additional information for these accounts.

- **Numbered accounts** (accounts designating a number rather than a name as the account name).
- **Any account requesting confidential handling** of its name, mailing of confirmation and statements, *etc.*
- **Accounts domiciled in high risk countries.** Accounts domiciled in countries identified by OFAC or the Financial Action Task Force on Money Laundering (FATF) as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- **Foreign public officials.** Includes individuals in high offices of foreign governments, political party officials and their families and close associates (if known and/or readily identifiable).
- **Correspondent and Private Banking accounts.** See the section *Due Diligence For Correspondent And Private Banking Accounts*.

7.17 Customer Identification Program (CIP)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; FINRA Notice to Members 03-34; FinCEN Frequently Asked Questions: <https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-customer-identification>; FinCEN No-Action position on CIP requirements under clearing arrangements: FIN-2008-G002; Guidance on Obtaining and Retaining Beneficial Ownership Information, FinCEN Guidance, FIN-2010-G001 March 5, 2010]

The opening of customer accounts is subject to customer identity verification requirements under CIM Securities's Customer Identification Program (CIP). Requirements for employees opening accounts as explained in the chapter *ACCOUNTS* are duplicated in this section to consolidate all AML requirements within this chapter.

7.17.1 Definition Of Customer Under CIP Rule

The definition of "customer" under the CIP rule is different than definitions under other rules. Who is a "customer" under this Rule affects CIM Securities's obligations.

Under the CIP rule and for purposes of this section, "customer" is defined as:

- A person that opens a new account.
- An individual who opens a new account for:
 - An individual who lacks legal capacity; or
 - An entity that is not a legal person.

"Customer" does not include a financial institution regulated by a Federal regulator; a bank regulated by a state bank regulator; those exempted under Federal rule include municipalities; or a person with an existing account at CIM Securities providing there is reasonable belief that the true identity of the person is known.

7.17.2 Accounts Opened By Other Financial Institutions

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer
Resources	<ul style="list-style-type: none"> • Other financial institution's CIP • Contract with other financial institution
Frequency	<ul style="list-style-type: none"> • Initially when an institution opens accounts and updated as needed - evaluate institution's CIP • Annual - obtain certification

Action	<ul style="list-style-type: none"> • Where required: <ul style="list-style-type: none"> ○ Confirm institution is subject to AML rules/requirements ○ Evaluate other institution's CIP ○ Contract with other institution regarding compliance with CIM Securities's CIP requirements ○ Obtain annual certification
Record	<ul style="list-style-type: none"> • Evaluation of other institution's CIP • Contract with other financial institution • Annual certifications from the financial institution

7.17.2.1 Financial Intermediaries As Customers Vs. Beneficial Owners

[Guidance from Dept. of Treasury and SEC regarding broker-dealer CIP rule: <http://www.sec.gov/divisions/marketreg/ga-bdidprogram.htm>]

Financial institutions (such as banks, clearing firms, investment advisers, *etc.*) act as intermediaries opening accounts including master and omnibus accounts. The SEC has stated that the underlying beneficial owners are **not** "customers" subject to CIP requirements under the following circumstances outlined in the SEC's guidance:

1. the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus account holder provides limited information to CIM Securities solely for the purpose of delivering assets to the custody account of the beneficial owner at another financial institution;
2. the limited information given to CIM Securities about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution;
3. all transactions in the omnibus account or sub-accounts at CIM Securities are initiated by the financial intermediary; and
4. the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer.

CIM Securities is not obligated to look through the intermediary financial institution to the underlying beneficial owners if the intermediary identifies itself as the account holder. Even if CIM Securities has some information about beneficial owners, the intermediary (not the beneficial owner) is treated as the customer for purposes of the CIP rule under these circumstances.

7.17.2.2 Reliance On Other Financial Institutions

[CIP Rule paragraph (b)(6)]

CIM Securities may rely on another financial institution (such as a bank, clearing firm, another broker-dealer, *etc.*) to conduct CIP reviews with respect to dual customers of both CIM Securities and the financial institution that is opening an account or has established an account or a similar business relationship between the customer and the other financial institution to provide or engage in services, dealings, or other financial transactions. CIM Securities may rely on the other financial institution if the following conditions are met:

- Reliance on the other institution is reasonable (knowledge of the other institution's AML program);
- The other institution is subject to AML requirements; and
- The other institution enters into a contract with CIM Securities requiring annual certification to CIM Securities that it has implemented its AML program and will perform (or its agent perform) requirements of CIM Securities's CIP.

7.17.2.3 Registered Investment Adviser Accounts

[SEC Division of Market Regulation No-Action Letter to SIFMA dated January 9, 2015: <http://www.sec.gov/divisions/marketreg/mr-noaction/2015/sifma-010915-17a8.pdf>]

Responsibility	<ul style="list-style-type: none">• AML Compliance Officer
Resources	<ul style="list-style-type: none">• New investment adviser accounts
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• For each SEC-registered adviser opening accounts with CIM Securities where CIM Securities will rely on the adviser for CIP compliance:<ul style="list-style-type: none">○ Conduct due diligence to review adviser including confirming adviser's SEC registration and update as needed○ Obtain the adviser's written agreement to comply with CIP requirements○ Obtain annual certification
Record	<ul style="list-style-type: none">• Due diligence review• Written agreement of CIP compliance• Annual certifications

CIM Securities may rely on an SEC-registered investment adviser to perform some or all of the CIP obligations related to customers where CIM Securities and the investment adviser have a customer relationship, under the following conditions.

- it is reasonable to rely on the adviser's assurances;
- the investment adviser is a U.S. investment adviser registered with the SEC under the Investment Advisers Act of 1940; and
- the adviser enters into a written agreement with CIM Securities in which the adviser agrees that:
 - it has implemented its own AML Program consistent with the requirements of 31 U.S.C. 5318(h) and will update such AML Program as necessary to implement changes in applicable laws and guidance;
 - it (or its agent) will perform the specified requirements of CIM Securities's CIP in a manner consistent with Section 326 of the PATRIOT Act;
 - it will promptly disclose to the broker-dealer potentially suspicious or unusual activity detected as part of the CIP being performed on the broker-dealer's behalf in order to enable CIM Securities to file a Suspicious Activity Report, as appropriate based on CIM Securities's judgment;
 - it will certify annually to CIM Securities that the representations in the reliance agreement remain accurate and that it is in compliance with such representations; and
 - it will promptly provide its books and records relating to its performance of CIP to the Commission, to an SRO that has jurisdiction over CIM Securities, or to authorized law enforcement agencies, either directly or through CIM Securities, at the request of (i) CIM Securities, (ii) the SEC, (iii) an SRO that has jurisdiction over the broker-dealer or (iv) an authorized law enforcement agency.

7.17.3 Master Accounts And Sub-Accounts

[FINRA Regulatory Notice 10-18; SEC National Exam Risk Alert "Master/Sub-accounts:" <http://www.sec.gov/about/offices/ocie/riskalert-mastersubaccounts.pdf>]

Accounts are sometimes established as "master accounts" that represent multiple sub-accounts. Depending on facts and circumstances (discussed below), master/sub-accounts may be recognized as separate customer accounts subject to CIP reviews.

7.17.3.1 Description Of Master/Sub-Accounts

A master account may have multiple underlying accounts on behalf of underlying investors; sub-advisers may be authorized to effect transactions without the intermediation of the master account owner. Also, an individual or entity may set up sub-accounts for separate trading strategies or algorithms. Sub-accounts may be used by individual traders or groups of traders. The master account may be another broker-dealer or a partnership that provides its individual partners trading authority over separate sub-accounts.

7.17.3.2 Obligations To Conduct CIP Reviews

Except for accounts opened by investment advisers and financial institutions discussed under *Accounts Opened By Other Financial Institutions* and meeting the conditions of that section, when there are separate owners of the sub-accounts, CIM Securities has an obligation to identify the beneficial owners. Indicators that there may be separate owners requiring CIP review of the sub-accounts include:

- The sub-account owner is entering orders for itself.
- CIM Securities has actual notice the sub-accounts have different owners.
- The sub-accounts are separately documented and/or receive separate reports.
- The sub-accounts are addressed separately in terms of transaction, tax or other reporting.
- The services provided to the sub-accounts engender separate surveillance and supervision of the sub-accounts for compliance with rules or for risk management purposes consistent with the review of separately owned accounts.*
- There are financial arrangements or transactions with the sub-accounts, or separate account terms, that reasonably raise questions concerning whether such accounts represent separate beneficial owners.*
- The sub-accounts incur charges for commissions, clearance and similar expenses, separately, based upon the activity only of that subject sub-account.*
- There is evidence of financial transactions or transfers of assets or cash balances that would reasonably evidence separate beneficial ownership of the sub-accounts.*
- CIM Securities (or RR) is aware of or has access to a master account or like agreement that evidences that the sub-accounts have different beneficial owners.
- There is evidence that a party maintaining a master/sub-account arrangement has interposed sub-accounts that have or are intended to have the effect of hiding the beneficial ownership interest.*
- The number of sub-accounts maintained is so numerous as to reasonably raise questions concerning whether such accounts represent separate beneficial owners.*

* Items above would not apply in the case of accounts opened by a registered BD or a bona fide investment adviser.

7.17.4 Customer Due Diligence (CDD)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1010, Part 1020, Part 1023, Part 1024 and Part 1026; FinCEN 2016 FAQs: <https://www.ffiiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf>; FinCEN 2018 FAQs: <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-customer-due-0>; FINRA Rule 3310; FINRA Regulatory Notice 18-19 and 17-40]

This section is duplicated from the chapter *ACCOUNTS*.

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • New account application and other customer ID information
Frequency	<ul style="list-style-type: none"> • When accounts are opened
Action	<ul style="list-style-type: none"> • Before approving an account, determine that customer identification (ID) verification information is included with the new account application and meets CIM Securities's requirements • For legal entity customers: <ul style="list-style-type: none"> ◦ Obtain beneficial ownership certifications ◦ Determine whether a threshold lower than 25% ownership is warranted depending on the customer's risk for potential enhanced monitoring or to collect additional information including expected account activity • For non-documentary verification, check the information included with the new account application for completeness and consistency with other customer-provided information (name, address, phone number, taxpayer ID number, etc.) • For unacceptable verification information (incomplete, inconsistent), return the application to the RR for further information or disapprove the account • Identify accounts where CIM Securities may rely on other financial institutions to satisfy CIP requirements and confirm eligibility to rely on exception • Obtain annual certification from other financial institutions • Include beneficial owners in AML monitoring
Record	<ul style="list-style-type: none"> • New account records include customer ID verification as well as the supervisor's approval and customer certifications • Identification and verification of reliance on other financial institutions • Annual certifications from other financial institutions • Certifications from legal entity customers or documentation of oral certification, where applicable

When opening new accounts, the customer's identity must be verified, as required by federal law. Customer identification (ID) information must be completed on the new account application. This includes, under FinCEN's requirements:

1. customer identification and verification;
2. beneficial ownership identification and certification;
3. understanding the nature and purpose of customer relationships; and
4. ongoing monitoring for reporting suspicious transactions and, on a risk basis maintaining and updating customer information.

Customer ID verification does NOT apply to accounts for:

- persons with an existing account at CIM Securities (unless the account requires approval by the AML Compliance Officer)
- banks
- governmental entities
- issuers of listed equity securities

- other financial institutions subject to regulation by the SEC, CFTC, Federal Reserve Board, OCC, FDIC, Office of Thrift Supervision, or the National Credit Union Administration
- persons opening accounts to participate in an ERISA plan

In addition, for accounts defined as "legal entity customers" (defined below), information must be obtained about beneficial owners. This requirement applies to accounts established May 11, 2018 or later. If CIM Securities becomes aware of a change of beneficial ownership after May 11 for accounts established before that date, the customer's records must be updated under CDD requirements.

7.17.4.1 Definitions

[Exchange Act Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

The regulations should be consulted for more complete definitions.

Legal entity customer: corporation; limited liability company; another entity created by a public filing with a Secretary of State or equivalent; general partnership; limited partnership; business trust created through a state filing; or any similar entity formed under federal law. Does not include sole proprietorships, unincorporated associations, and natural persons opening their own account. Other exclusions are a federal- or state-regulated financial institution; political departments and agencies of the U.S. or a State; various different types of entities registered with the CFTC or SEC; and other entities included in the regulation. [Questions 22-28, 2018 FAQs]

Beneficial owner:

- each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (*i.e.*, the ownership prong); and
- a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (*e.g.*, a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (*i.e.*, the control prong).

Ownership and control prongs: The CDD rule utilizes a two-pronged approach to defining a beneficial owner - an ownership prong and a control prong. Under the ownership prong, a beneficial owner is defined as each individual, if any, who, directly or indirectly, owns 25 percent or more of the equity interests of a legal entity customer. However, the rule recognizes that there may be instances when no single individual owns 25 percent or more of the equity interest of the legal entity; in such instances, CIM Securities is still required to collect the required information for one individual who controls, manages or directs the legal entity customer. Under the control prong, a beneficial owner is defined as a single individual with significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager (*e.g.*, a chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president or treasurer) or any other individual who regularly performs similar functions. The ownership and control prongs, although related, are independent requirements. Thus, satisfaction of, or exclusion from, regulatory obligations under one prong does not mean CIM Securities's obligations under the other prong are also satisfied or excluded. [Question 9, 2016 FAQs]

7.17.4.2 Required Customer Information

[Exchange Act Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

Basic information required **prior to opening the account** includes:

- **Name**
- **Date of birth**, for an individual
- **Address:**

- for an individual, residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
- for a non-individual (corporation, trust, *etc.*) a principal place of business, local office, or other physical location.
- **Telephone number**
- **Employment status** (including occupation and whether the person is associated with a broker dealer)
- **Annual income**
- **Net worth** (excluding value of primary residence)
- Account's investment objectives
- For joint accounts, information on each joint owner (financial information may be combined)
- **Taxpayer identification number** for a U.S. person (U.S. citizen or non-individual established or organized under U.S. or state laws).
- **Identification number for non-U.S. person** which may include a taxpayer ID number; passport number and country of issuance; alien identification card number; or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photo or similar safeguard.
- **Beneficial owners** (see the section that follows) including information about the following:
 - the nature and purpose of customer relationships to develop a customer risk profile
 - information sufficient at the time of account opening so customer activity may be assessed for SAR requirements (may include type of customer requesting services; type of account being opened; services or products being used)

In the case of a customer who has applied for a taxpayer identification number but has not yet received it, notation must be made on the new account application that the taxpayer ID has been applied for. The account will be restricted to liquidating transactions if the taxpayer ID number is not received within 5 days of opening the account.

In addition, under FINRA Rule 4512 CIM Securities will retain the name of the RR responsible for the account and, if multiple RRs are assigned to the account, a record indicating the scope of their responsibilities with respect to the account. This requirement does not apply to an institutional account.

7.17.4.3 Accounts For Individuals

When opening an account for an individual, the following information is required:

- An unexpired government-issued identification including a photo and nationality or residence such as a driver's license or passport and record information from it on the new account application, **OR**
- A copy of the photo ID with the new account application. (The photo ID [original or copy] must be seen by the employee opening the account to record the information. This information may NOT be taken from the customer over the phone.)
- If the photo ID is not available at the time the new account application is being completed, the RR is to indicate on the new account application whether the customer will provide a copy of photo ID within 5 days of account opening **OR**, if the customer cannot provide a photo ID, the reason why not.
- If the photo ID is not received within 5 days, the account will be restricted to liquidating transactions only until the ID is received.

If the customer has not appeared in person at CIM Securities's office, "non-documentary" information will ALSO be required, as explained in a section that follows.

If the customer cannot produce the required photo ID, an explanation must be included on the new account application AND non-documentary information will be required to open the account.

7.17.4.4 Accounts For Legal Entity Customers

[SEC Release No. 34-61651: Policy Statement on Obtaining and Retaining Beneficial Ownership Information for Anti-Money Laundering Purposes]

For legal entity customers, information must be obtained and verified regarding beneficial owners [Question 4, 2018 FAQs]. Obligations when opening accounts that include underlying owners or beneficiaries include the following:

- Determine whether the customer is acting as an agent for or on behalf of another, and if so, obtaining information regarding the capacity in which and on whose behalf the customer is acting.
- Where the customer is a legal entity that is not publicly traded in the United States, such as an unincorporated association, a private investment company (PIC), trust or foundation, obtain information about the structure or ownership of the entity so as to allow CIM Securities to determine whether the account poses heightened risk.
- Where the customer is a trustee, obtain information about the trust structure to allow CIM Securities to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.
- Obtain the identities of individuals who satisfy the definition as beneficial owners, either directly or indirectly through multiple corporate structures (complex ownership structures). [Question 3, 2018 FAQs]
- Obtain from the legal entity customer's representative a completed certification form identifying beneficial owners; updating information may require re-certification. [Questions 6 & 16, 2018 FAQs]
[\[https://www.fincen.gov/resources/filing-information\]](https://www.fincen.gov/resources/filing-information)
- Determine the nature and purpose of the customer relationship to determine risk profiles and identify the need for additional monitoring. [Questions 35-37, 2018 FAQs]

If CIM Securities has affiliates with public customers, information may be shared across the enterprise to cross-check beneficial ownership information.

7.17.4.4.1 Reliance On Customer Representations

CIM Securities may reasonably rely on information provided by customers if it has no knowledge of facts that would call into question the reliability of the information.

- There is no requirement to independently investigate a legal entity customer's ownership structure.
- CIM Securities may rely on information provided by the customer to determine if the legal entity is excluded from the definition of legal entity customer.

7.17.4.4.2 Retention Of Beneficial Ownership Information

Identifying information will be maintained for a period of five years after the legal entity's account is closed. Verification records must be maintained for a period of five years after the record is made. CIM Securities will also retain a description of each document relied on for verification, any non-documentary methods and results of measures undertaken for verification and the resolution of substantive discrepancies discovered in identifying and verifying the identification information for five years after the record is made. [Questions 9 & 10, 2018 FAQs]

7.17.4.4.3 Specific Account Requirements

Existing customers: For existing customers subject to CIP, CIM Securities may rely on information obtained through the CIP to fulfill CDD requirements, providing that a representative of the customer certifies or confirms (orally or in writing) the accuracy of pre-existing CIP information. This also applies to the opening of multiple accounts, simultaneously or not. Oral confirmation must be documented in account records, and written confirmation will be retained with account information. [Questions 7 & 13, 2018 FAQs]

Foreign customers: Companies traded on foreign exchanges are subject to CDD requirements (while companies traded on U.S. exchanges are exempt). A "risk-based" approach may NOT be taken for these foreign customers, but CIM Securities may rely on their public disclosures as are available for other legal entity customers (whether listed or not). A foreign financial institution (FFI) is excluded from the definition of a legal entity customer if its foreign regulator collects and maintains beneficial ownership information about the FFI. CIM Securities may rely on representations of the FFI as to whether the exclusion applies. Lacking reasonable reliance on the FFI's representation, CIM Securities will contact the foreign regulator to confirm retention of beneficial ownership information.

Internal recordkeeping and operational accounts: When CIM Securities opens an account or subaccount (e.g., to accommodate trading strategies) relating to an existing legal entity customer, the account is not considered a new account and is not subject to CDD beneficial ownership requirements. [Question 11, 2018 FAQs]

Trusts as beneficial owners: If a trust owns 25% or more of the equity interests of a legal entity customer, the beneficial owner is the trustee, regardless of whether the trustee is a natural person or a legal entity. If there are multiple co-trustees of a trust that is a 25% or greater owner of equity interests of a legal entity customer, CIM Securities is not required to identify and verify the identity of all co-trustees. It must collect and verify the identity of, at minimum, one co-trustee of such a multi-trustee trust. [Questions 19 & 20, 2018 FAQs]

Pooled investment vehicles (PIV): For a PIV whose operators or advisers are not excluded from the definition of a legal entity customer, CIM Securities is not required to look through the PIV to identify and verify individuals who own 25% or more of its equity interests. However, CIM Securities is required to collect beneficial ownership information. [Question 18, 2018 FAQs]

Lower-risk customers: For certain lower-risk customers, the nature and purpose of the relationship can be developed by inherent or self-evident information.

7.17.4.4.4 Anti-Money Laundering Requirements

Beneficial owners are subject to AML requirements. See other requirements in this chapter.

7.17.4.4.5 Currency Transaction Reporting (CTR) Requirements

CDD requirements do not change existing CTR requirements. CIM Securities will presume different businesses that share a common owner are operated separately and independently from each other and from the common owner. Transactions across commonly owned legal entity customers will not be aggregated absent indications the businesses are not operating independently (*i.e.*, same staff or location, accounts of one business are repeatedly used to pay the expenses of another business). Beneficial owners of a trust or estate account are not required when completing a CTR. Beneficial owner listing is only required if CIM Securities knows that the transaction(s) requiring filing is made on behalf of a beneficial owner and results in either cash in or cash out totaling more than \$10,000 during any one business day. [Questions 32 & 33, 2018 FAQs]

7.17.4.4.6 OFAC

Beneficial owners are subject to OFAC reviews outlined in this AML chapter.

7.17.4.5 Enhanced Due Diligence (EDD)

Some types of accounts, because of the potential risk for hiding the identity of underlying beneficial owners or money laundering activities, are subject to enhanced due diligence. The AML Compliance Officer will determine which accounts are subject to EDD and what reviews are necessary. Procedures for correspondent and private banking accounts are included in a separate section of this AML program. Certain trusts, corporate entities, shell entities, and private investment companies are examples of customers that may pose heightened risk.

EDD may include steps, in accordance with the level of risk presented, to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner. EDD information may be used for monitoring purposes and to determine whether there are discrepancies between information obtained regarding the account's intended purpose and expected account activity and the actual sources of funds and uses of the account.

7.17.4.6 Third Party Accounts

Customer ID required for third party accounts includes the following:

On behalf of an incompetent person: Obtain customer ID of the person holding power of attorney.

With power of attorney or trading authorization held by a third party: Obtain customer ID of the owner of the account. Customer ID is not necessary for the individual with authority over the account unless that person is unfamiliar to the RR or the circumstances regarding the opening of the account raises questions (customer requires wiring funds to an offshore address; third party is a foreign citizen; *etc.*).

7.17.4.7 Reliance On Other Financial Institutions

[C.F.R. 1023.220(a)(6)]

CIM Securities may rely for CIP purposes on another financial institution (including an affiliate) that opens a customer account provided that:

- reliance is reasonable under the circumstances;
- the other financial institution is subject to anti-money laundering requirements [U.S.C. 5318(h)] and is regulated by a Federal regulator; and
- the other financial institution enters into a contract requiring it to annually certify that it has implemented its AML program and it will perform (or its agent) specified requirements of CIM Securities's CIP.

7.17.4.8 Intermediated Account Relationships

[Various guidance from the U.S. Treasury and SEC regarding mutual fund CIP rule, BD CIP rule, FAQs regarding FCMs and introducing brokers, and foreign accounts]

If an intermediary is the customer and CIM Securities has no CIP obligation regarding the intermediary's underlying customers under existing guidance, CIM Securities will treat the intermediary as its legal entity

customer. For example, the intermediary may be treated as the customer for transactions through omnibus accounts if:

- the omnibus account was established to execute transactions for settlement at another institution or the intermediary provides limited customer information to CIM Securities;
- the limited information provided is used primarily for recordkeeping purposes or to establish sub-accounts that hold positions for limited durations;
- all transactions in the omnibus account are initiated by the intermediary; and
- the beneficial ownership has no direct control over the omnibus account.

7.17.4.9 Accounts For Non-Individuals

Account documents usually obtained for non-individual accounts (trust instruments, articles of incorporation, partnership agreements, government-issued business license, *etc.*) will usually satisfy customer ID requirements. In the case of corporations, a certified copy of the articles of incorporation is required. These documents must be obtained within 30 days of account opening to satisfy the requirement.

7.17.4.10 Non-Documentary Methods Of Verifying Customer Identification

Non-documentary methods of verifying customer ID involve other procedures. Non-documentary methods must be used in the following circumstances:

- An individual is unable to present acceptable photo ID.
- The documents presented are unfamiliar.
- The account is opened without obtaining documents.
- The customer opens the account without appearing in person at CIM Securities.
- Other circumstances, at the discretion of the RR's supervisor, New Accounts, and/or the AML Compliance Officer, where CIM Securities is unable to verify the customer's identity.

In these circumstances, a non-documentary method must be indicated by the RR on the new account application:

- Direct customer contact information
- Information from a consumer reporting agency or other database
- References from another financial institution
- Obtained a financial statement

7.17.4.11 Additional Verification For Certain Customers

For the following types of customers, a minimum of TWO forms of customer ID are required in addition to review and approval by the AML Compliance Officer **prior to** opening the account:

- Numbered accounts
- Accounts domiciled in high-risk countries included on the Treasury Dept. OFAC list (check with Operations personnel for a list of those countries or go to <http://www.treas.gov/offices/enforcement/lists/>)
- Accounts for foreign public officials (individuals in high office in other countries, their families and close associates, political party officials)

7.17.4.12 Lack Of Customer ID Verification

When CIM Securities cannot form a reasonable belief that it knows the true identity of a customer, CIM Securities will:

- not open an account
- impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity
- close an account after attempts to verify customer's identity fail

For **customers who fail to provide required ID or documents within 5 days of account opening**, the account will be restricted to liquidating transactions only until satisfactory ID verification is received.

For **accounts where non-documentary verification results in substantive, unresolved discrepancies** (information that is inconsistent such as name, address, taxpayer ID number, *etc.*), either the account will not be opened or will be immediately closed.

Where inability to verify raises questions about the customer, filing a Suspicious Activity Report will be considered (see the section *Suspicious Activity Reports*).

Questions regarding accounts that do not comply with requirements to verify customer ID should be referred to the AML Compliance Officer.

7.17.4.13 Customer Notice

Customers are provided notice, prior to opening an account, that their identification will be verified. This notice may be on CIM Securities's web site, on new account applications, or in other disclosures provided at the time of account opening.

7.17.5 CIP Records

Customer identification verification records are retained with new account application records in accordance with rule recordkeeping requirements and the terms of the other financial institution's CIP including:

- all identifying information recorded on the new account application
- documentary verification including information from or copies of government-issued IDs or passports
- non-documentary verification
- account approval or disapproval
- resolution of discrepancies
- referral of the account to the AML Compliance Officer
- closing of an account that fails to meet CIP requirements
- other records as may be required

Records are retained for at least 5 years after the account is closed.

7.17.6 Comparison With Government Lists

As required by law, CIM Securities compares customer information against government lists. The section *OFAC List And Blocked Property* in the Anti-Money Laundering Program describes comparison of accounts with lists published by the Treasury Dept.

7.18 Identity Theft Prevention Program (Red Flags Rule)

[Exchange Act Regulation S-ID; Fair and Accurate Credit Transactions Act (FACT Act) Section 114 and 315; FINRA Regulatory Notice 19-18; FINRA Red Flags Rule web site: <https://www.finra.org/rules-guidance/key-topics/customer-information-protection/ftc-red-flags-rule>; Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation: <http://www.govcollect.org/files/Appendix%20A%20to%20Part%20681.pdf>]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • New account information • Order records • Transaction information about cash or security transfers • Information reported by employees • Information from third party providers, customers, victims of identity theft, law enforcement agencies or others about potential identity theft
Frequency	<ul style="list-style-type: none"> • When new accounts are opened • When account addresses are changed • Ongoing - review of order records and transaction information • As received - employee information • As required - when a third party is engaged, confirm third party providers (including clearing firms) have identity theft program procedures which may be included in an affirmation in the third party's contract with CIM Securities • Annually - review of controls and procedures • As required - provide revised procedures to the Board, Board committee, or CEO • Annually - report to CEO • Annually (or more frequently) - provide training for employees
Action	<ul style="list-style-type: none"> • Establish and maintain the Identity Theft Program <ul style="list-style-type: none"> ○ Provide initial Program and subsequent material changes to the Board, a Board Committee or CEO (if no Board exists) for review and approval ○ Review controls and procedures annually as part of the annual testing described in the chapter <i>SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS</i> • Conduct reviews of orders and transactions to identify red flags • When red flags are identified, take corrective action which may include: <ul style="list-style-type: none"> ○ Consultation with the RR and/or supervisor ○ Monitoring the account ○ Contacting the customer ○ Changing passwords, security codes, or other security devices that permit access to an account ○ Reopening an account with another account number ○ Not opening a new account ○ Closing an existing account ○ Filing a Suspicious Activity Report ○ Notifying law enforcement ○ Taking no action if warranted • Conduct other reviews which may include:

	<ul style="list-style-type: none"> ○ Periodic use of internet search engines to identify web sites using CIM Securities's or an RR's name ○ Review online advertising to identify web sites for unauthorized links to promote stock fraud or that appear to be illegitimate • If CIM Securities's or an RR's identity is being used in a scam, take action which may include notifying regulators and the FBI, lodging a complaint at www.ftc.gov, and if it involves email solicitation or spoofing, forwarding email to spam@uce.gov • If a customer's account has been compromised, take action (described in a section that follows) • Include Identity Theft Prevention Program in the annual report to CEO (see the chapter <i>SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS</i>), reporting: <ul style="list-style-type: none"> ○ Effectiveness of the policies and procedures in addressing the risk of identity theft ○ Third party provider arrangements ○ Significant incidents involving identity theft and management's response ○ Recommendations for material changes to the Program • Review third party providers (including clearing firms) for adequacy of identity theft programs <ul style="list-style-type: none"> ○ Contractually require them to have policies and procedures to detect Red Flags included in firm policies and report them to CIM Securities and/or take appropriate steps of their own to prevent/mitigate identity theft • Send confirmation of address change to the customer's old address when a change of address is made (see the section <i>Change Of Addresses On Accounts</i> in the chapter <i>FINANCIAL AND OPERATIONS PROCEDURES</i>) • Training: <ul style="list-style-type: none"> ○ Include identity theft in AML training ○ Develop training, identify target employees, and administer training
Record	<ul style="list-style-type: none"> • Policies and procedures and revisions • Reviews of orders and transactions with record of action taken • Red flags identified and record of action taken • Annual testing of procedures (see <i>SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS</i>) • Annual report to CEO (see <i>SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS</i>) • Confirmation that third party providers (including clearing firms) have adequate ITPPs and include in the contracts with third parties • Records of training including subjects included, date, who administered and who attended

7.18.1 Introduction – ITPP Not Applicable at Present Time (7.18.1-7.18.3)

Under Regulation S-ID, financial institutions with "covered accounts" are required to establish an Identity Theft Prevention Program (ITPP) to prevent, detect, and act on the theft of customers' identity. "Covered account" includes an account for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and any other accounts (for individuals or entities) where there is a reasonable foreseeable risk to customers or the safety or soundness of CIM Securities including financial, operational, compliance, reputational, or litigation risks.

7.18.2 Establishment, Administration, And Updates Of The ITPP

The AML Compliance Officer is responsible for:

- Establishing the program and obtaining Board, Board committee, or CEO approval
- Updating the program when necessary and communicating changes to appropriate personnel including the Board/CEO
- Administering the program including:
 - identifying supervisors' responsibilities and communicating those responsibilities to respective supervisors
 - monitoring regulatory changes and industry trends
- Establishing training for supervisors and RRs
- Maintaining records of the ITPP and any updates
- Maintaining records of training or delegation of training to supervisors; records include subjects covered, who administered the training, date of training, and who attended

7.18.3 Red Flags

The ITPP is based on identifying "red flags" that indicate identity theft may have occurred. This section describes CIM Securities's methods of identifying red flags and responding to them. Regulators have identified red flags as potential indicators of identity theft. All of the red flags may not apply to CIM Securities because of the nature of its business and types of customers. The following section identifies red flags, how they are detected, and potential action when red flags are identified.

The following factors were considered in establishing the ITPP and are assessed in annual reviews of the program in determining identity theft risks at CIM Securities:

- Types of accounts offered by CIM Securities
- Methods to open and access accounts
- Prior experience with identity theft
- Regulatory/industry releases and industry experience with identity theft
- Technology/reports available to identify red flags
- Use of third parties (including clearing firms) for processing accounts and/or transactions
- Sources of red flags including: reports from credit agencies; suspicious documents; suspicious personal identifying information; suspicious account activity; and notice from other sources, including the customer himself/herself

This list is not intended to be an exhaustive or mandatory list of items but provides guidelines for where risks may appear. Some areas may not be relevant to CIM Securities's business at a particular time.

7.18.4 Identifying And Responding To Red Flags

The following chart identifies identity theft red flags and potential responses which depend on the nature and seriousness of the red flags. **In addition, refer to FINRA Regulatory Notice 19-18 for a comprehensive list of potential red flags.**

Red Flag	Action
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	

1. A fraud or active duty alert is included on a consumer credit report.	Verify that the fraud or active duty alert covers an applicant or customer and review the allegations in the alert.
2. A notice of credit freeze is given in response to a request for a consumer credit report.	Verify that the credit freeze covers an applicant or customer and review the freeze.
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	Verify that the notice of address or other discrepancy covers an applicant or customer and review the address discrepancy.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	Verify that the consumer credit report covers an applicant or customer, and review the degree of inconsistency with prior history.
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Scrutinize identification presented in person to make sure it is not altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.	Determine that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the identification presenter is saying.	Determine that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Determine that the identification presented and other information we have on file from the account are consistent.
9. The application looks like it has been altered, forged or torn up and reassembled.	Scrutinize each application to identify alterations or forgery (for example, a form that has been cut up and reassembled).
Category: Suspicious Personal Identifying Information	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	Check personal identifying information to determine that the SSN given has been issued but is not listed on the SSA's Master Death File. If we receive a consumer credit report, check to see if the addresses on the application and the consumer report match.
11. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	Check personal identifying information to confirm that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Compare the information presented with addresses and phone numbers on accounts or applications that were reported to be fraudulent.
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop,	Validate the information presented when opening an account by looking up addresses on the Internet to

or a prison; or a phone number is invalid, or is for a pager or answering service.	ensure they are real and not for a mail drop or a prison; call the phone numbers given to ensure they are valid and not for pagers or answering services.
14. The SSN presented was used by someone else opening an account or other customers.	Compare the SSNs presented to see if they were given by others opening accounts or other customers.
15. The address or telephone number presented has been used by many other people opening accounts or other customers.	Compare address and telephone number information to see if they were used by other applicants and customers.
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Track when applicants or customers have not responded to requests for required information and follow up with the applicants or customers to determine why they have not responded.
17. Inconsistencies exist between what is presented and what our firm has on file.	Verify key items from the data presented with information we have on file.
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	Authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
19. Soon after CIM Securities gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	Operations (or the clearing firm) verifies change of address requests by sending a notice of the change to both the new and old addresses so the customer will learn of any unauthorized changes and can notify CIM Securities.
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.	Review new account activity to ensure that first and subsequent payments are made, and that credit is primarily used for other than cash advances and securities easily converted into cash.
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	Review accounts on at least a monthly basis and check for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or a big change in spending or electronic fund transfers.
22. An account that is inactive for a long time is suddenly used again.	Review our accounts on at least a monthly basis to see if long inactive accounts become very active.
23. Mail CIM Securities sends to a customer is returned repeatedly as undeliverable even though the account remains active.	Note any returned mail for an account and immediately check the account's activity.
24. We learn that a customer is not getting his or her paper account statements.	Record on the account any report that the customer is not receiving paper statements and immediately investigate them.
25. We are notified that there are unauthorized charges or transactions to the account.	Verify if the notification is legitimate and involves a firm account, and then investigate the report.
Category: Notice From Other Sources	

26. An outside agency, law enforcement, a clearing firm, or other source notifies CIM Securities that an account has been opened or used fraudulently.	Verify that the notification is legitimate and involves a firm account, and then investigate the report.
27. CIM Securities is notified of potential unauthorized access to customer personal information due to data loss from an outside provider or a breach of an outside provider's data.	In consultation with the outside provider, determine the extent of the loss of data or breach of the provider's systems and determine action to be taken which may include notification of customers and notification of regulatory authorities including states depending on state requirements.
28. Notice from a customer of the loss of information (e.g., loss of wallet, birth certificate, etc.).	Contact the customer to learn the details of the unauthorized access to determine if other steps are warranted.

7.18.5 Compromised Accounts

[FINRA Checklist for Compromised Accounts: <https://www.finra.org/rules-guidance/key-topics/customer-information-protection/firm-checklist-compromised-accounts>]

If an unauthorized person may have gained entry or attempted entry to a customer's account, the AML Compliance Officer will take the following actions, depending on the nature and scope of the intrusion.

- Monitor, limit, or temporarily suspend activity in the account
- Contact the customer using CIP information on file for him/her, describe what has been found, and verify that there has been an attempted or actual identity theft
- Determine if there is a heightened risk of ease of access such as a customer's lost wallet, mail theft, a data security incident, or the customer gave account information to an imposter claiming to represent CIM Securities or the customer gave information to a fraudulent web site
- Check similar accounts where there may be unauthorized access
- Collect incident information including (if available):
 - Firm information (both introducing and clearing firms: firm name, CRD number, contact name and telephone number)
 - Dates and times of activity
 - Securities involved (name and symbol)
 - Details of trades or unexecuted orders
 - Details of wire transfer activity
 - Customer accounts affected by the activity including name and account number
 - Whether the customer will be reimbursed and by whom
- Alert other appropriate firm personnel to be aware of unusual activity in other customer accounts and notify the AML Compliance Officer of any such incidences
- Identify, to the extent possible, the cause of the account intrusion (*i.e.*, the firm's system was compromised; individual account was hacked); whether the customer has been subject to identity theft; whether intrusion is limited to one account or whether it involves multiple accounts
- Notify clearing firm, if applicable
- Contact the SEC, FINRA, and state regulators
- If appropriate, contact law enforcement such as the FBI or the U.S. Postal Inspector, if mail is involved
- Determine whether CIM Securities must provide a specific type of notification to the customer or others under state law
- Determine whether a SAR should be filed
- Review CIM Securities's insurance policy which may require timely notice or prior consent for any settlement
- Provide customer assistance to minimize the impact of potential or actual identity theft, as applicable and determined by the AML Compliance Officer:
 - Consider changing passwords, security codes or other ways to access threatened accounts

- Offer to close the account and reopen with a new account number
- Consider not collecting on the account or selling it to a debt collector
- Advise the customer to go to the FTC Identity Theft Web Site (<http://www.ftc.gov/bcp/edu/microsites/idtheft>); calling the FTC's Identity Theft Hotline (877-438-4338); or writing the Identity Theft Clearinghouse (FTC, 6000 Pennsylvania Avenue, NW, Washington, D.C. 20580)

7.19 Due Diligence For Correspondent And Private Banking Accounts

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 312 and 313]

Note: CIM does not open Correspondent and Private Banking Accounts

Responsibility	<ul style="list-style-type: none"> • AML Compliance Officer
Resources	<ul style="list-style-type: none"> • New account application • Foreign bank certification • Information about a foreign bank subsequent to opening that indicates it is a foreign shell bank where an account may not be maintained
Frequency	<ul style="list-style-type: none"> • As required when accounts are opened • Monthly - review of accounts identified for due diligence reviews
Action	<ul style="list-style-type: none"> • Conduct due diligence for correspondent and private banking accounts • Review selected accounts for potential money laundering activity and, if potential activities are identified, take corrective action which may include: <ul style="list-style-type: none"> ○ Restricting activity in the account ○ Closing the account ○ Filing an SAR • For foreign bank accounts: <ul style="list-style-type: none"> ○ Review certification to determine: <ul style="list-style-type: none"> ▪ All required information is included ▪ Inconsistencies (<i>i.e.</i>, location of the foreign bank's regulated affiliate is consistent with the designated banking authority that supervises the foreign bank and its regulated affiliate) ○ Ensure procedures are in place to restrict transactions in accounts that do not provide certification within 30 days of opening the account ○ Close existing prohibited accounts for foreign shell banks ○ Review re-certifications ○ Ensure procedures are in place to re-certify foreign banks within three years of original certification
Record	<ul style="list-style-type: none"> • Record of the AML Officer's review is maintained in new account records on the applicable form: <ul style="list-style-type: none"> ○ New account application ○ Certification form ○ Re-certification form • Records of account reviews including corrective action taken • Records of closing or restricting accounts are retained with new account records

Due diligence requirements apply when opening and handling correspondent and private banking accounts that are maintained in the U.S. for non-U.S. persons. "Enhanced due diligence" is required for:

- Correspondent accounts for foreign banks in jurisdictions of money laundering concern or operating under an off-shore license
- Private banking accounts for senior foreign political figures

The purpose of these requirements is to detect and report known or suspected money laundering activity.

7.19.1 Definitions

Correspondent account: Includes any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign institution, or to handle other financial transactions related to such foreign financial institution. This type of account presumes a formal relationship through which the financial institution provides regular services.

Private banking account: A private banking account is an account that is established or maintained for the benefit of one or more non-U.S. persons, requires minimum aggregate deposit of funds or other assets of not less than \$1,000,000, and is assigned to a bank employee who is a liaison between the financial institution and the non-U.S. person. If the account otherwise satisfies the definition but the institution does **not** require a minimum balance of \$1,000,000, the account does not qualify as a private banking account.

Senior foreign political figure ("politically exposed person") includes:

- a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise (Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources.)
- immediate family members of the above, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure
- a corporation, business, or other entity formed by or for the benefit of one of the above individuals
- a person "widely and publicly known" as a close associate of such a person

Proceeds of foreign corruption: any asset acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and include any other property into which any such assets have been transformed or converted.

Foreign bank: defined under the Bank Secrecy Act as a bank organized under foreign law, or an agency, branch, or bank office located outside the United States. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

Foreign shell bank: a foreign bank without a physical presence in any country.

"Owner" of a foreign bank for purposes of enhanced due diligence: Any person who directly or indirectly owns, controls, or has the power to vote 10% or more of any class of securities of the bank.

Payable-through account: A correspondent account maintained by a covered financial institution for a foreign bank by means of which the foreign bank permits its customers to engage, either directly or through a subaccount, in banking activities usual in connection with the business of banking in the U.S.

Regulated affiliate: a foreign shell bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or a foreign country, as applicable; and (2) is subject

to supervision by a banking authority in the foreign country regulating such affiliated depository institution, credit union, or foreign bank.

7.19.2 Due Diligence For Correspondent Accounts For Foreign Financial Institutions

Due diligence requirements apply to the following types of foreign financial institutions:

- Foreign bank
- Foreign branch of a U.S. Bank
- A business organized under a foreign law that, if located in the U.S., would be a securities broker-dealer, futures commission merchant, introducing broker in commodities, or a mutual fund
- A money transmitter or currency exchanger organized under foreign law

The Dept. of Treasury has established the following minimum due diligence requirements:

- determine whether the account is subject to enhanced due diligence
- assess the money laundering risk posed, based on risk factors. Potential risk factors include:
 - the nature of the foreign financial institution's business and the markets it serves
 - the type, purpose, and anticipated activity of the correspondent account
 - the nature and duration of CIM Securities's relationship with the foreign financial institution
 - the AML and supervisory regime in which the foreign financial institution is chartered or licensed
 - information known or reasonably available to CIM Securities about the foreign financial institution's AML record
- apply risk-based policies, procedures and controls to each account, including periodic review of activity

Factors considered in determining due diligence include:

- nature of services provided to the account
- length of relationship
- the AML supervisory regime in the account's home country
- any information known or reasonably available about the account's AML record

Due diligence procedures include the following:

Correspondent accounts for foreign financial institutions are forwarded to the AML Compliance Officer, at the time of opening, for review.

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
 - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including source of revenue and assets, whether the person/entity has existing accounts with CIM Securities, length of time the RR has known the account, who referred the account, and other available information about account background and how the account came to CIM Securities.
- Conduct a risk-based assessment considering factors listed above.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.
 - File a SAR, if appropriate.
- If the account is approved for opening, determine whether ongoing review is necessary.
 - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer.
 - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

7.19.2.1 Enhanced Due Diligence For Some Foreign Banks

Enhanced due diligence is required for a correspondent account for a foreign bank that is operating:

- under an offshore license;
- under a license issued by a country that has been designated as being non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the U.S. is a member and with which the U.S. concurs regarding the designation; or
- under a license issued by a country designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

Such accounts are subject to risk-based enhanced due diligence, including the following:

- Compliance is responsible for identifying and monitoring such accounts.
- If the bank's shares are not publicly traded, identify the owners of the bank and verify they do not appear on U.S. lists of restricted individuals or companies.
- Obtain and consider information about the bank's AML program to assess money laundering risk.
- Obtain information from the bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account and the sources and beneficial owner of funds or other assets in the payable-through account.
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by CIM Securities and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks.
- Monitor such accounts for potential money laundering, either manually or electronically depending on available information.
- Report the account, upon initial review or in the course of monitoring, if necessary.

If enhanced due diligence cannot be performed, the account will not be opened, trading will be suspended, a suspicious activity report will be filed, and/or the account will be closed.

7.19.2.2 Prohibition Against Correspondent Accounts For Foreign Shell Banks

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 313]

CIM Securities is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank. The prohibition does not apply to a foreign shell bank that is a regulated affiliate. If an account is inadvertently opened for an unregulated foreign shell bank, the AML Compliance Officer must be notified and the account will be immediately closed.

7.19.2.3 Foreign Bank Certification

[FinCEN Frequently Asked Questions re Certification: <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-foreign-bank-recertifications>]

When opening an account for a foreign bank, CIM Securities is obligated to ensure the bank is not a foreign shell bank and must obtain information about the foreign bank's owners and an agent for service of process. The bank must complete the Foreign Bank Certification which must be submitted to the AML Compliance Officer with a copy of the new account application for review. Every three years the bank is also required to re-certify the information filed with CIM Securities.

7.19.2.4 Special Measures

[USA PATRIOT Act Section 311; Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart F; FINRA Notice to Members 06-41]

Some foreign jurisdictions, foreign financial institutions, international transactions, or types of accounts are designated to be of "primary money laundering concern" by the Secretary of the Treasury. This designation obligates CIM Securities to take certain "special measures" against the primary money laundering concern. The Secretary of Treasury announces when an entity is considered to be a primary money laundering concern. These special measures include:

- A prohibition against opening or maintaining a correspondent account in the U.S. for or on behalf of the primary money laundering concern including at the time of announcement, review of existing account records to identify any prohibited accounts
- Notification to correspondent account holders that the account may not be used to provide the primary money laundering concern with access to CIM Securities [sample notification is included in Notice to Members 06-41 and may be transmitted by a one-time notice by mail, fax, or e-mail or by including the information in the next regularly occurring transmittal to the account, such as an account statement]
- Reasonable steps to identify an indirect use of correspondent accounts by the primary money laundering concern by review of transaction-based records

The clearing firm is responsible for complying with special measures including notification of correspondent accounts and retaining records of compliance.

7.19.3 Due Diligence For Private Banking Accounts

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F]

Private banking accounts:

- include accounts established for a non-U.S. beneficial owner.
- include accounts where the beneficial owner is an individual:
 - who has a level of control over, or entitlement to, the funds in the account
 - who directly or indirectly controls, directs, or manages the account
 - for whom an account is established, maintained, or administered in the U.S.
- exclude accounts for hedge funds (and other pooled vehicles) and corporations (that are not personal investment companies ["PICs"]).
- include accounts for PICs and trusts for the benefit of individual owners.

Requirements for due diligence:

- Determine the identity of all nominal and beneficial owners of the private banking account.
- Determine the purpose and expected use of the account.
- Determine whether any such owner is a senior foreign political official.
- Determine the source(s) of funds deposited into the private banking account and the purpose and expected use of the account.
- Review the account activity:
 - to ensure consistency with information about the account.
 - to report suspected money laundering activity.

Factors considered in determining due diligence include:

- Is the client from a jurisdiction identified by the federal government as a jurisdiction subject to OFAC restrictions or as having weak AML controls?

- Is the customer's business cash intensive?

CIM Securities cannot rely on foreign institutions to perform due diligence for private banking accounts, and due diligence obligations are ongoing. If appropriate due diligence cannot be performed for the account, the account will be closed.

7.19.4 Enhanced Scrutiny For Accounts Of Senior Foreign Political Figures

Accounts for senior foreign political figures (including persons and entities defined in this section) are subject to enhanced scrutiny:

Prior to opening, the account is referred to the AML Officer for review and approval.

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
 - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including employment history, sources of income and assets, whether the person/entity has existing accounts with CIM Securities, length of time the RR has known the account, who referred the account, and other available information about account background of the account and how the account came to CIM Securities.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.
 - File a SAR, if appropriate.
- If the account is approved for opening, determine whether ongoing review is necessary.
 - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer.
 - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity and report such activity if necessary and close the account.

7.20 Shell Companies

[FinCEN advisory on shell companies: <https://www.fincen.gov/resources/statutes-regulations/guidance/potential-money-laundering-risks-related-shell-companies>]

Shell companies can represent a potential money laundering risk. Most shell companies are formed for legitimate business reasons, but some have been used for illicit purposes.

"Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. Legitimate purposes including holding stock or intangible assets of another business entity (such as subsidiary company shares) but are not engaged in active business operations or facilitating domestic and cross-border currency and asset transfers and corporate mergers. State laws allow shell companies to obscure company structure, ownership, and activities, so there is little transparency to enable CIM Securities to understand with whom they are dealing.

Agents that act as intermediaries or nominee incorporation services (NIS) can play a central role in creating, maintaining, and supporting shell companies. Some agents and NIS firms also provide individuals and businesses with nominee services that preserve the anonymity of underlying officers, directors, and stockholders.

Shell companies are subject to review which may include:

- Checking accounts and owners (if information is available) against OFAC restrictions (applies to all accounts)
- Obtaining information about underlying owners
- Obtaining assurances from the shell company representative that principals have been screened

8 INSIDER TRADING

[Insider Trading and Securities Fraud Enforcement Act of 1988; SEC Securities Exchange Act of 1934 Rule 10b-5; FINRA Notice to Members 89-5; SEC Staff Summary Report on Examinations of Information Barriers: <http://www.sec.gov/about/offices/ocie/informationbarriers.pdf>; SEC Guidance on the use of company web sites (application of Regulation FD): <http://www.sec.gov/rules/interp/2008/34-58288.pdf>; <http://www.sec.gov/about/offices/ocie/informationbarriers.pdf>]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor • Compliance
Resources	<ul style="list-style-type: none"> • Daily Transaction Report • Employee transactions (see the section <i>Employee, Employee-Related and Proprietary Trading</i>) • Customer and proprietary and affiliate asset management (if applicable) transactions • Restricted and watch lists • Inquiries from regulators • Transactions in securities on CIM Securities's Watch or Restricted Lists (see the sections <i>Watch List</i> and <i>Restricted List</i>) • Questions or transactions referred by managers or other firm personnel • Access controls including key card controls, computer networks
Frequency	<ul style="list-style-type: none"> • Daily and as required • Monthly - Review of controlled access • Annually and ongoing - develop and provide training
Action	<ul style="list-style-type: none"> • Supervisors reviewing trades: refer questioned trades to Compliance • Compliance will review the referred transaction and take appropriate action which may include: <ul style="list-style-type: none"> ○ Determination if further information is necessary ○ Consultation with RR or other firm personnel regarding the nature of the transaction(s) including reason for transaction, solicited vs. unsolicited ○ Review of other transactions by the same customer and/or RR ○ Consultation with in-house or outside counsel ○ Referral of transaction(s) to appropriate regulator • Compliance <ul style="list-style-type: none"> ○ reviews transactions (employee/customer/proprietary/affiliate asset management) against restricted and watch lists to identify potential breaches ○ reviews access controls (key cards, network controls) for unauthorized access ○ investigates potential breaches ○ takes corrective action which may include: <ul style="list-style-type: none"> ▪ Contact with affected personnel ▪ Consultation with outside counsel ▪ Disciplinary action ▪ Added training ▪ Referral to regulators

	<ul style="list-style-type: none"> ○ Develop and provide training for all personnel and particularly for those with access to inside information
Record	<ul style="list-style-type: none"> • Initials on Daily Transaction Report by the designated reviewer • Compliance's review of transactions documented to include who conducted the review; when reviewed; identification of the transaction(s) reviewed; copies of the records used to conduct the review; and notation of action taken • Compliance review of controlled access and corrective action taken, if applicable • Compliance and supervisors' records of employee training on insider trading

8.1 Insider Trading Policies And Procedures

Broker-dealers are required to establish, maintain, and enforce policies and procedures to prevent the misuse of material non-public information ("inside information"). These requirements are included in the Insider Trading and Securities Fraud Enforcement Act of 1988. CIM Securities has established policies and procedures reasonably designed to prevent the misuse of inside information considering CIM Securities's business, structure, size and other relevant factors.

At the time of hire, employees are provided with the *Firm Policy Memorandum Regarding Insider Trading* included in this chapter. Updates to this policy are provided by Compliance when required.

8.2 Prohibition Against Acting On Or Disclosing Inside Information

CIM Securities policy prohibits employees and associated persons from effecting securities transactions while in the possession of material, non-public information. Employees are also prohibited from disclosing such information to others. The prohibition against insider trading applies not only to the security to which the inside information directly relates, but also to related securities, such as options or convertible securities.

If employees receive inside information, they are prohibited from trading on that information, whether for the account of CIM Securities or any customer, or their own account, any accounts in which they have a direct or indirect beneficial interest (including accounts for family members) or any other account over which they have control, discretionary authority or power of attorney.

8.3 Tippees Are Insiders

An employee may, depending on the circumstances, become an "insider" or "tippee" when obtaining **apparently** material, non-public information by happenstance, including information derived from social situations, business gatherings, overheard conversations, "tips" from "insiders," or other third parties. In these situations, the employee must, **unless Compliance advises otherwise**, treat the information as inside information and comply with all of the policies on insider trading.

8.4 Misuse Constitutes Fraud

The misuse of material, nonpublic or "inside" information constitutes fraud, a term broadly defined under federal securities laws. Engaging in fraud is subject to civil and criminal penalties (including imprisonment), SEC administrative actions, disgorgement of profits, penalties from exchanges, and dismissal by CIM Securities. There are no circumstances where any person becomes aware of inside information, for whatever purpose, may use that information to trade for personal benefit, for CIM Securities's benefit, or for the benefit of another. If any employee believes he or she has received inside information, he or she should immediately advise their supervisor or Compliance.

8.5 Annual Certification

Employees and associated persons are required to annually certify their knowledge of and compliance with CIM Securities's insider trading policy. This certification is included in the Annual Certification form.

8.6 Firm Policy Memorandum Regarding Insider Trading

This policy memorandum is intended to provide information and guidance concerning the restrictions on insider trading, which is an enforcement priority of the Securities and Exchange Commission and the Department of Justice. It also explains policies adopted by CIM Securities to prevent fraudulent or deceptive practices relating to trading on material, non-public information ("insider trading"). Trading in securities on the basis of material, non-public information ("inside information") is prohibited and contrary to firm policy. The penalties for insider trading can be considerable, including loss of profits plus treble damages, criminal sanctions including incarceration, loss of employment and permanent bar from the securities industry. This policy applies to all associates of CIM Securities. Specific departments of CIM Securities may have insider trading policies that supplement this policy.

READ THIS MEMORANDUM VERY CAREFULLY. You will be asked to sign a statement affirming that you have read and understand the policies set forth herein and that you will abide by them.

THE PROHIBITION

The prohibition against insider trading includes the following: if you are in possession of material non-public information about a company or the market for a company's securities, you must either publicly disclose the information to the marketplace or refrain from trading. Generally, disclosure is not an option and the effect is to require an individual to refrain from trading. You also may not communicate inside information to a second person who has no official need to know the information.

Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in deciding to buy or sell a security. In addition, information that, when disclosed, is likely to have a direct effect on a security's price should be treated as material. Examples include information concerning impending tender offers, leveraged buy-outs, mergers, sales of subsidiaries, significant earnings changes and other major corporate events.

Information is non-public when it has not been disseminated in a manner making it available to investors generally. Information is public once it has been publicly disseminated, such as when it is reported on the Dow Jones or other news services or in widely disseminated publications, and investors have had a reasonable time to react to the information. Once the information has become public or stale (*i.e.*, no longer material), it may be traded on or disclosed freely.

Generally, a person violates the insider trading prohibition when that person violates a duty owed either to the person on the other side of the transaction or to a third party (such as a customer or employer) by trading on or disclosing the information. The insider trading prohibition applies to an issuer's directors, officers and employees, investment bankers, underwriters, accountants, lawyers and consultants, as well as other persons who have entered into special relationships of confidence with an issuer of securities.

Virtually anyone can become subject to the insider trading prohibition merely by obtaining material non-public information by unlawful means or by lawfully obtaining such information and improperly using it. This is known as misappropriation. If you receive material, non-public information as part of your legitimate business dealings on behalf of CIM Securities or its customers and you use that information to trade in securities or if you transmit that information to another person for purposes of trading in securities (so-called "tipping"), you would likely be guilty of insider trading. Insider trading liability may also be derivative. A person who has obtained inside information (so-called "tippee") from a person who has breached a duty or who has misappropriated information may also be held liable.

The foregoing is just a synopsis of the insider trading prohibition. Because the law in this area is complex, CIM Securities has adopted the following guidelines which are designed to prevent violations of the insider trading rules.

WHEN CIM Securities IS AN INSIDER

CIM Securities may be deemed an insider when it comes into possession of inside information through its various activities such as investment banking and research. Research analysts may become insiders (or tippees) upon receiving inside information from a company officer, director or employee. In addition, the intention to update or downgrade a research recommendation might be material information and should not be disclosed, prior to public dissemination, to anyone outside the Research Department (and in some instances to some within the Research Department) unless there is a need to know the information.

CIM Securities will remain an insider as long as it has inside information, regardless whether the prospective banking client decides to engage another investment banking firm or whether CIM Securities declines to accept the proposed engagement.

REGULATION FD (FAIR DISCLOSURE)

SEC Regulation FD governs the release by public companies of information that may reasonably be expected to affect the market price of securities issued by the public company. While obligations under the Regulation fall primarily on public companies, it is equally important for employees of CIM Securities to be aware of the requirements and to act appropriately if an employee becomes privy to inside information about the company. Further explanations for research personnel and investment bankers are included in the chapters *INVESTMENT BANKING* and *RESEARCH*.

The goal of the Regulation is to create a "level playing field" so that the dissemination of information that is reasonably likely to affect the market price of a security is released simultaneously to all investors. In general, the issuer, its executive officers, directors, investor relations personnel or other employees with similar duties are prohibited from selectively disclosing material, nonpublic information to securities analysts, to other securities professionals, or to a shareholder when it is foreseeable that a recipient of such information will trade on the information. The Regulation requires action by the issuer if there is intentional or unintentional selective disclosure of such information.

Employees must not expect or seek to obtain, other than in the normal course of confidential investment banking activities, material non-public information from issuers and their employees.

GUIDELINES

TREATMENT OF CUSTOMER INFORMATION. CIM Securities considers confidential all information concerning its customers including, by way of example, their financial condition, prospects, plans and proposals. The fact that we have been engaged by a company as well as the details of that engagement are also confidential. CIM

Securities's reputation is one of its most important assets. The misuse of customer information can damage that reputation as well as customer relationships.

WHAT TO DO IF YOU LEARN INSIDE INFORMATION. It is not illegal to learn inside information. CIM Securities learns material non-public information from its customers and is permitted to use that information in a lawful manner to advise and assist them. It is, however, illegal for you to trade on such information or to pass it on to others who have no legitimate business reason for receiving such information.

If you believe you have learned inside information, other than in the ordinary course of business (such as investment bankers who learn inside information when working on an engagement), contact Compliance immediately so that we may address the insider trading issues and preserve the integrity of CIM Securities's activities. Do not trade on the information or discuss the possible inside information with any other person at CIM Securities. If you become aware of a breach of these policies or of a leak of inside information, advise Compliance immediately.

INVESTIGATIONS OF TRADING ACTIVITIES. From time to time, the Exchanges, FINRA and the SEC request information from CIM Securities concerning trading in specific securities. Requests for information should be referred directly to Compliance. You may be asked to sign a sworn affidavit that, at the time of such trading, you did not have any inside information about the securities in question. Your employment may be terminated if you refuse to sign such an affidavit. CIM Securities may submit these affidavits to the Exchanges, FINRA or SEC.

STEPS YOU CAN TAKE TO PRESERVE THE CONFIDENTIALITY OF MATERIAL NON-PUBLIC INFORMATION.

If you are in a position within CIM Securities to access inside information, the following are steps you must take to preserve the confidentiality of inside information:

1. Material inside information should be communicated only when there exists a justifiable reason to do so on a "need to know" basis inside or outside CIM Securities. Before such information is communicated to persons within CIM Securities, your department, or another person you believe needs to know, contact your department manager or Compliance.
2. Do not discuss confidential matters in elevators, hallways, restaurants, airplanes, taxicabs or any place where you can be overheard.
3. Do not leave sensitive memoranda on your desk or in other places where they can be read by others. Do not leave a computer terminal without exiting the file in which you were working.
4. Do not read confidential documents in public places or discard them where they can be retrieved by others. Do not carry confidential documents in an exposed manner.
5. On drafts of sensitive documents use code names or delete names to avoid identification of participants.
6. Do not discuss confidential business information with spouses, other relatives or friends.
7. Protect electronic information on laptops and other portable devices by encrypting confidential data.
8. Avoid even the appearance of impropriety. Serious repercussions may follow from insider trading and the law proscribing insider trading can change. Since it is often difficult to determine what constitutes insider trading, you should consult with Compliance whenever you have questions about this subject.

YOUR OWN SECURITIES TRADING. Firm policy is to require all employees to maintain their securities accounts at CIM Securities except with the approval of Compliance. If you have an account outside of CIM Securities and have not already done so, please advise Compliance immediately. This includes outside accounts in which you have a financial interest or direct the trading.

CONCLUSION

CIM Securities has a vital interest in its reputation, the reputation of its associates, and in the integrity of the securities markets. Insider trading would destroy that reputation and integrity. CIM Securities is committed to preventing insider trading and to punishing any employee who engages in this practice or fails to comply with the above steps designed to preserve confidentiality of inside information. These procedures are a vital part of CIM Securities's compliance efforts and must be adhered to.

8.7 Employee, Employee-Related, And Proprietary Trading

Responsibility	<ul style="list-style-type: none"> • CCO, IB Supervisor
Resources	<ul style="list-style-type: none"> • Daily Transaction Report, if applicable • Confirmations/statements for employees' outside accounts
Frequency	<ul style="list-style-type: none"> • Daily
Action	<ul style="list-style-type: none"> • Identify transactions in securities included on CIM Securities's Restricted or Watch Lists (refer to sections on those procedures)
Record	<ul style="list-style-type: none"> • Notations are included in Compliance's files regarding identified transactions including details of each trade, action taken and initials or signature of reviewer.

Employee and proprietary trades, if applicable, are reviewed by Compliance for trades contrary to restrictions because of underwriting activities, other restrictions, and potential insider trading. This review includes review of employees' outside securities accounts to identify transactions in securities on CIM Securities's Restricted List or Watch List.

8.8 Watch List

Note: The Firm's Restricted List also acts as a Watch list.

Responsibility	<ul style="list-style-type: none"> • IB Supervisor, CCO
Resources	<ul style="list-style-type: none"> • Notification of confidential investment banking activities • Notification of pending material research reports/recommendations • Daily Transaction Report • Confirmations/statements for employees' outside accounts
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Maintain confidential Watch List • Review transactions to identify trades in securities on the Watch List including debt and derivative securities • For identified trades: <ul style="list-style-type: none"> ○ Evaluate whether there is a potential breach in CIM Securities's Information Barriers considering solicited vs. unsolicited; timing or unusual nature of transaction ○ For pending research reports, determine whether trading activities must be limited or suspended depending on the materiality of the report/recommendation and its likely affect on market prices ○ Take corrective action, if necessary

Record	<ul style="list-style-type: none"> • Compliance maintains records of: <ul style="list-style-type: none"> ○ Watch Lists, including the date and time a company is added or deleted ○ The name of the person adding or deleting the company ○ Identified trades, including date of review; accounts involved; underlying records possibly including memos, analyses, and statements/confirmations; summary of disposition; and initials/signature of reviewer.
---------------	---

Compliance will maintain a confidential Watch List which will include issues where CIM Securities may be in possession of material, non-public information. This includes pending research recommendations which may affect the market price of the security (debt or equity) and its derivatives. The Watch List is available only to specified CIM Securities personnel. Compliance will monitor daily trading to identify transactions in securities on the Watch List and take action as necessary. Compliance will also record the date and time when an issue is added to and removed from the Watch List.

8.9 10b5-1 Plans

[ABA guidance regarding 10b5-1 plans (<http://www.abanet.org/buslaw/blt/2008-05-06/parris.shtml>)]

Responsibility	<ul style="list-style-type: none"> • Compliance
Resources	<ul style="list-style-type: none"> • RR regarding 10b5-1 plans
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Review the request and the nature of the RR's participation/activity • Approve or disapprove • If approved, provide guidance regarding allowable activities/limitations
Record	<ul style="list-style-type: none"> • Requests, approval/disapproval, and communications regarding guidelines and allowable activities/limitations

Under Rule 10b-5 of the '34 Securities Exchange Act, a person can face insider trading liability for trading securities while aware of material, nonpublic information about the issuer or its securities. 10b-5 also provides some affirmative defenses or exceptions to this liability. One of the defenses for executives subject to knowledge of inside information is the use of a pre-existing trading plan (10b5-1 Plan) that complies with the requirements of 10b-5(c). This section only summarizes requirements and guidelines regarding such plans. The executive at risk for 10b-5 liability is ultimately responsible for conferring with legal counsel and assuring himself or herself that such a plan is structured properly for avoidance of liability.

- The written plan must be adopted before the individual becomes aware of any material, nonpublic information.
- The plan must specify either the amount and price and dates of for purchases or sales or a written algorithm or computer program to determine the amount and price of the securities to be purchased or sold and the dates of purchases or sales.
- The plan must not permit the executive to exercise any subsequent influence over how, when, or whether purchases or sales would be effected under the plan.
- It must be demonstrable that purchases or sales actually took place under the plan.

- There cannot be alterations or deviations from the terms of the plan (changing the amount, price or timing) and cannot be alterations to a corresponding or hedging transaction or position.
- The plan must be entered into in good faith and not as part of a scheme to evade the prohibitions of 10b-5.

The plan may have to comply with the issuer's insider trading policies and procedures and public disclosure of such a plan may be necessary. Other guidelines may strengthen the defensibility of the plan and its execution including eliminating communications between the broker and the executive; avoiding multiple plans for one executive; and minimizing modifications to a plan which may call into question the good faith basis for establishing the plan.

Compliance must be contacted prior to engaging in transactions on behalf of a 10b5-1 plan.

9 ACCOUNTS

This chapter outlines requirements when opening and maintaining accounts for customers. References to "suitability" apply only to those recommendations NOT subject to Regulation Best Interest (BI) which applies to retail customers and is addressed in a separate chapter by that name. Suitability requirements apply to entities and institutions (e.g., pension funds) and natural persons who will not use recommendations primarily for personal, family, or household purposes (e.g., small business owners and charitable trusts). Refer to the chapter *REGULATION BEST INTEREST (BI)* for requirements when dealing with retail customers.

9.1 New Accounts

[SEC Securities Exchange Act of 1934 Rule 17a-3(a)(17); FINRA Rule 2090; FINRA Information Notice 10/21/08 New Account Application Template]

When opening and maintaining customer accounts, CIM Securities and its RRs are obligated to use reasonable diligence to "know the customer" by obtaining essential facts about the customer and the authority of each person acting on behalf of the customer. Key requirements include the following:

- The new account application (which is designed to include information required by rules) must be complete prior to submission for approval. If the customer refuses to provide certain information, this must be indicated on the new account application.
- Where recommendations will be made to a non-institutional customer, account information includes the customer's financial status, tax status, investment objectives, and other information used or to be considered to determine the suitability of recommendations.
- The new account form must be signed by the RR opening the account.
- Under anti-money laundering requirements, the customer's identification must be verified.
- Required account documents, which vary depending on the type of account opened, must be obtained. Failure to obtain required documents may result in closure of the account.
- The customer's new account information will be sent to the customer for verification within 30 days of opening the account and every three years thereafter. When account information is changed, the changed information will be sent to the customer for verification within 30 days of the change.

This section provides an explanation of certain requirements that apply to new accounts.

9.1.1 Trusted Contact Person

[FINRA Rule 2165, 4512(a)(1)(F) and 4512.06; FINRA FAQs: Frequently Asked Questions Regarding FINRA Rules Relating to Financial Exploitation of Senior Investors <https://www.finra.org/rules-guidance/guidance/faqs/frequently-asked-questions-regarding-finra-rules-relating-financial-exploitation-seniors#:~:text=To%20this%20end%2C%20Rule%204512%20%28a%29%20%281%29%20%28F%29,natural%20persons%20from%20being%20named%20as%20trusted%20contacts.>]

Among other required new account information, a trusted contact person should be identified for a "specified adult" under FINRA Rule 2165 which includes natural person customers age 65 or older or who have physical or mental impairments CIM Securities reasonably believes are unable to protect their own interest. At the time of account opening the customer will be notified, in writing (which may include electronic), that CIM Securities is authorized to contact the trusted contact person and to disclose to the trusted person information about the customer's account to address possible financial exploitation, to confirm the specifics of the customer's current contact information, health status, or the identity of any legal guardian, executor, trustee or holder of a power of attorney.

9.1.2 Regulation Best Interest (BI)

Regulation BI applies to new accounts in two key ways:

- New customers must be provided with the Form CRS Relationship Summary at the time the account is opened.
- Recommendations to open accounts are subject to Regulation BI requirements and require provision of the Form.

The standards for making account recommendations in the customer's best interest are included in the chapter: *REGULATION BEST INTEREST (BI)*.

9.1.3 Designation Of Accounts

[FINRA Rule 3250]

All accounts must be in the name of the customer except that an account may be designated by a number or symbol if the customer provides a written statement attesting to the ownership of the account.

9.1.4 Anti-Money Laundering (AML) New Account Requirements

AML rules apply to the opening of new accounts. This section summarizes the more complete requirements explained in the chapter *ANTI-MONEY LAUNDERING (AML) PROGRAM*.

9.1.4.1 Accounts Requiring Approval By The AML Compliance Officer

The following accounts require review and approval by the AML Compliance Officer at the time of opening. The AML Compliance Officer may require additional information for these accounts.

- **Numbered accounts** (accounts designating a number rather than a name as the account name).
- **Any account requesting confidential handling** of its name, mailing of confirmation and statements, *etc.*
- **Accounts domiciled in high risk countries.** Accounts domiciled in countries identified by OFAC or the Financial Action Task Force on Money Laundering (FATF) as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- **Foreign public officials.** Includes individuals in high offices of foreign governments, political party officials and their families and close associates (if known and/or readily identifiable).
- **Correspondent and Private Banking accounts.** See the section *Due Diligence For Correspondent And Private Banking Accounts*.

9.1.4.2 Customer Identification Program (CIP)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; FINRA Notice to Members 03-34; FinCEN Frequently Asked Questions: <https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-customer-identification>; FinCEN No-Action position on CIP requirements under clearing arrangements: FIN-2008-G002; Guidance on Obtaining and Retaining Beneficial Ownership Information, FinCEN Guidance, FIN-2010-G001 March 5, 2010]

New customer accounts are subject to CIP reviews mandated under anti-money laundering rules.

9.1.4.2.1 Definition Of Customer Under CIP Rule

The definition of "customer" under the CIP rule is different than definitions under other rules. Who is a "customer" under this Rule affects CIM Securities's obligations.

Under the CIP rule and for purposes of this section, "customer" is defined as:

- A person that opens a new account.
- An individual who opens a new account for:
 - An individual who lacks legal capacity; or
 - An entity that is not a legal person.

"Customer" does not include a financial institution regulated by a Federal regulator; a bank regulated by a state bank regulator; those exempted under Federal rule include municipalities; or a person with an existing account at CIM Securities providing there is reasonable belief that the true identity of the person is known.

9.1.4.2.2 Accounts Opened By Other Financial Institutions

There are certain accounts opened by financial institutions where the underlying beneficial owners are not subject to customer identification requirements (see *Customer Due Diligence*) or where CIM Securities may rely on the other financial institution to conduct customer due diligence under their own AML program. A key issue is whether the account is a "customer" of CIM Securities. "Customer" accounts are subject to reviews by CIM Securities or by the financial institution opening the account. More detail is included in the AML chapter. CIM Securities is not obligated to conduct due diligence under the Customer Identification Rule in the following circumstances, depending on conditions explained in the AML chapter. Questions should be referred to the AML Compliance Officer.

- Some financial intermediaries such as banks, clearing firms, investment advisers, *etc.* open accounts for their own customers and provide limited information when opening an account to facilitate clearing of transactions or transfer of assets. The beneficial owners of these accounts are not considered "customers" and are not subject to CIM Securities's due diligence reviews.
- CIM Securities may rely on the other financial institutions to conduct reviews of shared customers where it is reasonable to rely on the other institution; the other institution is subject to AML rule requirements; and the other institution enters into a contract attesting to its performance of AML reviews.
- Shared accounts opened by investment advisers are not subject to CIM Securities's review if the investment adviser:
 - is determined to be reasonable to rely upon;
 - is registered with the SEC; and
 - enters into a written agreement with CIM Securities.

9.1.4.3 Master Accounts And Sub-Accounts – Not applicable

[FINRA Regulatory Notice 10-18; SEC National Exam Risk Alert "Master/Sub-accounts:" <http://www.sec.gov/about/offices/ocie/riskalert-mastersubaccounts.pdf>]

Accounts are sometimes established as "master accounts" that represent multiple sub-accounts. Depending on facts and circumstances (discussed below), master/sub-accounts may be recognized as separate customer accounts subject to CIP reviews.

9.1.4.3.1 Description Of Master/Sub-Accounts

A master account may have multiple underlying accounts on behalf of underlying investors; sub-advisers may be authorized to effect transactions without the intermediation of the master account owner. Also, an individual or entity may set up sub-accounts for separate trading strategies or algorithms. Sub-accounts may be used by individual traders or groups of traders. The master account may be another broker-dealer or a partnership that provides its individual partners trading authority over separate sub-accounts.

9.1.4.3.2 Obligations To Conduct CIP Reviews

Except for accounts opened by investment advisers and financial institutions discussed under *Accounts Opened By Other Financial Institutions* and meeting the conditions of that section, when there are separate owners of the sub-accounts, CIM Securities has an obligation to identify the beneficial owners. Indicators that there may be separate owners requiring CIP review of the sub-accounts include:

- The sub-account owner is entering orders for itself.
- CIM Securities has actual notice the sub-accounts have different owners.
- The sub-accounts are separately documented and/or receive separate reports.
- The sub-accounts are addressed separately in terms of transaction, tax or other reporting.
- The services provided to the sub-accounts engender separate surveillance and supervision of the sub-accounts for compliance with rules or for risk management purposes consistent with the review of separately owned accounts.*
- There are financial arrangements or transactions with the sub-accounts, or separate account terms, that reasonably raise questions concerning whether such accounts represent separate beneficial owners.*
- The sub-accounts incur charges for commissions, clearance and similar expenses, separately, based upon the activity only of that subject sub-account.*
- There is evidence of financial transactions or transfers of assets or cash balances that would reasonably evidence separate beneficial ownership of the sub-accounts.*
- CIM Securities (or RR) is aware of or has access to a master account or like agreement that evidences that the sub-accounts have different beneficial owners.
- There is evidence that a party maintaining a master/sub-account arrangement has interposed sub-accounts that have or are intended to have the effect of hiding the beneficial ownership interest.*
- The number of sub-accounts maintained is so numerous as to reasonably raise questions concerning whether such accounts represent separate beneficial owners.*

* Items above would not apply in the case of accounts opened by a registered BD or a bona fide investment adviser.

9.1.4.3.3 Market Access

Where access to markets is provided to master accounts, CIM Securities and the master accounts are subject to SEC Rule 15c3-5 regarding controls on such access. The master account participants must be determined to confirm compliance with Market Access Rule requirements.

Refer to the section *Market Access* that appears in the following chapters:

- ORDERS
- EQUITY TRADING AND MARKET MAKING

- CORPORATE FIXED INCOME SECURITIES SALES AND TRADING
- NYSE FLOOR BROKER PROCEDURES

9.1.4.3.4 Information Security

CIM Securities has procedures to protect information and information systems from unauthorized access, disclosure, tampering, and other breaches of information security. Where there are master accounts with sub-account access to Firm systems, all participants will be required to participate in training, validate their participant authority to trade in sub-accounts; and use Firm-issued passwords which will be periodically changed.

9.1.4.3.5 Surveillance

Transactions for master and sub-accounts are subject to CIM Securities's surveillance to identify potential insider trading and market manipulation activities.

9.1.5 Customer Due Diligence (CDD)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1010, Part 1020, Part 1023, Part 1024 and Part 1026; FinCEN 2016 FAQs: <https://www.ffiiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf>; FinCEN 2018 FAQs: <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-customer-due-0>; FINRA Rule 3310; FINRA Regulatory Notice 18-19 and 17-40]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • New account application and other customer ID information
Frequency	<ul style="list-style-type: none"> • When accounts are opened
Action	<ul style="list-style-type: none"> • Before approving an account, determine that customer identification (ID) verification information is included with the new account application and meets CIM Securities's requirements • For legal entity customers: <ul style="list-style-type: none"> ○ Obtain beneficial ownership certifications ○ Determine whether a threshold lower than 25% ownership is warranted depending on the customer's risk for potential enhanced monitoring or to collect additional information including expected account activity • For non-documentary verification, check the information included with the new account application for completeness and consistency with other customer-provided information (name, address, phone number, taxpayer ID number, etc.) • For unacceptable verification information (incomplete, inconsistent), return the application to the RR for further information or disapprove the account • Identify accounts where CIM Securities may rely on other financial institutions to satisfy CIP requirements and confirm eligibility to rely on exception • Obtain annual certification from other financial institutions • Include beneficial owners in AML monitoring • Provide ongoing training for appropriate personnel

	<ul style="list-style-type: none"> • Designate and identify to FINRA the individual responsible for implementing and day-to-day operations and internal controls of the program and notify FINRA regarding any change in designation
Record	<ul style="list-style-type: none"> • New account records include customer ID verification as well as the supervisor's approval and customer certifications • Identification and verification of reliance on other financial institutions • Annual certifications from other financial institutions • Certifications from legal entity customers or documentation of oral certification, where applicable • Records of training including content, date of training, and attendees • Record of designation to FINRA of responsible person

When opening new accounts, the customer's identity must be verified, as required by federal law. Customer identification (ID) information must be completed on the new account application. This includes, under FinCEN's requirements:

1. customer identification and verification;
2. beneficial ownership identification and certification;
3. understanding the nature and purpose of customer relationships; and
4. ongoing monitoring for reporting suspicious transactions and, on a risk basis maintaining and updating customer information.

Customer ID verification does NOT apply to accounts for:

- persons with an existing account at CIM Securities (unless the account requires approval by the AML Compliance Officer)
- banks
- governmental entities
- issuers of listed equity securities
- other financial institutions subject to regulation by the SEC, CFTC, Federal Reserve Board, OCC, FDIC, Office of Thrift Supervision, or the National Credit Union Administration
- persons opening accounts to participate in an ERISA plan

In addition, for accounts defined as "legal entity customers" (defined below), information must be obtained about beneficial owners. This requirement applies to accounts established May 11, 2018 or later. If CIM Securities becomes aware of a change of beneficial ownership after May 11 for accounts established before that date, the customer's records must be updated under CDD requirements.

9.1.5.1 Definitions

[SEC Securities Exchange Act of 1934 Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

The regulations should be consulted for more complete definitions.

Legal entity customer: corporation; limited liability company; another entity created by a public filing with a Secretary of State or equivalent; general partnership; limited partnership; business trust created through a state filing; or any similar entity formed under federal law. Does not include sole proprietorships, unincorporated associations, and natural persons opening their own account. Other exclusions are a federal- or state-regulated financial institution; political departments and agencies of the U.S. or a State; various different types of entities registered with the CFTC or SEC; and other entities included in the regulation. [Questions 22-28, 2018 FAQs]

Beneficial owner:

- each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (*i.e.*, the ownership prong); and
- a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (*e.g.*, a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (*i.e.*, the control prong).

Ownership and control prongs: The CDD rule utilizes a two-pronged approach to defining a beneficial owner - an ownership prong and a control prong. Under the ownership prong, a beneficial owner is defined as each individual, if any, who, directly or indirectly, owns 25 percent or more of the equity interests of a legal entity customer. However, the rule recognizes that there may be instances when no single individual owns 25 percent or more of the equity interest of the legal entity; in such instances, CIM Securities is still required to collect the required information for one individual who controls, manages or directs the legal entity customer. Under the control prong, a beneficial owner is defined as a single individual with significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager (*e.g.*, a chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president or treasurer) or any other individual who regularly performs similar functions. The ownership and control prongs, although related, are independent requirements. Thus, satisfaction of, or exclusion from, regulatory obligations under one prong does not mean CIM Securities's obligations under the other prong are also satisfied or excluded. [Question 9, 2016 FAQs]

9.1.5.2 Required Customer Information

[SEC Securities Exchange Act of 1934 Rule 17a-3(a)(17)(i)(A); FINRA Rule 4512]

Basic information required **prior to opening the account** includes:

- **Name**
- **Date of birth**, for an individual
- **Address:**
 - for an individual, residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
 - for a non-individual (corporation, trust, *etc.*) a principal place of business, local office, or other physical location.
- **Telephone number**
- **Employment status** (including occupation and whether the person is associated with a broker dealer)
- **Annual income**
- **Net worth** (excluding value of primary residence)
- Account's investment objectives
- For joint accounts, information on each joint owner (financial information may be combined)
- **Taxpayer identification number** for a U.S. person (U.S. citizen or non-individual established or organized under U.S. or state laws).
- **Identification number for non-U.S. person** which may include a taxpayer ID number; passport number and country of issuance; alien identification card number; or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photo or similar safeguard.
- **Beneficial owners** (see the section that follows) including information about the following:
 - the nature and purpose of customer relationships to develop a customer risk profile
 - information sufficient at the time of account opening so customer activity may be assessed for SAR requirements (may include type of customer requesting services; type of account being opened; services or products being used)

In the case of a customer who has applied for a taxpayer identification number but has not yet received it, notation must be made on the new account application that the taxpayer ID has been applied for. The account will be restricted to liquidating transactions if the taxpayer ID number is not received within 5 days of opening the account.

In addition, under FINRA Rule 4512 CIM Securities will retain the name of the RR responsible for the account and, if multiple RRs are assigned to the account, a record indicating the scope of their responsibilities with respect to the account. This requirement does not apply to an institutional account.

9.1.5.3 Accounts For Individuals

When opening an account for an individual, the following information is required:

- An unexpired government-issued identification including a photo and nationality or residence such as a driver's license or passport and record information from it on the new account application, **OR**
- A copy of the photo ID with the new account application. (The photo ID [original or copy] must be seen by the employee opening the account to record the information. This information may NOT be taken from the customer over the phone.)
- If the photo ID is not available at the time the new account application is being completed, the RR is to indicate on the new account application whether the customer will provide a copy of photo ID within 5 days of account opening **OR**, if the customer cannot provide a photo ID, the reason why not.
- If the photo ID is not received within 5 days, the account will be restricted to liquidating transactions only until the ID is received.

If the customer has not appeared in person at CIM Securities's office, "non-documentary" information will ALSO be required, as explained in a section that follows.

If the customer cannot produce the required photo ID, an explanation must be included on the new account application AND non-documentary information will be required to open the account.

9.1.5.4 Accounts For Legal Entity Customers

[SEC Release No. 34-61651: Policy Statement on Obtaining and Retaining Beneficial Ownership Information for Anti-Money Laundering Purposes]

For legal entity customers, information must be obtained and verified regarding beneficial owners [Question 4, 2018 FAQs]. Obligations when opening accounts that include underlying owners or beneficiaries include the following:

- Determine whether the customer is acting as an agent for or on behalf of another, and if so, obtaining information regarding the capacity in which and on whose behalf the customer is acting.
- Where the customer is a legal entity that is not publicly traded in the United States, such as an unincorporated association, a private investment company (PIC), trust or foundation, obtain information about the structure or ownership of the entity so as to allow CIM Securities to determine whether the account poses heightened risk.
- Where the customer is a trustee, obtain information about the trust structure to allow CIM Securities to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.
- Obtain the identities of individuals who satisfy the definition as beneficial owners, either directly or indirectly through multiple corporate structures (complex ownership structures). [Question 3, 2018 FAQs]
- Obtain from the legal entity customer's representative a completed certification form identifying beneficial owners; updating information may require re-certification. [Questions 6 & 16, 2018 FAQs]
[\[https://www.fincen.gov/resources/filing-information\]](https://www.fincen.gov/resources/filing-information)

- Determine the nature and purpose of the customer relationship to determine risk profiles and identify the need for additional monitoring. [Questions 35-37, 2018 FAQs]

If CIM Securities has affiliates with public customers, information may be shared across the enterprise to cross-check beneficial ownership information.

9.1.5.4.1 Reliance On Customer Representations

CIM Securities may reasonably rely on information provided by customers if it has no knowledge of facts that would call into question the reliability of the information.

- There is no requirement to independently investigate a legal entity customer's ownership structure.
- CIM Securities may rely on information provided by the customer to determine if the legal entity is excluded from the definition of legal entity customer.

9.1.5.4.2 Retention Of Beneficial Ownership Information

Identifying information will be maintained for a period of five years after the legal entity's account is closed. Verification records must be maintained for a period of five years after the record is made. CIM Securities will also retain a description of each document relied on for verification, any non-documentary methods and results of measures undertaken for verification and the resolution of substantive discrepancies discovered in identifying and verifying the identification information for five years after the record is made. [Questions 9 & 10, 2018 FAQs]

9.1.5.4.3 Specific Account Requirements

Existing customers: For existing customers subject to CIP, CIM Securities may rely on information obtained through the CIP to fulfill CDD requirements, providing that a representative of the customer certifies or confirms (orally or in writing) the accuracy of pre-existing CIP information. This also applies to the opening of multiple accounts, simultaneously or not. Oral confirmation must be documented in account records, and written confirmation will be retained with account information. [Questions 7 & 13, 2018 FAQs]

Foreign customers: Companies traded on foreign exchanges are subject to CDD requirements (while companies traded on U.S. exchanges are exempt). A "risk-based" approach may NOT be taken for these foreign customers, but CIM Securities may rely on their public disclosures as are available for other legal entity customers (whether listed or not). A foreign financial institution (FFI) is excluded from the definition of a legal entity customer if its foreign regulator collects and maintains beneficial ownership information about the FFI. CIM Securities may rely on representations of the FFI as to whether the exclusion applies. Lacking reasonable reliance on the FFI's representation, CIM Securities will contact the foreign regulator to confirm retention of beneficial ownership information.

Internal recordkeeping and operational accounts: When CIM Securities opens an account or subaccount (e.g., to accommodate trading strategies) relating to an existing legal entity customer, the account is not considered a new account and is not subject to CDD beneficial ownership requirements. [Question 11, 2018 FAQs]

Trusts as beneficial owners: If a trust owns 25% or more of the equity interests of a legal entity customer, the beneficial owner is the trustee, regardless of whether the trustee is a natural person or a legal entity. If there are multiple co-trustees of a trust that is a 25% or greater owner of equity interests of a legal entity customer, CIM Securities is not required to identify and verify the identity of all co-trustees. It must collect and verify the identity of, at minimum, one co-trustee of such a multi-trustee trust. [Questions 19 & 20, 2018 FAQs]

Pooled investment vehicles (PIV): For a PIV whose operators or advisers are not excluded from the definition of a legal entity customer, CIM Securities is not required to look through the PIV to identify and verify individuals who own 25% or more of its equity interests. However, CIM Securities is required to collect beneficial ownership information. [Question 18, 2018 FAQs]

Lower-risk customers: For certain lower-risk customers, the nature and purpose of the relationship can be developed by inherent or self-evident information.

9.1.5.4.4 Anti-Money Laundering Requirements

Beneficial owners are subject to AML requirements. Also see the chapter *ANTI-MONEY LAUNDERING (AML) PROGRAM and AML Manual*.

9.1.5.4.5 Currency Transaction Reporting (CTR) Requirements

CDD requirements do not change existing CTR requirements. CIM Securities will presume different businesses that share a common owner are operated separately and independently from each other and from the common owner. Transactions across commonly owned legal entity customers will not be aggregated absent indications the businesses are not operating independently (*i.e.*, same staff or location, accounts of one business are repeatedly used to pay the expenses of another business). Beneficial owners of a trust or estate account are not required when completing a CTR. Beneficial owner listing is only required if CIM Securities knows that the transaction(s) requiring filing is made on behalf of a beneficial owner and results in either cash in or cash out totaling more than \$10,000 during any one business day. [Questions 32 & 33, 2018 FAQs]

9.1.5.4.6 OFAC

Beneficial owners are subject to OFAC reviews outlined in the AML chapter.

9.1.5.5 Enhanced Due Diligence (EDD)

Some types of accounts, because of the potential risk for hiding the identity of underlying beneficial owners or money laundering activities, are subject to enhanced due diligence. The AML Compliance Officer will determine which accounts are subject to EDD and what reviews are necessary. Procedures for correspondent and private banking accounts are included in a separate section of this AML program. Certain trusts, corporate entities, shell entities, and private investment companies are examples of customers that may pose heightened risk.

EDD may include steps, in accordance with the level of risk presented, to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner. EDD information may be used for monitoring purposes and to determine whether there are discrepancies between information obtained regarding the account's intended purpose and expected account activity and the actual sources of funds and uses of the account.

9.1.5.6 Third Party Accounts

Customer ID required for third party accounts includes the following:

On behalf of an incompetent person: Obtain customer ID of the person holding power of attorney.

With power of attorney or trading authorization held by a third party: Obtain customer ID of the owner of the account. Customer ID is not necessary for the individual with authority over the account unless that person is unfamiliar to the RR or the circumstances regarding the opening of the account raises questions (customer requires wiring funds to an offshore address; third party is a foreign citizen; *etc.*).

9.1.5.6.1 Reliance On Other Financial Institutions

[C.F.R. 1023.220(a)(6)]

CIM Securities may rely for CIP purposes on another financial institution (including an affiliate) that opens a customer account provided that:

- reliance is reasonable under the circumstances;
- the other financial institution is subject to anti-money laundering requirements [U.S.C. 5318(h)] and is regulated by a Federal regulator; and
- the other financial institution enters into a contract requiring it to annually certify that it has implemented its AML program and it will perform (or its agent) specified requirements of CIM Securities's CIP.

9.1.5.6.2 Intermediated Account Relationships

[Various guidance from the U.S. Treasury and SEC regarding mutual fund CIP rule, BD CIP rule, FAQs regarding FCMs and introducing brokers, and foreign accounts]

If an intermediary is the customer and CIM Securities has no CIP obligation regarding the intermediary's underlying customers under existing guidance, CIM Securities will treat the intermediary as its legal entity customer. For example, the intermediary may be treated as the customer for transactions through omnibus accounts if:

- the omnibus account was established to execute transactions for settlement at another institution or the intermediary provides limited customer information to CIM Securities;
- the limited information provided is used primarily for recordkeeping purposes or to establish sub-accounts that hold positions for limited durations;
- all transactions in the omnibus account are initiated by the intermediary; and
- the beneficial ownership has no direct control over the omnibus account.

9.1.5.7 Accounts For Non-Individuals

Account documents usually obtained for non-individual accounts (trust instruments, articles of incorporation, partnership agreements, government-issued business license, *etc.*) will usually satisfy customer ID requirements. In the case of corporations, a certified copy of the articles of incorporation is required. These documents must be obtained within 5 days of account opening to satisfy the requirement. The authorizing documents must indicate who has the authority to act on behalf of the account.

9.1.5.8 Non-Documentary Methods Of Verifying Customer Identification

Non-documentary methods of verifying customer ID involve other procedures. Non-documentary methods must be used in the following circumstances:

- An individual is unable to present acceptable photo ID
- The documents presented are unfamiliar
- The account is opened without obtaining documents
- The customer opens the account without appearing in person at CIM Securities
- Other circumstances, at the discretion of the RR's supervisor, New Accounts, and/or the AML Compliance Officer, where CIM Securities is unable to verify the customer's identity

In these circumstances, a non-documentary method must be indicated by the RR on the new account application:

- Direct customer contact information

9.1.5.9 Additional Verification For Certain Customers

For the following types of customers, a minimum of TWO forms of customer ID are required in addition to review and approval by the AML Compliance Officer **prior to** opening the account:

- Accounts domiciled in high-risk countries included on the Treasury Dept. OFAC list (check with Operations personnel for a list of those countries or go to <http://www.treas.gov/offices/enforcement/lists/>)

9.1.5.10 Lack Of Customer ID Verification

When CIM Securities cannot form a reasonable belief that it knows the true identity of a customer, CIM Securities will:

- not open an account
- impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity
- close an account after attempts to verify customer's identity fail

For **customers who fail to provide required ID or documents within 5 days of account opening**, the account will be restricted to liquidating transactions only until satisfactory ID verification is received.

For **accounts where non-documentary verification results in substantive, unresolved discrepancies** (information that is inconsistent such as name, address, taxpayer ID number, *etc.*), either the account will not be opened or will be immediately closed.

Where inability to verify raises questions about the customer, filing a Suspicious Activity Report will be considered (see the section *Suspicious Activity Reports*).

Questions regarding accounts that do not comply with requirements to verify customer ID should be referred to the AML Compliance Officer.

9.1.5.11 Customer Notice

Customers are provided notice, prior to opening an account, that their identification will be verified. This notice may be on CIM Securities's web site, on new account applications, or in other disclosures provided at the time of account opening.

9.1.6 SIPC Disclosure

[FINRA Rule 2266]

When new accounts are opened, new customers will be provided information about the Securities Investor Protection Corporation (SIPC) including SIPC's web site address and phone number. This information is also provided annually in writing to all customers.

9.1.7 Approval

Note: Firm currently uses a Client Suitability Form which contains required information under FINRA Rule 4512.

[Exchange Act Rule 17a-3(17)(i)(A); FINRA Rule 4512]

Responsibility	<ul style="list-style-type: none">• IB Supervisor
Resources	<ul style="list-style-type: none">• New Account Form
Frequency	<ul style="list-style-type: none">• Daily
Action	<ul style="list-style-type: none">• Review new account form for:<ul style="list-style-type: none">○ Completeness○ Proper styling of account○ Unacceptable accounts (accounts in name of minor only, fictitious accounts, numbered accounts without disclosure of owner, <i>etc.</i>)○ Potential improper addresses (post office boxes, addressed to RR or CIM Securities, <i>etc.</i>)○ Consistency of investment objectives with financial status, prior investment experience, <i>etc.</i>○ Initial transaction consistent with investment objectives○ RR registration in state of customer's residency
Record	<ul style="list-style-type: none">• Supervisor's signature on New Account Form• New account forms are retained by Operations

A completed new account form or similar document, signed by the RR, is required for each new account opened. The designated supervisor is responsible for reviewing the new account form for the necessary information and will promptly approve each new account.

9.1.8 Customer Account Information

[SEC Securities Exchange Act of 1934 Rule 17a-3(17)(i)(A)]

Within 30 days of opening an account (or with the next scheduled account statement), the clearing firm will send the customer a copy of new account information for verification. In addition, account information will be verified with the customer every three years. In the event there is a change to the customer's account (including changes in investment objectives), the changed account information will be sent to the customer for verification within 30 days of submission of the change.

Compliance will review customer responses that revise new account information and will notify the RR, the RR's supervisor, and New Accounts of the changes.

9.1.9 Addresses On Customer Accounts

[SEC Securities Exchange Act of 1934 Rule 17a-3(a)(17)(i)(B)(2)]

If applicable, confirmations and statements and other account information will be transmitted to the customer at the address requested by the customer. CIM Securities or an employee may not be the sole addressee for a customer's account unless the account is for the direct benefit of CIM Securities or employee.

Acceptable addresses include:

- **for an individual:** residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
- **for a non-individual (corporation, trust, etc.):** a principal place of business, local office, or other physical location.
- **for a P.O. Box address:** a legal address for the customer must also be provided.

Accounts **may not** be addressed to CIM Securities, an RR or other employee of CIM Securities with the exception of accounts for the beneficial ownership of the RR or employee. Accounts **may not** be addressed care/of (c/o) someone else unless the customer provides written authorization requesting such an address.

Address changes require written instructions from the customer. Upon notification of a change of address, a notice will be sent to the customer's old address confirming that an address change has been made to the account. Compliance will follow up regarding questions about address changes.

Where the account is opened by a fiduciary such as an investment adviser on behalf of the fiduciary's customer, CIM Securities will provide either confirmations or periodic account statements to the underlying beneficial account holder. CIM Securities will make a good faith effort to obtain the information necessary to send confirmations directly to the beneficial owner; however, if this information is not provided by the fiduciary, CIM Securities will forward confirmations to the owner's custodian or, if there is no custodian or CIM Securities is the custodian, CIM Securities will send the confirmation directly to the fiduciary.

9.1.10 Account Documents

Additional account documents may be required depending on the type of account opened. The designated supervisor is responsible for establishing procedures outlining the necessary account documents and follow-up regarding missing documents.

9.1.11 Predispute Arbitration Agreements With Customers

[FINRA Rule 2268; FINRA Notice to Members 05-32 and 05-09]

Customers may be provided with copies of any signed agreements that include a predispute arbitration agreement within 30 days of signing; the customer will acknowledge receipt of the arbitration agreement on the agreement itself or on a separate document. The pre-dispute arbitration agreement, if utilized, will conform to FINRA Rule 2268.

9.1.12 Revisions To Customer Agreements

Firm policy does not permit revisions to pre-printed language on customer agreements. Requests for changes should be referred to Compliance for review.

9.1.13 Accounts Requiring Notification To Customer's Employer

[FINRA Rule 3210]

Responsibility	<ul style="list-style-type: none">• IB Supervisor/CCO
Resources	<ul style="list-style-type: none">• New Account Form
Frequency	<ul style="list-style-type: none">• Daily
Action	<ul style="list-style-type: none">• Code account for duplicate confirmations and/or statements as requested by other broker-dealers• For accounts of employees of FINRA code the accounts for duplicate confirmation and statements to FINRA
Record	<ul style="list-style-type: none">• Record of duplicate confirmations and statements is included with new account records

9.1.13.1 Employees Of Other Broker-Dealers

When opening an account for a person employed by another broker-dealer (including accounts where the employee has control or a personal financial interest), the other broker-dealer must be notified. CIM Securities will provide duplicate confirmations, statements, or other information requested by the employing broker-dealer.

9.1.13.2 Transactions Involving FINRA Employees

[FINRA Rule 2070]

When CIM Securities has notice that a FINRA employee has a financial interest in, or controls trading in, an account, CIM Securities will obtain and implement instructions from the employee to provide duplicate account statements to FINRA.

CIM Securities or its employees are prohibited from making a loan of money or securities to any FINRA employee other than disclosed, routine banking and brokerage agreements (or loans originating from a personal or family relationship).

CIM Securities or its employees cannot directly or indirectly give anything (other than something of nominal value such as a logo hat, pen, *etc.*) to a FINRA employee who has responsibility for a regulatory matter involving CIM Securities. "Regulatory matter" includes examinations, disciplinary proceedings, membership applications and dispute-resolution proceedings.

9.1.14 Post Office Addresses

If the customer opens an account using a post office address, the street address must also be provided on the new account form. The only exception is for customers who reside in rural areas where the post office address is the only address, which should be noted on the new account form.

9.1.15 Unacceptable Accounts

The following are examples of accounts that are unacceptable. Questions regarding whether new accounts may be opened should be referred to Compliance.

Unacceptable accounts include:

- Fictitious accounts in a name other than the name of the legal owner
- Accounts in the name of a minor
- Margin accounts for minors

9.2 Transferring Accounts

[FINRA Rule 2140 and 11870]

9.2.1 Accounts Transferring In – Not applicable at Present

When new accounts are transferred from another broker-dealer, a transfer form must be completed by the customer authorizing the transfer and provided to the receiving firm. Most accounts transfer via ACATS which expedites validation and transfer from the other BD.

Orders to sell securities to be transferred from the other firm may not be entered until validation is received. RRs should contact Operations to confirm whether the transfer has been validated.

9.2.2 Accounts Transferring Out – Not applicable at Present

When validated instruction has been received to transfer a customer's securities account assets to another firm, the account will be "frozen," *i.e.*, all open orders (with the exception of option positions that expire within 7 business days) must be canceled and no new orders taken.

CIM Securities and its employees may not interfere with a customer's request to transfer his or her account unless there is a *bona fide* reason for doing so, such as a lien for money owed.

9.3 Accounts And Securities Subject To Blocking

[Various Treasury Department regulations]

CIM Securities is prohibited from doing business in specific countries or with organizations or individuals the subject of Government sanctions. The U. S. Treasury Department's Office of Foreign Assets Control (OFAC) is responsible for administering and enforcing economic and trade sanctions. Sanctions target foreign countries,

terrorism sponsoring organizations, narcotics traffickers, money launderers, and other entities and individuals. Sanctions include the freezing of assets and blocking securities issued by embargoed foreign issuers.

As part of its anti-money laundering program, CIM Securities monitors accounts and securities included on OFAC's lists, available at OFAC's web site at www.treas.gov/ofac. OFAC information is updated whenever the Government issues new sanctions that result in blocking requirements.

Blocking will occur under the following circumstances:

- An account is opened for someone included on an OFAC list.
- The owner of an existing account is added to an OFAC list.
- A security is identified in a customer account where the issuer is the subject of blocking requirements.
- A request is made by a customer to pay or transfer funds or securities to a blocked person or entity.

RRs will be notified if one of their customer accounts; a security held in one of their accounts; or a requested transfer of funds or securities is blocked. In addition to the above, open orders will be cancelled for any account that is blocked.

Compliance with blocking requirements is very important. Violations can result in substantial fines against CIM Securities or persons engaging in prohibited transactions. Questions regarding blocked accounts, transfers, or securities should be referred to Compliance.

9.4 Updating Account Information And Periodic Affirmation

[SEC Securities Exchange Act of 1934 Rule 17a-3(a)(17)]

RRs should promptly update customer new account information whenever they are informed or become aware of changes. Updates may be recorded by making revisions to existing forms or completing new forms. New forms require the approval of the designated supervisor and signature of the customer, where required.

Within 30 days of changes to a customer's investment objectives, CIM Securities (or its clearing firm, if applicable) will send a copy of new account information, including the change, to the customer with a request for correction of any inaccurate information.

If applicable, at least every 36 months customers will be provided with new account information on record for their accounts and will be asked to advise of any changes or updates. Responses will be forwarded to Compliance. This notification is not required for accounts that have been inactive for 36 months or where no recommendations are made to the customer.

9.5 Sweep And Cash Management Account (CMA) Programs

[SEC Securities Exchange Act of 1934 Rule 15c3-3(j)(2)(ii); SEC FAQs regarding financial responsibility rules: <http://www.sec.gov/divisions/marketreg/amendments-to-broker-dealer-financial-responsibility-rule-faq.htm>; FINRA Rule 3260]

NOT APPLICABLE AT PRESENT

Free credit balances held in a customer's securities account may be transferred to a product in CIM Securities's sweep program or a customer's interest may be transferred between sweep programs. Four conditions regarding customer disclosures apply:

1. The customer must give **prior** written affirmative consent to having free credit balances included in the sweep program after being notified of (a) the general terms and conditions of the Program; and (b) that CIM Securities may change the products available under the Program.

2. Disclosures and notices required by SROs will be provided to customers.
3. Quarterly notice is included with statements that swept funds or money market shares can be liquidated and remitted to the customer.
4. 30-day prior written notice of any changes to the sweep program and sweep products will be provided.

CIM Securities and its RRs may not:

- Imply that a brokerage account is similar to or the same as a "checking or savings account" at a bank
- Imply that brokerage accounts themselves are bank deposit accounts insured by the FDIC

9.6 Margin Accounts – Not applicable at Present

[FINRA Rule 4210; Federal Reserve Regulation T]

This section outlines requirements for margin accounts **which ARE NOT** applicable at the present time.

9.6.1 Opening Margin Accounts

Prior to engaging in margin transactions, the customer's account must have on deposit at least \$2,000 in cash or securities. Customers must sign CIM Securities's margin agreement which must be received within five days from the first margin trade.

9.6.2 Employee Accounts

Extensions and prepayments are not permitted in employee accounts, except under extraordinary circumstances and with approval of the designated supervisor.

9.6.3 Disclosures

9.6.3.1 Margin Disclosure Statement

[FINRA Rule 2264]

Under FINRA rules, all non-institutional customers who open a margin account must be provided with a margin disclosure statement when the account is opened. CIM Securities's disclosure statement must be included when the margin agreement is sent to the customer for signing. In addition, all margin customers will be provided annually with a copy of the disclosure statement or an abbreviated version of the statement. RRs are responsible for providing the initial disclosure statement; CIM Securities (or its clearing firm, if applicable) will send annual disclosures. The margin disclosure statement also appears on CIM Securities's web site.

Under this requirement, the term "**non-institutional customer**" includes all customers **except**:

- A bank, savings and loan association, insurance company, or registered investment company.
- An investment adviser registered either with the SEC or with a state securities commission
- Any other entity (whether a natural person, corporation, partnership, trust, or otherwise) with total assets of at least \$50 million

The Clearing Firm is responsible for providing the initial disclosure document to new non-institutional margin account customers.

The RR is responsible for providing the annual disclosure document.

9.6.3.2 Disclosure Of Credit Terms

[SEC Securities Exchange Act of 1934 Rule 10b-16]

Upon opening a margin account, the customer will be provided a written statement explaining the operation of a margin account and the calculation of interest charges on debit balances. It is the FINOP's responsibility to establish procedures for providing the required disclosure.

The Compliance is responsible for providing credit disclosures to margin customers.

9.6.3.3 Securities Loan Transactions

[FINRA Rule 4330(a), 4330(b)(2), 4330.04 and 4330.05]

CIM Securities (or its clearing firm) may engage in borrowing and lending customers' fully paid or excess margin securities. The customer's agreement is included in CIM Securities's margin agreement and disclosures will be provided as described in the next section.

There must be reasonable grounds for believing that the customer's loan(s) of securities are appropriate for the customer, including consideration of (but not limited to) the customer's financial situation and needs, tax status, investment objectives, investment time horizon, liquidity needs, risk tolerance, and any other information disclosed by the customer in connection with entering into securities loans. Determining the appropriateness of customer loans of securities is not required for institutional customers under Rules 4512(c) and 2111(b).

9.6.3.4 Other Disclosures

[FINRA Rule 4330(b)(2)(B)]

Prior to entering into a securities borrowing arrangement with a customer, the customer will be provided with written (which may include electronic) notice stating that the provisions of the Securities Investor Protection Act of 1970 may not protect the customer with respect to the customer's securities loan transaction and that the collateral delivered to the customer may constitute the only source of satisfaction of CIM Securities's obligation in the event CIM Securities fails to return the borrowed securities. Other required disclosures (such as loss of proxy voting rights on margined shares and risk of receiving payments-in-lieu of dividends) will be provided in customer margin agreements, by separate notice, in customer monthly statements, and/or on CIM Securities's web site.

9.6.4 Equal Credit Opportunity Act Requirements

CIM Securities will not discriminate in the extension of credit to customers. Where credit is denied, CIM Securities will provide information to the credit applicant in accordance with the provisions of the Equal Credit Opportunity Act.

9.6.5 Arranging Credit

RRs are not permitted to assist a customer in making credit arrangements to purchase securities outside CIM Securities, other than on terms consistent with those permitted by Regulation T and other rule requirements.

9.6.6 Suitability/Regulation BI

Margin accounts may involve more risk than cash accounts, depending on a number of factors including leverage used and types of transactions. The RR is responsible for determining the suitability/compliance with Reg BI (for retail customers) of margin trading in a customer's account including understanding the customer's investment objectives and financial profile.

9.6.7 Margin Requirements

Initial and maintenance requirements are available by contacting Operations.

9.6.8 New Issues

Margin on new issues are not permitted for a period of 30 days from the effective date of the distribution.

9.6.9 Credit On Restricted Securities

Extension of credit or margin transactions in securities for corporate insiders require the prior approval of Operations. If a customer who holds restricted securities wishes to deposit those securities in a margin account, Operations should be notified to determine the marginability of the securities.

9.6.10 Fiduciary Accounts

Margin transactions are permitted for accounts controlled by an administrator, conservator, custodian (not including UTMA/UGMA accounts), executor, guardian or trustee as follows:

- when such person holds explicit power to engage in margin transactions
- after review of the appointment and applicable document (trust agreement, trust certification, will, *etc.*) explaining investment powers and approval by Compliance

RRs should submit the appropriate enabling document (trust agreement, *etc.*) to Compliance prior to engaging in margin transactions.

9.6.11 Portfolio Margin Accounts

[FINRA Rule 4210(g); FINRA Notice 08-41, 07-14 and 07-11]

Customers with portfolio margin accounts must be provided with a special written disclosure describing the nature of, and risks associated with, portfolio margining. Customers must sign and acknowledge that they have read and understand the disclosure statement and agree to the terms of maintaining a portfolio margin account. RRs are responsible for providing the disclosure and obtaining signed acknowledgment which will be retained in the customer's account file.

Portfolio margining is a margin methodology that sets margin requirements for an account based on the greatest projected net loss of all positions in a product class or group using computer modeling to perform risk analysis using multiple pricing scenarios. It is applicable to all margin equity securities, listed options, security futures products, unlisted derivatives, warrants, index warrants and related instruments.

There are eligibility requirements for customers (other than broker-dealers):

- Meet basic standards for having an account approved for uncovered writing
- Have and maintain at all times account net equity of at least \$5 million (waived for accounts solely limited to listed security futures contracts and listed single stock options) aggregated across all accounts under identical ownership at the clearing broker

Portfolio margining generally permits greater leverage resulting in greater risk for loss. The time limit for meeting margin calls is shorter than for a standard margin account. Operations procedures should be consulted for more detailed information regarding portfolio margining requirements.

9.7 Third Party Accounts

When a third party who is not the principal or named person on the account will give instructions regarding orders, disposition of funds, or other actions involving an account, CIM Securities must have a signed third-party trading authorization. The authorization is signed by the principal of the account and the third party, giving the third party authority to act on behalf of the principal. An example of a third party account is an account for a wife whose husband will give instructions regarding his wife's account. The signed trading authorization must be received BEFORE accepting instructions from the third party.

CIM Securities has two types of trading authorizations:

- Limited trading authorizations limit the third party to giving instructions regarding the purchase and sale of securities and does NOT give authority regarding the disposition of funds or securities.
- Full trading authorizations give the third party authority to give instructions regarding purchases and sales as well as the disposition of funds or securities in the account.

9.8 Discretion For Orders And Accounts

[SEC no-action letters regarding cash management accounts (<http://sec.gov/divisions/investment/noaction/ubs092905.htm>) and family/related accounts (<http://sec.gov/divisions/investment/noaction/morganlewis111705.htm>)]

CIM Securities does **not** permit discretionary accounts where the customer signs a discretionary trading authorization and permits the RR to make decisions for the account without consulting with the customer first.

This prohibition does not include temporary or limited discretion in the following examples:

- Price and time discretion for an order.

- Isolated or infrequent discretion, such as when a customer is unavailable for a limited period of time. The customer must sign a trading authorization in advance, an expiration date must be noted on the agreement, and the limited discretion must be approved by the RR's supervisor.
- Exchanging one money market fund for another or its cash equivalent.
- Transactions to satisfy margin requirements.
- Selling bonds and buying similar bonds permitting the customer to take a tax loss on the original purchase.
- Buying a bond with a specified credit rating and maturity.
- Buying or selling a security or type of security within limited specific parameters established by the customer (requires the customer's instructions in writing).
- The RR acts as conservator, trustee, attorney-in-fact, or other agent as a result of a family or personal relationship with the account.

9.9 Accounts For Minors – If applicable

[Uniform Gifts To Minors Act; Uniform Transfers To Minors Act; FINRA Regulatory Notice 20-07]

UTMA/UGMA accounts are custodial accounts that allow for the transfer of funds, securities and other assets to minors without the need for a formal trust. UGMA and UTMA are model laws developed and approved by the Uniform Law Commission for application by states.

There are a number of requirements and restrictions that affect minors' accounts:

- The donor names a custodian and donates assets to the account
- Only one custodian is permitted for each account
- Custodians generally may not delegate authority to another person
- Only one minor may be named in each account
- Margin transactions are not permitted
- Gifts to minors are irrevocable, *i.e.*, the custodian may not direct distribution of assets from the account except for the benefit of the minor
- The minor's social security number must be used when opening the account
- Minors may not be a party to a joint account, investment club, or partnership
- The custodianship generally terminates when the beneficiary reaches the age of majority (or other alternative age in state statutes or if the beneficiary dies)
- Some states permit extending custodianship to a higher age; the beneficiary should be notified of his or her right to compel distribution of assets upon reaching a specified age
- CIM Securities and the RR should be aware when a custodianship is terminated and assets are to be distributed which may include flagging custodianship accounts to identify termination and notifying RRs to verify the custodian's continuing authority and to obtain instructions about distribution of the assets

The custodian manages the account assets including executing transactions and withdrawing or transferring funds for the benefit of the beneficiary (the minor).

9.10 Coverdell Education Savings Accounts – If applicable

[26 USC §530 - Coverdell Education Savings Accounts]

A Coverdell Education Savings Account (ESA) is an account created as an incentive to help parents and students save for education expenses. An alternative is the 529 College Savings Plan which is included in the *MUNICIPAL SECURITIES* chapter in the section *529 College Savings Plans (Municipal Fund Securities)*. For more information, refer to the IRS site above; plan sponsors; and the customer's tax adviser.

The following summarizes some of the key features of Coverdell accounts.

- The maximum annual contribution is \$2,000 subject to limits on the donor's modified adjusted gross income.
- Contributions are made from after-tax dollars; there is no tax deduction for contributions.
- ESAs are available for beneficiaries (students) who are under the age of 18 when the account is established. There are exceptions for beneficiaries with special needs.
- The funds are controlled by the account owner (e.g., the parent) at all times.
- Investment choices are broad but may not include life insurance contracts.
- Assets may be used for elementary- and secondary-school tuition as well as for higher education.

The following compares some features of Coverdell and 529 plans.

Feature	Coverdell Account	529 Plan
Contribution limits	\$2000 annual	No restrictions up to maximum lifetime contribution
Allowable investments	Allows almost all types of investments including stocks, bonds, and mutual funds (parallels rules for IRAs)	Limited to state-run allocation programs
Distribution of assets	Must be disbursed on qualified education expenses by the beneficiary's 30th birthday or given to another family member below the age of 30	No age limit
	Federal tax-free if used for qualified education expenses; some states offer tax benefits	Same
	Income tax and penalties may apply for ineligible distributions	Same
Qualified education	Elementary and secondary schools; higher education	Does not allow elementary and secondary education expenses
Income limits affecting contributions	Limits on modified adjusted gross income at certain levels	No limits
Ownership of assets	Owned by person establishing the account, not the child	Same
Designation of new beneficiary	Must be eligible family member of the previous beneficiary to avoid taxes or penalties	Same

9.11 Accounts For Senior Investors

[SEC/NASAA 2008 report on Protecting Senior Investors: <http://www.sec.gov/spotlight/seniors/seniorspracticesreport092208.pdf>; 2010 addendum to 2008 report: <http://www.sec.gov/spotlight/seniors/seniorspracticesreport081210.pdf>; SEC web site Senior Investors: <http://www.sec.gov/divisions/marketreg/seniorinvestors.htm>; FINRA Rule 2165 and 4512; FINRA Regulatory Notice 22-05, 17-11, 11-52 and 07-43; FINRA FAQs re financial exploitation of seniors: <http://www.finra.org/industry/frequently-asked-questions-regarding-finra-rules-relating-financial-exploitation-seniors>; Senior Safe Act: Sec. 303 of Economic Growth, Regulatory Relief and Consumer Protection Act; NASAA/SEC/FINRA Senior Safe Act Fact Sheet: <http://www.nasaa.org/wp-content/uploads/2019/05/Senior-Safe-Act-Fact-Sheet.pdf>; Report on FINRA's Examination and Risk Monitoring Program: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • New account records • Order records/available reports • Indications of financial exploitation • Requests for temporary holds • Advertising targeting senior investors • Seminar materials
Frequency	<ul style="list-style-type: none"> • Training - as scheduled • Ongoing - other actions
Action	<ul style="list-style-type: none"> • Conduct training on dealing with senior investors including elements of this section such as holds for financial exploitation • Provide written disclosure to customers to explain the circumstances under which CIM Securities may contact a Trusted Contact Person • When reviewing investments for seniors, take into particular consideration the factors included in the subsection <i>Recommendations To Senior Investors</i> • Review product-specific guidelines when reviewing for suitability of investments • Refer to new account information when necessary to identify investment objectives and other customer information • Review account activity when appropriate • For escalated issues: <ul style="list-style-type: none"> ○ Contact the Trusted Contact Person ○ Consider direct contact with the investor ○ Notify state or other authorities (after conferring with Compliance) regarding potential elder abuse • Confer with RR regarding suitability questions • Confer with Compliance when necessary • Contact customer when necessary to confirm customer's understanding of and agreement with transactions • Modify or restrict future transactions, as appropriate
Record	<ul style="list-style-type: none"> • Order records/reports • Record of escalation of an issue including who reviewed the issue and what action, if any, is taken • Temporary holds (see following section)

9.11.1 General Requirements

When opening and handling accounts for specified adults (definition below), there are certain considerations in addition to usual account handling procedures. For purposes of this section, the following definitions apply.

Specified Adult: (A) a natural person age 65 and older; or (B) a natural person age 18 and older who the member reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests.

Account: any account of a member for which a Specified Adult has the authority to transact business.

Trusted Contact Person: the person who may be contacted about the Specified Adult's Account in accordance with Rule 4512.

Financial exploitation:

- A. the wrongful or unauthorized taking, withholding, appropriation, or use of a Specified Adult's funds or securities; or
- B. any act or omission by a person, including through the use of a power of attorney, guardianship, or any other authority regarding a Specified Adult, to:
 - i. obtain control, through deception, intimidation or undue influence, over the Specified Adult's money, assets or property; or
 - ii. convert the Specified Adult's money, assets or property.

In this section "financial exploitation" is understood to include where there is reasonable belief that financial exploitation has occurred, is occurring, has been attempted, or will be attempted.

9.11.2 Opening Accounts For Specified Adults

When opening accounts, the following should be considered:

- Encourage customers to identify a Trusted Contact Person and obtain permission to contact that person in the event there is an issue or event that requires clarification (such as the customer suffers diminished mental capacity in the future); document account information if the customer refuses to identify a contact person. The customer will be notified in writing (including electronically) that CIM Securities or an associated person is authorized to contact the Trusted Contact Person to disclose information about the customer's account and possible financial exploitation.
- Indicate "retired" or similar on the new account record.
- Obtain "lifestyle" information such as when the investor plans to retire, if not already retired; how much money will be needed after retirement; whether there are prospects for future employment; whether a dependent is supported by the investor; other expenses including healthcare expenses anticipated by the investor; the existence of a will and financial power of attorney

Accounts must NOT be opened for a Specified Adult if there is evidence of financial exploitation or diminished capacity; orders should not be accepted under such circumstances, either.

9.11.3 Recommendations To Senior Investors

[FINRA Regulatory Notice 07-43]

Suitability considerations are a concern for all types of accounts. While suitability requirements do not specifically refer to age or life stage, these factors should be considered when making recommendations to older investors. Considerations when dealing with senior investors include:

- Current and future prospects for employment
- Primary expenses including whether the customer still has a mortgage
- Sources of income and whether it is fixed or will be in the future
- Income needed to meet fixed or anticipated expenses
- Savings for retirement and how they are invested
- Liquidity needs
- Financial and investment goals (income needs, preservation of capital, accumulation of assets for heirs)
- Health care insurance and future needs to fund health costs

9.11.4 Diminished Mental Capacity

A difficult issue is a customer who appears to be suffering from diminished mental capacity. If a customer's behavior suggests reduced capacity, it is important to take steps to protect the customer, the RR, and CIM Securities. Relatives or estate beneficiaries may file a complaint or lawsuit if they believe the customer was unable to understand what was occurring in his or her account.

There are a number of steps that may be taken to address the issue:

- Contact the Trusted Contact Person
- Have a conversation with the customer with the branch manager or other supervisor present to assist in making a determination.
- Raise the issue with family members and determine if the customer has given power of attorney to another person.
- Document meetings, conversations, and other exchanges with relatives about the situation.
- Document communications with the customer about investments.
- As a final alternative, decide not to continue doing business with the customer.

Contact Compliance with questions about a proper course of action.

9.11.5 Potential Indication Of Elder Financial Exploitation

[FinCEN Advisory FIN-2011-A003: <https://www.fincen.gov/news/news-releases/memorandum-financial-institution-and-law-enforcement-efforts-combat-elder>]

This section includes an excerpt from a FinCEN advisory. This information provides guidance to RRs and other employees when handling accounts for elderly customers. Questions regarding potential elder abuse should be referred to your supervisor or Compliance.

The following red flags could indicate the existence of elder financial exploitation. This list of red flags identifies only possible signs of illicit activity. Financial institutions should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. In addition, financial institutions may become aware of such scams through their direct interactions with elderly customers who are being financially exploited. In many cases, branch personnel familiarity with specific victim customers may lead to identification of anomalous activity that could alert bank personnel to initiate a review of the customer activity.

- Erratic or unusual banking transactions, or changes in banking patterns:
 - Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
 - Sudden Non-Sufficient Fund activity;
 - Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
 - Debit transactions that are inconsistent for the elder;
 - Uncharacteristic attempts to wire large sums of money;
 - Closing of CDs or accounts without regard to penalties.
- Interactions with customers or caregivers:
 - A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
 - The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;

- The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;
- A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
- The customer moves away from existing relationships and toward new associations with other "friends" or strangers;
- The elderly individual's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;
- The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

9.11.6 Escalating Issues Involving Senior Investors

When dealing with senior investors, there may be changes or events that require escalation of an issue to the RR's designated supervisor and/or Compliance. Following are some issues that may require escalation for handling. Any questions regarding dealing with senior investors should be referred to Compliance.

- Suspected elder abuse including financial abuse (contacting appropriate state or other authorities may be necessary; confer with Compliance regarding such referrals)
- Suspected diminished capacity

Having the RR's designated supervisor or Compliance make direct contact with the investor or Trusted Contact Person may be appropriate.

9.11.7 Financial Exploitation - Temporary Holds

[FINRA Rule 2165; FINRA Regulatory Notice 17-11]

To protect certain customers, CIM Securities may place temporary holds on transactions and/or disbursements of funds or securities from the account of Specified Adults where there is reasonable belief that financial exploitation has occurred, is occurring, has been attempted, or will be attempted. Conditions of a temporary hold include the following:

- Temporary holds include the disbursement of funds or securities or transactions in securities.
- No later than two business days after the date the temporary hold is first placed provide notification oral or in writing (electronic included) to all parties authorized to transact business on the account unless a party is unavailable or it is believed the Trusted Contact Person(s) is involved in the financial exploitation.
- Immediately initiate an internal review of the facts and circumstances about the financial exploitation.
- The temporary hold expires 15 business days after the hold is first placed.
- Unless otherwise terminated or extended by a state regulator or agency or court of competent jurisdiction and if CIM Securities's internal review supports the finding of financial exploitation:
 - The temporary hold may be extended 10 business days
 - The temporary hold may be extended an additional 30 business days beyond the initial 25 days (the first 15-day hold plus the extension of 10 days) for a total potential hold of 55 business days

9.11.8 Reverse Mortgages- Not applicable at Present

[FINRA Investor Alert: Reverse Mortgages, Avoiding a Reversal of Fortune]

A reverse mortgage is an interest-bearing loan secured by the equity in a home. Generally the borrower and any other co-borrowers (such as a spouse) must own the home and be 62 or older (some lenders may have other criteria). Home equity may be converted to cash that can be used for any purpose. The homeowner makes no interest or principal payments during the life of the loan; interest is added to the principal. Unless the loan is a fixed-term loan, the loan only becomes due when the homeowner dies, sells the home, or otherwise leaves the home for more than 12 months. If any of these events occur, the borrower or heirs must repay the loan, including compounded interest, in full. Usually the home is sold and the loan is paid from proceeds of the sale.

RRs are not permitted to recommend customers use reverse mortgages to fund investments. If a customer indicates he or she has funds available for investment from the proceeds of a reverse mortgage, the following is required.

1. Provide the customer with a copy of the FINRA Investor Alert *Reverse Mortgages: Avoiding A Reversal of Fortune*. Obtain a letter from the customer acknowledging receipt of the Alert.
2. Consult with the customer about investment objectives and the need for the proceeds as living expenses.
3. Recommend investments consistent with those needs; most investments should be conservative and suitable for someone with a limited lifespan and potentially facing expenses for health issues.
4. Recommendations other than conservative investments must be approved by the designated supervisor **prior to** making the investments. Provide the supervisor with a copy of the new account information and a written explanation of funds available, the needs of the investor, and how they are to be invested.

9.11.9 Luncheon Programs And Seminars

[SEC/NASAA report on free lunch seminars: <http://www.sec.gov/spotlight/seniors/freelunchreport.pdf>]

Responsibility	<ul style="list-style-type: none">• IB Supervisor• Compliance
Resources	<ul style="list-style-type: none">• Public Speaking/Seminar/Luncheon Request• Materials to be provided to attendees• Proposed advertising of the event
Frequency	<ul style="list-style-type: none">• As required when the form is submitted
Action	<ul style="list-style-type: none">• The designated supervisor is responsible for:<ul style="list-style-type: none">○ reviewing the form and making changes, if needed, to the proposed event and related materials or advertising○ submitting the form and attached materials to Compliance for review○ attending or designating someone to attend meetings randomly at least once every two months to confirm compliance with CIM Securities requirements○ if non-compliance or questionable activities are identified, confer with the RR and Compliance regarding corrective action• Compliance reviews and revises the submitted materials and responds to the designated supervisor, approving or disapproving
Record	<ul style="list-style-type: none">• Designated supervisor retains:

	<ul style="list-style-type: none"> ○ copy of request form and related materials ○ record of randomly attending luncheons/seminars and corrective action taken, if necessary • Compliance retains: <ul style="list-style-type: none"> ○ the form and all related materials including notations of changes and approval or disapproval ○ record of corrective action taken when necessary
--	---

Luncheon programs and seminars are a common approach to reach investors and have become particularly popular in soliciting senior investors. These programs, as for all public speaking, require the approval of the designated supervisor including submission of the invitation, any related advertisement, an outline of subjects to be covered and copies of materials to be distributed or shown in presentations (slide shows, Powerpoint presentations, etc.). Advertising must be approved by Compliance.

Luncheon programs cannot infer that no products will be sold or mislead invitees as to the purpose of the luncheon. Products offered must be suitable for the target audience and the suitability of any recommendation must be considered for each investor individually.

- Attach materials to be provided to attendees as well as proposed advertising of the event to IB Supervisor and Compliance.

9.11.10 Advertising Targeting Seniors

Advertising that targets seniors must be balanced and may only include products or services suitable for senior investors. All advertising must be approved by Compliance prior to publication or distribution.

9.12 Incompetent Persons

Accounts for incompetent persons may only be opened with the appropriate authority from a court-appointed guardian. If an RR becomes aware that a customer has become incompetent, the RR should contact the branch manager or Compliance for further guidance.

If a customer becomes incompetent while a third party trading authorization is in effect for his or her account, the authority generally is considered invalid and requires a court order for reinstatement. "Durable" powers of attorney, recognized by some states, remain in effect after a person is declared incompetent. Questions should be referred to Compliance.

9.13 Trust Accounts

If applicable, new accounts for trusts require a copy of the trust agreement or a trust certification signed by the authorized trustee. The following activities in trust accounts require **prior** approval as follows:

- Margin trading requires approval by Compliance
- Option trading requires approval by Compliance
- Discretionary accounts require approval by Compliance (if CIM Securities permits discretionary accounts)

Fiduciaries (executors, trustees, guardians, administrators, conservators, *etc.*) may not be able to delegate their duties to a third party (whether the RR or an outside person) to manage the account unless the trust or other authorizing instrument specifically permits delegation. Some states require the fiduciary to obtain a court order to delegate authority to a third party.

9.14 Registered Persons (RRs) Being A Customer's Beneficiary Or Holding A Position Of Trust

[FINRA Rule 3241; FINRA Regulatory Notice 20-38; Report on FINRA's Examination and Risk Monitoring Program: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

RRs are limited from being named a beneficiary, executor or trustee, or having a power of attorney or similar position of trust for or on behalf of a customer^{*}. The RR is responsible for immediately notifying Compliance of any such potential designation. The notice requirement includes RRs who hold a beneficiary or position of trust status for an account transferring from a prior employer; the transferring RR must provide notice within 30 days of employment.

These limitations do **not** apply where the customer is a member of the registered person's "immediate family"^{**}. In addition, a registered person who does not have customer accounts assigned to him/her is not subject to these requirements.

Exceptions to this limitation must be requested, in writing, from Compliance. The request must include the name(s) of the customer's account(s) and in what role the registered person will act (beneficiary, executor, trustee, *etc.*) as well as the following:

- length and type of relationship between the customer and the registered person
- the customer's age
- the size of any bequest relative to the size of the customer's estate
- any remuneration to be paid to the RR
- any customer mental or physical impairment that renders the customer unable to protect his or her own interests

Registered persons may **not** accept such a role without **prior** approval from Compliance. In addition, a registered person may not instruct or ask a customer to name another person, such as the registered person's spouse or child, to be a beneficiary of the customer's estate or to receive a bequest from that estate.

In the event a registered person unknowingly becomes the subject of these limitations (*e.g.*, notification of receiving a bequest, being named an executor, *etc.*), the registered person is obligated to decline the role or bequest unless written notice is provided to Compliance and approval is received.

*"Customer" under this Rule includes any customer that has, or in the previous six months had, a securities account assigned to the registered person including a brokerage account, mutual fund account or variable insurance product account and accounts held directly at a mutual fund or variable insurance product issuer. It also includes someone who is a customer of another broker-dealer which subjects the activity to Rule 3241 on limitations explained in this section as well as Rule 3270 regarding outside business activities.

** For purposes of Rule 3241, "immediate family" includes parents, grandparents, in-laws, spouse or domestic partner, sibling, children, grandchildren, first cousin, aunt or uncle, niece or nephew, and any other person who resides in the same household as the registered person and the registered person financially supports, directly or indirectly, to a material extent, and including step and adoptive relationships.

9.15 Correspondent And Private Banking Accounts And Accounts For Senior Foreign Political Figures

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart F; USA PATRIOT Act Section 312 and 313]

Under anti-money laundering (AML) rules, there are special requirements that apply to "correspondent" and "private banking" accounts as well as to accounts for "senior foreign political figures." Definitions of these and other terms follow the summary of requirements. Questions should be referred to the AML Compliance Officer.

9.15.1 Summary Of Requirements

- Correspondent accounts require due diligence to determine ownership of the account.
- Accounts cannot be opened for foreign shell banks.
- When opening an account for a foreign bank, the Foreign Bank Certification form must be submitted to the AML Compliance Officer with the New Account Form for review and approval.
- Every three years foreign banks will be required to re-certify the information in the Foreign Bank Certification.
- When opening an account for a senior foreign political figure, the new account application must be submitted to the AML Compliance Officer for review and approval.

9.15.2 Definitions

Correspondent account: Includes any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign institution, or to handle other financial transactions related to such foreign financial institution. This type of account presumes a formal relationship through which the financial institution provides regular services. Due diligence requirements apply to correspondent accounts maintained for the following foreign financial institutions:

- Foreign bank
- Foreign branch of a U.S. bank
- Business organized under a foreign law that, if located in the U.S., would be a securities broker-dealer, futures commission merchant, introducing broker in commodities, or a mutual fund
- Money transmitter or currency exchanger organized under a foreign law

Private banking account: A private banking account is an account that is established or maintained for the benefit of one or more non-U.S. persons, requires minimum aggregate deposit of funds or other assets of not less than \$1,000,000, and is assigned to a bank employee who is a liaison between the financial institution and the non-U.S. person. If the account otherwise satisfies the definition but the institution does **not** require a minimum balance of \$1,000,000, the account does not qualify as a private banking account.

Senior foreign political figure includes:

- a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise (Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources.)
- immediate family members of the above, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure
- a corporation, business, or other entity formed by or for the benefit of one of the above individuals

Proceeds of foreign corruption: any asset acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and include any other property into which any such assets have been transformed or converted.

Foreign bank: a bank organized under foreign law, or an agency, branch, or bank office located outside the United States. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

Foreign shell bank: is defined as a foreign bank without a physical presence in any country.

Regulated affiliate: is a foreign shell bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or a foreign country, as applicable; and (2) is subject to supervision by a banking authority in the foreign country regulating such affiliated depository institution, credit union, or foreign bank.

9.15.3 Prohibition Against Correspondent Accounts For Foreign Shell Banks

CIM Securities is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank. The prohibition does not apply to a foreign shell bank that is a regulated affiliate. If an account is inadvertently opened for an unregulated foreign shell bank, the AML Compliance Officer should be notified and the account will be immediately closed.

9.15.4 Foreign Bank Certification

When opening an account for a foreign bank, CIM Securities is obligated to ensure the bank is not a foreign shell bank and must obtain information about the foreign bank's owners and an agent for service of process. The bank must complete the Foreign Bank Certification which must be submitted to the AML Compliance Officer with a copy of the New Account Form for review. Every three years the bank is also required to re-certify the information filed with CIM Securities.

9.15.5 Accounts For Foreign Political Figures

Accounts for foreign political figures (as defined above) are subject to special reviews to comply with Bank Secrecy Act requirements. RRs are required to identify, on the new account application, whether an account for a foreigner falls under the definition. The application must be submitted to the AML Compliance Officer for review and approval.

9.16 Wealth Events

Wealth events refer to those situations where an investor faces the decision about what to do with a large amount of money arising from an inheritance, life insurance payout, sale of a business or other major asset, divorce settlement or an IRA rollover, among other events. RRs must consider the following when advising a customer about investing such funds:

- Many wealth events have tax consequences. RRs are prohibited from providing tax advice; the customer should be advised to contact their tax adviser.

- Suitability requirements are important and must be considered by the RR prior to making any recommendation.
- RRs may not infer that the customer's only choice or sound option is rolling funds to an IRA managed by CIM Securities; also, IRAs cannot be represented as "free" or without cost or fees.

9.17 Pension And Retirement Accounts - Non-Fiduciary

[Employment Retirement Security Act (ERISA) of 1974; Department of Labor Rule 3.0; Prohibited Transaction Exemption 2020-02; PTE2020-02 FAQs: <https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/faqs/new-fiduciary-advice-exemption>]

This section explains the requirements for pension and retirement accounts. These accounts are regulated under the Employee Retirement Income Security Act of 1974 (ERISA), a federal law that sets minimum standards for most voluntarily established pension and health plans in private industry and provides protections for individuals in these plans. ERISA applies to all Internal Revenue Service-qualified pension and profit sharing plans and employee welfare benefit plans. Most IRA accounts, while not covered by ERISA, are subject to the prohibited transaction penalties. Limited exemptions apply to governmental (public employee) plans and certain offshore and church plans.

ERISA is administered by the Department of Labor (DOL) which issues rules, interpretations, and exemptions. Key elements of ERISA include:

- Who is a fiduciary subject to related requirements
- Exemptions from "prohibited transactions" which are considered self-dealing and not allowed in these accounts

This section begins with CIM Securities's policy on fiduciary status and follows with definitions and general information about retirement accounts. ERISA is complex because of its technical and legal nature; questions should be referred to Compliance or legal counsel.

9.17.1 Recommendations and Fiduciary Status Prohibited

Because of the complexity of laws and rules governing pension and retirement accounts and the legal liability when acting as a fiduciary, CIM Securities and its RRs are not permitted to provide services to pension and retirement accounts and IRAs (including rollovers) in a manner resulting in fiduciary status. This means:

- No recommendations may be made to these accounts including for IRA rollovers.
- All orders for these accounts must be marked "unsolicited."
- The prohibition extends to recommendations to prospects.

9.17.2 Fiduciary Status Defined – Replaced by Reg BI. Please refer to Reg BI section of this manual

In addition to the traditional fiduciary definition as included under definitions (discretionary authority and control), the DOL has outlined a "five-prong" test to identify who is a fiduciary. All five parts of the test must be satisfied to be a fiduciary making a recommendation. The person making the recommendation must:

1. Render advice to the plan, plan fiduciary, or IRA owner as to the value of securities or other property, or make recommendations as to the advisability of investing in, purchasing or selling securities or other property,
2. On a regular basis,

3. Pursuant to a mutual agreement, arrangement, or understanding with the plan, plan fiduciary, or IRA owner, that
4. The advice will serve as a primary basis for investment decisions with respect to plan or IRA assets, and that
5. The advice will be individualized based on the particular needs of the plan or IRA.

9.17.3 Disclosures To Plans

[ERISA Section 408(b)(2); Dept. of Labor Fact Sheet: <https://www.dol.gov/newsroom/releases/ebsa/ebsa20120507>]

Under ERISA, "covered service providers" are required to provide fee disclosures to covered plans to enable the plan fiduciary to make an informed decision about the reasonableness of fees as required under ERISA Section 404(a)(1). CIM Securities's obligation to provide disclosures depends on CIM Securities's role in dealing with a covered plan. This section provides a general explanation of the requirements which are complex; the ERISA section should be consulted for specific requirements.

9.17.3.1 Definitions

Covered plan: An ERISA-covered defined benefit and defined contribution pension plan. Does not include simplified employee pension plans (SEPs), SIMPLE retirement accounts, IRAs, employee welfare benefit plans, and certain annuity contracts and custodial accounts described in ERISA Code section 403(b).

Covered service provider: A service provider that enters into a contract or arrangement with the covered plan and expects \$1,000 or more in direct or indirect compensation that is received in connection with providing services defined in Section 408(b)(2) including:

- ERISA fiduciary service providers to a covered plan or to a "plan asset" vehicle in which such plan invests
- Investment advisers registered under Federal or State law
- Recordkeepers or brokers who make designated investment alternatives available to the covered plan (e.g., a "platform provider")
- Providers of one or more of the following services to the covered plan who also receive "indirect compensation" in connection with such services:
 - Accounting, auditing, actuarial, banking, consulting, custodial, insurance, investment advisory, legal, recordkeeping, securities brokerage, third party administration, or valuation services

9.17.3.2 Required Disclosures

Disclosures include:

- Disruption of services
- Compensation, including:
 - Description of all direct compensation either in aggregate or by service to be received
 - Indirect compensation expected to be received
 - Description that compensation will be paid among related parties including identification of payers and recipients of compensation
 - Description of any compensation to be received in connection with termination of the contract or arrangement and how any prepaid amounts will be calculated and refunded upon termination
- Recordkeeping services, if applicable, including direct and indirect compensation related to such services or, if not explicitly compensated, a reasonable and good faith estimate of the cost to the covered plan of such services

- Manner of receipt of the compensation
- Fiduciary services provided and related compensation
- Recordkeeping and brokerage services with respect to each designated investment alternative for which recordkeeping or brokerage services are provided

9.17.3.3 Timing Of Disclosures

- Required disclosures must be provided reasonably in advance of the date the contract or arrangement is entered into and extended or renewed.
- Changes must be provided as soon as practicable but no later than 60 days from the date on which the covered service provider is informed of the change.
- In the event of an error in a disclosure, the covered service provider must correct the information as soon as practicable but no later than 30 days after knowing of the error or omission.
- Requests for other compensation information from the fiduciary or covered plan administrator must be provided within 30 days following receipt of a written request.

9.17.3.4 Disclosures To Plan Participants

[ERISA Section 404(a)(5); SEC no-action letter to the Department of Labor dated October 26, 2011:
<https://www.dol.gov/newsroom/releases/ebsa/ebsa20120507-0>]

ERISA Rule 404(a)(5) requires the disclosure of certain plan and investment-related information, including performance information, to participants and beneficiaries in participant-directed individual account plans. Information is required to be presented in a comparative chart format to enable participants to make an informed decision when managing their accounts.

If CIM Securities compiles and/or provides the required information, it will comply with the requirements of Rule 404(a)(5). Where the investment alternatives include investment companies subject to other SEC and FINRA rules regarding communications with the public, the disclosures will comply with those requirements or exemptions to requirements.

9.17.4 Individual Retirement Accounts (IRAs)

[NYSE Information Memo 06-79]

IRAs are established by individuals through a plan sponsor; following are key features:

- Annual contributions are limited by law
- Older investors have higher contribution limits under a "catch-up" provision
- Contributions may or may not be tax deductible, depending on the IRA owner's income level
- Contributions are from earned income (other than contributions to a non-working spouse's IRA)
- Certain types of investments such as precious metals are not permitted in an IRA
- Early withdrawals (prior to age 59 1/2) may result in tax penalties
- Owners of traditional IRAs are required to begin withdrawing by the year following the year the owner turns 72

There are multiple types of IRAs including:

- Traditional IRAs; contributions may or may not be tax deductible depending on the IRA owner's income
- Roth IRA:

- all contributions are in after-tax dollars
- withdrawals are not taxed at the time of withdrawal if the IRA owner is at least 59 1/2 years old and the Roth IRA has been open 5 years or longer
- some high wage earners are not eligible to open Roth IRAs
- no mandatory withdrawals after age 72
- Individual retirement annuity; a traditional or Roth IRA set up with a life insurance company through the purchase of a special annuity contract
- Simplified Employee Pension (SEP-IRA); a traditional IRA set up by an employer for employees; limitations on contributions apply
- Spousal IRA; traditional or Roth IRA funded by a married taxpayer in the name of a spouse (who has limited earnings)
- Rollover IRA: funded with money that is already in a qualified retirement plan; allows moving the money without owing any tax at the time of the rollover (assuming the requirements for a rollover are met)

9.17.4.1 Rollovers

[FINRA Regulatory Notice 13-45]

If applicable, rollovers are transfers of IRA or other pension plans assets to a new plan. **RRs are not permitted to recommend rollovers; all such transactions must be marked "unsolicited."**

9.17.5 Employer-Sponsored Plans

Employers may offer different types of plans including traditional pension and profit-sharing plans that are funded entirely by the employer. All eligible employees participate and employer contributions are above and beyond the employee's salary. This section describes other types of employer-sponsored plans that give eligible employees the opportunity to put a portion of current income into a tax-deferred investment account. Participation may be voluntary or mandatory, and employers may make matching contributions.

The following sections provide a general explanation of these various plans.

9.17.5.1 401(k) Plans

- Established by corporations
- Permit their employees to make contributions through payroll deductions from pre-tax income [traditional 401(k) plans]; tax is applied when withdrawals are taken
- Roth 401(k) plans permit employees to make contributions through payroll from after-tax dollars; there is no tax on withdrawals made after age 59 1/2 and if the Roth 401(k) has been open 5 years or longer
- Both traditional and Roth 401(k) plans can be rolled over to an IRA (or a new employer's plan, if the plan permits) if the investor leaves the company
- No mandatory withdrawals for Roth 401(k) plans; mandatory scheduled withdrawals apply to traditional 401(k) plans

9.17.5.2 Limitations On Advice

[Pension Protection Act of 2006 Title VI; U.S. Department of Labor Field Assistance Bulletin No. 2007-01]

Providing investment advice to 401(k) plan sponsors and participants is subject to strict limitations and requirements. Providing investment advice places the RR in the role of a fiduciary which creates the legal liabilities associated with fiduciaries.

RRs are limited to offering firm-approved educational material and third-party advisory plans offered through CIM Securities.

9.17.5.3 403(b) Plans

[IRS 403(b) publication: <http://www.irs.gov/publications/p571/ch01.html>]

A 403(b) plan is a salary reduction plan offered by non-profit, tax-exempt employers such as schools and colleges, hospitals, and foundations. Individual accounts in a 403(b) plan invest in two categories of investments:

- An annuity contract provided through an insurance company (fixed or variable)
- Mutual funds

Features include:

- Individuals cannot establish 403(b) accounts; only employers may set up accounts
- For non-Roth plans:
 - Employees make pre-tax contributions and employers sometimes match contributions
 - Tax on contributions and earnings and gains on investments are paid when the investor begins withdrawing funds
 - Mandatory withdrawals after age 72
- If the plan is a Roth contribution plan, tax is paid on contributions to the plan but withdrawals are not taxed; no mandatory withdrawals
- Some 403(b) plans impose steep surrender charges

9.17.5.4 457 Plans

These plans are offered by a state or local government or a non-profit organization. A 457 plan is a deferred compensation plan similar to 401(k) or 403(b) plans.

- Pre-tax income is contributed
- No tax on contributions; withdrawals are subject to tax
- Technically the portion of salary contributed to the plan is not owned by the employee; the plan sponsor owns all of the 457 plan assets which are held in trust for the employee in an account set up in the employee's name
- Mandatory withdrawals after age 72
- No early withdrawal tax penalties if funds are paid to the employee when leaving the job prior to reaching age 59 1/2; withdrawal is subject to normal income tax
- May be rolled over to an IRA or a new employer's plan to retain tax-deferred status

9.17.5.5 SIMPLEs (Savings Incentive Match Plans For Employees)

- Offered by small companies with 100 or fewer employees who earn at least \$5,000 each during the year
- Less complicated to set up and administer than 401(k) or 403(b) plans
- Two types: SIMPLE IRA and SIMPLE 401(k), both with same contribution limits and catch-up contributions for people 50 or older

- Employer must contribute to the plan in one of two ways, a fixed contribution or a matching contribution
- Account must be open for 2 years before the employee can move the money or take it out; early withdrawal is subject to significant tax penalties

9.17.6 Definitions

Covered plan: An ERISA-covered defined benefit and defined contribution pension plan. Does not include simplified employee pension plans (SEPs), SIMPLE retirement accounts, IRAs, employee welfare benefit plans, and certain annuity contracts and custodial accounts described in ERISA Code section 403(b).

Covered principal transaction: For purchases from a Plan or an IRA: any security or other investment property. For sales to a Plan or an IRA, transactions involving: - US dollar denominated corporate debt securities offered pursuant to a registration statement under the Securities Act of 1933, - US Treasury securities, debt securities issued or guaranteed by a US federal government agency other than the US Department of the Treasury, - debt securities issued or guaranteed by a government-sponsored enterprise, - municipal securities, - certificates of deposit, - interests in Unit Investment Trusts.

Covered service provider: A service provider that enters into a contract or arrangement with the covered plan and expects \$1,000 or more in direct or indirect compensation that is received in connection with providing services defined in Section 408(b)(2) including:

- ERISA fiduciary service providers to a covered plan or to a "plan asset" vehicle in which such plan invests
- Investment advisers registered under Federal or State law
- Recordkeepers or brokers who make designated investment alternatives available to the covered plan (e.g., a "platform provider")
- Providers of one or more of the following services to the covered plan who also receive "indirect compensation" in connection with such services:
 - Accounting, auditing, actuarial, banking, consulting, custodial, insurance, investment advisory, legal, recordkeeping, securities brokerage, third party administration, or valuation services

Covered transactions: The exemption under 2020-02 covers reasonable compensation paid to financial institutions and investment professionals as well as their affiliates and related entities in connection with two types of transactions: investment advice provided to retirement investors and riskless and covered principal transactions.

Fiduciary: Generally anyone with discretionary authority or control over the management of a plan, the administration of the plan, or the disposition of plan assets. Fiduciaries must comply with certain statutory duties which include prudence and diversification of investments and the duty to act in accordance with the governing instruments of the plan. **This includes Investment Professionals and Institutions meeting the 5-part test in PTE 2020-02.**

Financial institution: An entity that: (i) is not disqualified or barred from making investment recommendations by any insurance, banking, or securities law or regulatory authority (including any self-regulatory organization); (ii) employs the Investment Professional or otherwise retains such individual as an independent contractor, agent or registered representative, and is: (iii) registered as an investment adviser under the Investment Advisers Act of 1940 or under state law; a bank or similar Financial Institution supervised by the United States or a state, or a savings association; an insurance company qualified to do business under the laws of a state, provided that it (A) has obtained a Certificate of Authority from the insurance commissioner of its domiciliary state which has neither been revoked nor suspended, (B) undergoes an annual examination by an independent certified public accountant or has undergone a financial examination by the state's insurance commissioner within the preceding five years, and (C) is domiciled in a state whose law requires an annual actuarial review of reserves to be reported to the appropriate regulatory authority; or (iv) a broker or dealer registered under the Securities Exchange Act of 1934.

Impartial Conduct Standards (applicable to fiduciary advice): The Impartial Conduct Standards have three components: a best interest standard, a reasonable compensation standard, and a requirement to make no misleading statements about investment transactions and other relevant matters.

- **Best Interest Standard:** Advice that (i) "reflects the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims, based on the investment objectives, risk tolerance, financial circumstances, and needs of the Retirement Investor," and (ii) "does not place the financial or other interest of the Investment Professional, Financial Institution or any Affiliate, Related Entity or other party ahead of the interests of the Retirement Investor, or subordinate the Retirement Investor's interests to their own."
- **Reasonable Compensation:** Compensation received by the Financial Institution, the Investment Professional, and any Affiliates and Related Entities must not exceed reasonable compensation within the meaning of ERISA section 408(b)(2). If applicable, the Financial Institution and Investment Professional must seek to obtain best execution (as required by securities laws) as part of the "reasonable compensation" requirement. Includes the requirements for best execution.
- **No Materially Misleading Statements:** The provider must not make materially misleading statements about the recommended transaction and other relevant matters at the time when the statements are made.

Individual Retirement Account (IRA): Any plan that is an account or annuity described in IRS Code section 4975(e)(1)(B) through (F).

Investment Advice: A five-part test to determine whether the institution or professionals are engaged in providing investment advice and therefore acting as a fiduciary; **all five parts must be satisfied to meet the definition:**

- render advice to the plan as to the value of securities or other property, or make recommendations as to the advisability of investing in, purchasing, or selling securities or other property
- provide advice on a regular basis
- provide advice pursuant to a mutual agreement, arrangement, or understanding the plan, plan fiduciary or IRA owner, that:
 - the advice will serve as a primary basis for investment decisions with respect to plan or IRA assets, and
 - the advice will be individualized based on the particular needs of the plan or IRA.

Investment Professional: A fiduciary of a Plan or IRA by reason of the provision of investment advice with respect to the assets of the Plan or IRA involved in the recommended transaction, who is an employee, independent contractor, agent, or representative of a Financial Institution, and satisfies the federal and state regulatory and licensing requirements of insurance, banking, or securities laws (including self-regulatory organizations) with respect to the covered transaction, as applicable, and is not disqualified or barred from making investment recommendations by any insurance, banking, or securities law or regulatory authority (including any self-regulatory organization).

Party-in-interest: A person or entity providing services to an ERISA plan is considered a "party-in-interest" to the plan.

Plan: Any employee benefit plan described in ERISA section 3(3) and any plan described in Code section 4975(e)(1)(A).

Prohibited transactions: Federal laws prohibit plan assets from being used by a fiduciary for certain transactions (known as "prohibited transactions"). Fiduciaries are prohibited from dealing in plan assets for their own benefit or for the benefit of a third party with whom the fiduciary is affiliated. The Department of Labor (and other government agencies) has issued exemptions from the prohibited transaction rules which allow plans and broker-dealers to engage in some but not all types of securities transactions. The range of permissible transactions varies depending on whether the broker-dealer is a fiduciary to the plan.

Prudent Investor Rule: Trading in ERISA accounts is subject to the "prudent investor" rule (also known as the Prudent Man Rule) which is a standard that is generally understood to mean that individuals involved with investment decision-making act with the same care, skill, prudence and diligence as a prudent man in the same capacity. This measure is not judged on the risk of a single investment but by the investment's relationship to the overall portfolio. ERISA also requires that investments in a covered plan be diversified to minimize the risk of large losses unless it is clearly prudent not to do so.

Retirement Investor: A participant or beneficiary of a Plan with authority to direct the investment of assets in his or her account or to take a distribution, the beneficial owner of an IRA acting on behalf of the IRA, or a fiduciary of a Plan or an IRA.

Riskless Principal Transaction: A Financial Institution, after having received an order from a Retirement Investor to buy or sell an investment product, purchases or sells the same investment product for the Financial Institution's own account to offset the contemporaneous transaction with the Retirement Investor.

9.18 Foreign Accounts

Accounts for residents of foreign countries may be subject to special requirements under securities laws of the foreign country. Before soliciting investors or opening an account for a person or entity residing in a foreign country, contact Compliance for further information regarding any special restrictions or requirements.

9.19 Payments To Unregistered Persons

[SEC Securities Exchange Act of 1934 Section 15(a); FINRA Rule 2040; FINRA Regulatory Notice 15-07]

Responsibility	<ul style="list-style-type: none"> • IB Supervisor • Compliance
Resources	<ul style="list-style-type: none"> • Requests regarding referral arrangements
Frequency	<ul style="list-style-type: none"> • Review of requests: As required • Annual: Review ongoing payments
Action	<ul style="list-style-type: none"> • Designated Supervisor: identify unauthorized referrals in reviews of public communications and refer them to Compliance for follow up • Compliance: <ul style="list-style-type: none"> ○ Confirm whether an unregistered person proposed to receive compensation is required to be registered by: <ul style="list-style-type: none"> ▪ Reviewing regulatory releases, no-action letters or interpretations ▪ Requesting an SEC no-action letter ▪ Obtaining a legal opinion from counsel ○ Review requests for referral arrangements and determine compliance with regulatory and firm policy requirements and approve or disapprove; for approved arrangements establish guidelines for arrangements including any compensation ○ For investment adviser referrals: <ul style="list-style-type: none"> ▪ If compensation will be received for referrals, determine whether investment adviser registration is required for CIM Securities and the RR

	<ul style="list-style-type: none"> ▪ Maintain a list of approved IAs ▪ Review IAs to be included on the approved list including registration status, investment policies, suitability guidelines for investors ▪ Establish monitoring program and monitor results vs. IA stated performance ▪ Re-evaluate IA participants at least annually <ul style="list-style-type: none"> ○ For foreign finders, conduct due diligence as outlined in <i>Referrals From Nonregistered Foreign Persons</i>; provide customer disclosure and obtain acknowledgment; and establish disclosure on customer confirmations • For hedge fund or other investment referrals, the proposed investment is subject to new product review procedures (see the related section in the chapter <i>FINANCIAL AND OPERATIONS PROCEDURES</i>)
Record	<ul style="list-style-type: none"> • Designated Supervisor review of communications and referrals to Compliance • Compliance: <ul style="list-style-type: none"> ○ Review/approval of referral arrangements ○ Reviews of IAs included on approved list ○ Reviews of nonregistered foreign persons; customer disclosure and acknowledgment ○ Records of monitoring and annual review

This section explains limitations and requirements for proposed payments to outside persons or entities and referral payments to other Firm employees or departments. Any such payments require **prior approval** by Compliance.

9.19.1 Definition Of Eligibility

FINRA rules prohibit firms or associated persons from directly or indirectly paying compensation, fees, concessions, discounts, commissions or other allowances to:

- any person that is not registered as a broker-dealer under Exchange Act Section 15(a); or
- any registered person unless such payment complies with all applicable federal securities laws, FINRA rules and Exchange Act rules and regulations.

Rule 2040(a) directs firms to look to SEC rules to determine whether the activities in question require registration as a broker-dealer under Exchange Act Section 15(a).

9.19.2 Referrals

Referrals are an important part of our business. Satisfied customers may refer others to CIM Securities and may also seek referrals from employees when they need services not provided by CIM Securities. It is important that referrals to others are based on sound knowledge about the other person or company. In addition, FINRA rules restrict compensation to unregistered persons or entities.

Key requirements regarding referrals include the following:

- Employees are expected to make referrals involving investments or investment advisory services only to persons or companies included in a firm-sponsored program or on a list of firm-approved providers.

- Employees are prohibited from receiving compensation for referrals except through firm-sponsored programs.
- Any proposed compensation, whether for referring or receiving referrals, must be approved **in advance** by Compliance.
- Referrals involving compensation may require disclosure to the customer of potential conflicts of interest.
- Non-cash compensation is subject to the policy described in the chapter *ORDERS*.

9.19.3 Referrals To Others

Employees **may not** accept compensation from someone outside CIM Securities for providing referrals. Compensation may be paid by CIM Securities under firm-sponsored programs such as wrap fee programs.

9.19.3.1 Referrals To Investment Advisers

Referring customers to investment advisers for compensation may require CIM Securities (and possibly the RR) to be registered as an investment adviser and investment adviser agent, respectively. If CIM Securities has a program for adviser referrals, required registrations will be obtained and a list of approved advisers will be provided to RRs. All advertising, sales material, marketing materials, scripts, and proposed presentations related to investment adviser referrals must be approved by Compliance prior to use.

Other than through firm-approved referrals, RRs should avoid referring customers to investment advisers unless Compliance has been contacted to make a determination regarding the registration status of the IA and to conduct other necessary reviews of the IA **before** making a referral.

9.19.3.2 Referrals To Hedge Funds Or Other Outside Investments

R Rs are expected to limit their investment recommendations to products or services offered by CIM Securities. Referrals to outside investments not part of a firm program are prohibited.

9.19.3.3 Referrals To Other Departments And Affiliates

Compensation paid by other firm departments because of business referrals must be reviewed and approved by Compliance **in advance**.

9.19.4 Referrals To The Firm

When others outside CIM Securities refer potential customers, referral fees or other compensation may not be paid to the outside person or firm. Questions and requests for exceptions should be referred to Compliance.

9.19.4.1 Referrals From Affiliated Bank Employees

[SEC Regulation R]

When operating on bank premises, compensation paid to unregistered bank employees for referring customers is strictly limited under federal regulations. RRs are prohibited from making payments to bank personnel and compensation is limited to a fixed dollar (not incentive) basis under CIM Securities's agreement with the bank.

9.19.4.2 Referrals From Nonregistered Foreign Persons

FINRA rules provide exceptions (with specific requirements) for payments to foreign persons who are not registered. Such arrangements require **prior** approval by Compliance. Payments for referrals from nonregistered foreign finders must meet the following requirements:

1. CIM Securities confirms that the finder is not required to be registered or is not subject to a disqualification and the arrangement does not violate foreign law;
2. the finder is a foreign national (not a U.S. citizen) or foreign entity domiciled abroad;
3. the customers are foreign nationals (not U.S. citizens) or foreign entities domiciled abroad transacting business in either foreign or U.S. securities;
4. customers receive a descriptive document, similar to that required by Rule 206(4)-3(b) of the Investment Advisers Act, that discloses what compensation is being paid to finders;
5. customers provide written acknowledgment to CIM Securities of the existence of the compensation arrangement and such acknowledgment is retained and made available for inspection by FINRA;
6. records reflecting payments to and arrangements with finders are maintained in CIM Securities's books and records; and
7. the confirmation of each transaction indicates that a referral or finder fee is being paid pursuant to an agreement.

9.20 Death Of A Customer

When a customer dies, the account assets owned by the deceased person may become subject to a will, estate laws, and other governing laws or documents. The assets are, therefore, frozen in the account until necessary documents are received and legal distribution has been determined. Joint accounts and other accounts where the deceased person is a joint owner with others may be subject to certain distribution requirements depending on the styling of the account.

When a customer dies, the RR should:

- immediately notify Operations
- consider assets in the deceased person's account as "frozen" until distribution of assets has been determined, *i.e.*, accept no orders and do not authorize sending of securities or funds from the account
- cancel all open orders

9.21 Active Accounts

If applicable, the IB Supervisor and/or Compliance will, on a quarterly basis, review accounts that are identified as "active." Items to be reviewed include, depending on the type of account and type of trading activity:

- Review of new account documentation to determine necessary documents are on file and to identify the customer's investment objectives and financial profile
- Review of trading activity in the account including types and size of trades and frequency of trades
- Contact with the RR and designated supervisor to determine additional information regarding the customer and trading activity

Additional reviews that may be conducted include:

- Profit and loss or change of equity calculation
- Turnover calculation
- Contact with the customer (written or oral)

Reviews of active accounts may include these items or other items at the discretion of Compliance. Compliance will establish the criteria and procedures for conducting the active account review.

Compliance, in conjunction with the designated supervisor of the department or branch handling the account, will determine whether contact will be made with the customer and whether that contact will be in the form of a letter, telephone call, or face-to-face contact to confirm investment objectives and the customer's knowledge regarding the trading activity in the account. All records of customer contact in conjunction with active account reviews (including telephone conversations and face-to-face meetings) are to be maintained in a file for the customer or an active accounts file.

9.22 Concentrations – Not applicable at Present

Accounts that are concentrated in certain security positions may increase risk for the customer, particularly if the security is purchased on margin. RRs must consider the following factors for concentrated customer accounts:

- Is the concentrated position in a margin account?
- Do trading characteristics (thinly-traded, limited markets) create added risk to the customer?
- If the concentrated position is higher-risk, is the customer aware of this risk and suitable for such a position or positions?
- Should the concentrated position be mitigated by reducing margin exposure or selling off some of the position?

10 SUPERVISORY SYSTEM, PROCEDURES, AND CONTROLS

[SEC Securities Exchange Act of 1934 Section 15(f); FINRA Rule 3110, 3120 and 3130; FINRA web page: <http://www.finra.org/RulesRegulation/IssueCenter/SupervisoryControl/index.htm>; MSRB Rule G-27; NASDAQ Rule 3010]

10.1 Introduction

CIM Securities has established a supervisory system, procedures and controls reasonably designed to comply with regulators' rules.

Supervisory system: The internal system to oversee business includes the designation of supervisors and allocation of responsibilities; assignment of RRs to appropriate supervisors; identification of areas of business and rules that govern those businesses; and development of procedures.

Supervisory procedures: Procedures in this manual (and in other policies or manuals, if referenced in specific chapters) include:

- compliance procedures for RRs and others that explain rule requirements and prohibitions as well as internal policies when conducting sales and other activities; and,
- supervisory procedures that explain how supervisors are to conduct their ongoing responsibilities. Most supervisory procedures are explained in "matrixes" that appear throughout this manual and include the following:

Responsibility	<ul style="list-style-type: none">• Who is the responsible supervisor? <i>Supervisors are sometimes referenced by name, sometimes by title or as "designated supervisor" which is cross-referenced to the "Designation Of Supervisors" table that appears in this manual.</i>
Resources	<ul style="list-style-type: none">• The information / reports / documents that supervisors use to conduct supervision.
Frequency	<ul style="list-style-type: none">• How often are supervisory reviews to be conducted (daily, weekly, etc.)?
Action	<ul style="list-style-type: none">• How supervision is to be conducted (<i>i.e.</i>, review a report, read correspondence, interview RR or customer, etc.).
Record	<ul style="list-style-type: none">• What record is made that supervision was conducted? <i>Generally supervisors are expected to initial and date reports or other records, note any action taken, and retain that information in their files.</i>

Supervisory Controls: Controls refer to testing and evaluation of systems and procedures to measure and maintain their effectiveness. Internal controls typically involve sampling of functions to test effectiveness and identify shortcomings, gaps, or other inefficiencies in supervisory systems and procedures. Internal controls also involve the ongoing reassessment of these functions to determine whether they are serving their intended purpose.

10.2 Responsibility

Responsibility for CIM Securities's supervisory system, policies, and controls includes the following:

- The Chief Compliance Officer (CCO) is responsible for establishing and maintaining the supervisory system, policies and procedures for all areas of the firm.
- The Financial and Operations Principal (FINOP) is responsible for establishing and maintaining systems, policies and controls regarding financial and accounting procedures and reporting.

10.3 Controls

10.3.1 Verification And Testing

CIM Securities periodically conducts reviews to test and verify its supervisory system and controls.

Testing and verification generally include:

- Identifying areas to be reviewed at least annually
- Developing reviews and a schedule for conducting the reviews
- Assigning responsibility for conducting reviews
- Preparing reports of reviews
- Providing reports to management, the audit committee, and other appropriate personnel for potential corrective action
- Following up regarding deficiencies in subsequent reviews

Records of testing are maintained by the department responsible for conducting testing and include:

- areas to be reviewed
- schedule of reviews
- reports of findings including a record of distribution of the report and responses from the supervisor of the area examined
- follow-up or corrective action taken

Testing and verification is the responsibility of:

- Compliance - compliance systems and procedures

10.3.2 Risk Management

[FINRA Notice to Members 99-92]

CIM Securities has established risk management procedures which are outlined in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*, in the section *Risk Management*.

10.3.3 Outside Auditors

CIM Securities's outside auditors conduct an annual review of internal financial and operational controls as well as compliance with selected rules and regulations. The FINOP (and other personnel, as required) is responsible for working with the outside auditors and providing them with requested information. The auditors' report is provided to senior management and CIM Securities's audit committee (if an audit committee has been established) who are responsible for delegating responsibility for taking corrective action on exceptions noted in the report.

The FINOP retains records of outside audits and reports.

10.4 Written Compliance And Supervisory Procedures

[SEC Securities Exchange Act of 1934 Rule 17a-4(e)(7); FINRA Rule 3110(b)(7) and 3110.11]

Compliance is responsible for maintaining and updating CIM Securities's compliance and supervisory procedures which are included in this manual.

This manual is updated and policies distributed as follows:

- New and amended rules and releases from regulators are reviewed on an ongoing basis and changes considered for written procedures and incorporated where necessary. Changes are considered at least bi-monthly.
- Changes are incorporated in written procedures including the date of the revision.
- Prior versions of the manual are archived for books and records purposes.
- When policy and procedure changes affect personnel, Compliance will distribute new or revised policies as follows:
 - In written form, where practical
 - By email
- Compliance provides manuals to new employees and obtains receipts that are maintained in employee or other compliance files.
- If a new policy manual is distributed, receipts will be requested and maintained in employee or compliance files.
- Policies may be made available to employees in electronic format. Changes will be promptly posted to the electronic version of policies and procedures.
- Electronic versions are protected to prevent changes by unauthorized persons. Compliance maintains a record of those authorized to change and post policies and procedures.

10.5 Chief Compliance Officer (CCO)

[FINRA Rule 3130(a)]

CIM Securities has designated a CCO who is listed on the *Designation Of Supervisors* chart and Schedule A of Form BD which is filed with regulators.

10.6 Internal Inspections

[FINRA Rule 3110(c)]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Records, reports, policies and procedures
Frequency	<ul style="list-style-type: none">• Annual (or more frequently for certain high-risk areas)
Action	<ul style="list-style-type: none">• Identify business areas subject to review• Prepare schedule of inspections considering the risk profile of each business area• Assign inspection responsibility considering any potential conflicts of interest including economic, commercial, or financial interests in the associated persons or business being inspected and ensuring the person assigned does not work in the business unit and is not directly or indirectly supervised by, or otherwise reporting to, an associated person assigned to the unit or location. Where compliance is not possible due to CIM Securities's size or business model, document in the report both the factors used to make this determination and how the inspection otherwise complies with the requirements of Rule 3110(c)(1)• Prepare draft report of review and provide to appropriate supervisory personnel for comment• Prepare final report and send to supervisor of the business area and senior management• Obtain response regarding corrective action from the supervisor• Follow up regarding deficiencies (at the latest at the next inspection)
Record	<ul style="list-style-type: none">• Records of internal inspections including when conducted, who conducted them, and reports and responses

CIM Securities reviews, at least annually on a calendar-year basis, the businesses in which it engages to identify potential non-compliance with Firm policies and procedures and regulatory rules, laws, and regulations.

Reviews may be conducted through a number of resources including (but not necessarily limited to):

- Compliance
- Clearing firm (for those areas that are the clearing firm's responsibility)
- Internal audit
- Outside auditors
- Outside consultants
- Risk management

Reviews conducted internally may use different approaches:

- Review of a specific period of time
- Review based on a sampling of the activity
- Other reviews appropriate to the area of business

OSJ and branch office inspections are described in the chapter *OFFICES* in the section *Office Inspections*.

10.7 Review And Testing Of Procedures And Controls

[FINRA Rule 3120(a)]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Records, reports, policies and procedures
Frequency	<ul style="list-style-type: none">• Annual
Action	<ul style="list-style-type: none">• Test procedures/controls• Identify gaps in procedures and document• Revise procedures where necessary
Record	<ul style="list-style-type: none">• Documentation of reviews and testing• Revised policies and procedures, as appropriate

CIM Securities conducts reviews of its supervisory procedures and controls at least annually to confirm procedures are current and include all areas of business. Procedures and controls are also tested to determine they achieve the necessary levels of compliance. Findings from internal inspections are also considered in this review.

Reviews and testing may be conducted through a number of resources including (but not necessarily limited to):

- Compliance

10.7.1 Conducting Risk-Based Reviews And Testing

Reviews and testing will be documented on the *Supervisory Policies, Procedures, And Controls Review & Testing* form or through similar types of reports or forms. This includes identifying who is conducting the review/testing and assigning risk levels to different areas of business. Areas of higher risk will be subject to more frequent and/or more extensive reviews which may include look-backs, larger samples and/or longer time periods for review, certifications by supervisors, or other reviews determined by the reviewer(s).

10.7.2 Findings And Follow-Up

Findings from reviews and testing are included in the CEO report and annual certification discussed in the next section. Compliance is responsible for:

- Amending policies and procedures to address gaps
- Reporting deficiencies (found in testing) to supervisors of appropriate business areas
- Follow up to determine deficiencies have been addressed
- Assembling findings for inclusion with the CEO report and annual certification (next section)

10.8 Internal Investigations Of Transactions

[FINRA Rule 3110(d)]

CIM Securities reviews securities transactions to identify trades that may violate provisions of the Exchange Act and its rules, rules of exchanges, or FINRA rules prohibiting insider trading and manipulative and deceptive devices. The accounts subject to these reviews include:

- accounts of CIM Securities;
- accounts introduced or carried by CIM Securities in which a person associated with CIM Securities has a beneficial interest or the authority to make investment decisions;
- outside accounts of a person associated with CIM Securities (see *Outside Accounts* in the chapter *GENERAL EMPLOYEE POLICIES*); and
- covered accounts (see definition below).

"Covered accounts" include any account, if applicable, introduced or carried by CIM Securities that is held by:

- the spouse of a person associated with the member;
- a child of the person associated with the member or such person's spouse, provided that the child resides in the same household as or is financially dependent upon the person associated with the member;
- any other related individual over whose account the person associated with the member has control; or
- any other individual over whose account the associated person of the member has control and to whose financial support such person materially contributes.

For questioned trades, a prompt internal investigation will be conducted to determine whether a violation of laws or rules has occurred.

10.8.1 Internal Investigation Reports

CIM Securities engages in investment banking services as defined in FINRA Rule 3110(d)(4)(B) and is required to file reports of internal investigations of transactions.

Potentially violative trades include:

- Trades in securities on Firm restricted lists
- Trading ahead of customer orders
- Trading ahead of block orders (frontrunning)
- Trading by research personnel in securities the subject of research recommendations
- Trading by investment banking or public finance personnel in securities the subject of banking engagements
- Trades in securities of companies before significant market-moving events affecting the company's securities

When a potential violation is identified, Compliance will:

- review the circumstances of the transaction including contact with the RR and RR's supervisor.
- determine whether a violation has occurred.
- determine (in consultation with outside counsel or others, if necessary) what corrective action should be taken.
- report to FINRA within 5 business days any internal investigation that concludes a violation has occurred.
- file a quarterly report with FINRA of internal investigations within 10 business days of the end of each calendar quarter.

- determine whether the violation must be reported in another form such as updating Form U4 or U5.

10.9 Escalation Of Issues

Employees (including supervisors) have an obligation to report issues that are potential problems involving wrongdoing. While each incident is unique, following is a general protocol for escalating such reporting when necessary.

1. The potential problem should initially be reported to the individual's direct supervisor.
2. If the problem involves the direct supervisor, or it appears there is inadequate response from the direct supervisor, report the issue to the direct supervisor's supervisor.
3. If the issue involves the supervisor's supervisor, or if it appears there is inadequate response, contact Compliance or internal counsel.
4. Compliance or internal counsel may:
 - contact outside counsel for further guidance
 - notify senior management
 - notify regulators

10.10 Annual Report And Certification Of Compliance And Supervisory Processes

[FINRA Rule 3120 and 3130]

Compliance prepares an annual compliance report for the CEO (or equivalent officer).

10.10.1 Meetings Between CEO And CCO

The CEO or equivalent officer meets once or more annually with the CCO to review compliance matters the subject of the annual certification.

10.10.2 Annual Report To CEO

The CCO will prepare and provide the CEO (or equivalent officer) with an annual report that includes a review of CIM Securities's supervisory system and procedures and key compliance issues. The report will also include a summary of testing results including significant identified exceptions and any amended supervisory procedures adopted in response to the test results. The CCO will meet with the CEO to discuss and review the report and will meet at other times, as needed, to discuss other compliance matters. If CIM Securities has designated multiple CCOs, each CCO will meet with and prepare a report for the CEO annually.

The annual report will be provided to members of the board of directors (or equivalent senior management) and the audit committee, if one has been established. The report will be provided to these governing bodies at the earlier of their next scheduled meetings or within 45 days after execution of the certification.

10.10.2.1 Firms With Annual Gross Revenue Of \$200 Million Or More

[FINRA Rule 3120(b)]

If CIM Securities has reported \$200 million or more in gross revenue in the previous calendar year, the report to the CEO must include the following, to the extent applicable to CIM Securities's business. Compliance is responsible for confirming whether this requirement applies.

(1) a tabulation of the reports pertaining to customer complaints and internal investigations made to FINRA during the preceding year; and

(2) discussion of the preceding year's compliance efforts, including procedures and educational programs, in each of the following areas:

- trading and market activities;
- investment banking activities;
- antifraud and sales practices;
- finance and operations;
- supervision; and
- anti-money laundering.

For purposes of this requirement, "gross revenue" means:

(1) total revenue as reported on FOCUS Form Part II or IIA (line item 4030) less commodities revenue (line item 3990), if applicable; or

(2) total revenue as reported on FOCUS Form Part II CSE (line item 4030) less, if applicable, (A) commissions on commodity transactions (line item 3991); and (B) commodities gains or losses (line items 3924 and 3904).

10.10.2.2 Certification

Annually (after receipt and review of the report), the Chief Executive Officer (or equivalent) will certify that CIM Securities has in place processes to establish, maintain, review, test, and modify written compliance policies and written supervisory procedures reasonably designed to comply with regulators' rules. Certification does not, by itself, establish line supervisory responsibility for those involved in the certification process. If CIM Securities has co-CEOs, each CEO will certify as if he/she were acting as sole CEO.

10.11 Supervision Of Supervisors

[FINRA Rule 3110(b)(6)(c) and 3110.10]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Designation of supervisors
Frequency	<ul style="list-style-type: none">• Ongoing
Action	<ul style="list-style-type: none">• Identify and designate supervision of supervisors and include in the "<i>Designation Of Supervisors</i>" chart, confirming supervision complies with the requirements of

	<p>this section ensuring supervisors do not report to someone they supervise or have compensation determined by such a person</p> <ul style="list-style-type: none"> • Identify supervisors who handle customer accounts and establish supervision in accordance with established procedures for supervising accounts • Where compliance with these requirements is not possible because of the size of CIM Securities or a supervisor's position in CIM Securities, document the factors used in making such a determination and how an alternative arrangement complies with the requirements • Ensure designated supervisors are aware of the designation and their responsibilities • Include review of supervision in inspections of offices
Record	<ul style="list-style-type: none"> • Designation of supervisors confirmation such designations do not conflict with requirements to exclude supervision by those reporting to the supervisor or who determines the supervisor's compensation • Documentation of exceptions • Reviews of supervisors' customer accounts • Review of supervision as part of inspection reports

Supervisors are subject to supervision of their activities by other designated supervisors. Supervisors are not permitted to:

- supervise their own activities; and
- report to, or have their compensation or continued employment determined by, a person or persons they are supervising.

Where it is not feasible to comply with these requirements, CIM Securities's records will be documented justifying the exception and how supervisory requirements will be met. Rule exceptions include instances where:

- CIM Securities is a sole proprietor in a single-person firm;
- a registered person is CIM Securities's most senior executive officer (or similar position); or
- a registered person is one of several of CIM Securities's most senior executive officers (or similar positions).

10.11.1 Supervision Of Customer Account Activity

As required by rule, all supervisors will be assigned to a designated supervisor who is responsible for oversight of the supervisor's activities.

Day-to-day customer account activity conducted by office managers, sales managers, regional or district managers or other supervisors is subject to review and supervision by someone senior to or independent of the supervised person. This includes account activity in family accounts.

10.12 Conflicts Of Interest

[FINRA Report on Conflicts of Interest October 2013]

CIM Securities has an obligation to mitigate potential conflicts of interest and put the customer's interest before its own. Potential conflicts are addressed in the following sections which also address supervision of these potential conflicts.

1. CIM Securities's addresses the following issues, as applicable:
 - Confidentiality of CIM Securities's business, its employees, customers, suppliers or consumers
 - Actions constituting acting in self-interest
 - Gifts and entertainment
 - Bequests
 - Privacy of customer information and requests for information from affiliates
 - Holding outside offices or appointments
 - Internal accounting controls
 - Reporting ethics violations and disciplinary action
 - Trading in the stock of Firm customers, suppliers, or vendors
 - Full and fair disclosure regarding documents filed on behalf of CIM Securities
 - Employee compliance with Firm policies and rule requirements, obligations to report
 - Contacts regarding ethics issues
 - Supervision vested in supervisors
 - Administration of the Code of Ethics
2. Insider trading (*see the chapter INSIDER TRADING*)
3. Policies regarding employee outside business activities, outside accounts (*see the chapter GENERAL EMPLOYEE POLICIES*)
4. Customer privacy policies and procedures (*see the chapter COMMUNICATIONS WITH THE PUBLIC*)
5. Identity theft (*see the chapter ACCOUNTS*)

10.13 Cross Reference To Other Supervisory Control Subjects

The purpose of this section is to identify SRO supervisory control rule subjects that do not appear in the chapter *SUPERVISORY SYSTEM, CONTROLS AND PROCEDURES* and that appear in other chapters of this manual.

Subject	CHAPTER	Section / Subsection(s)
Transmittals of customer funds and securities to: <ul style="list-style-type: none">• Third parties• Outside entities (banks, investment companies, <i>etc.</i>)• Post office or c/o addresses• Customer by RRs	FINANCIAL AND OPERATIONS PROCEDURES	Transmittals Of Customer Funds And Securities
Customer changes of address	ACCOUNTS	<ul style="list-style-type: none">• Addresses On Customer Accounts• New Accounts - Post Office Addresses

Customer changes of address	FINANCIAL AND OPERATIONS PROCEDURES	Customer Confirmations And Statements - Change Of Customer Addresses On Accounts
Confirming changes in customer investment objectives ['34 Act Rule 17a-3(17)(i)(A)]	ACCOUNTS	<ul style="list-style-type: none"> • New Accounts - Customer Account Information • Updating Account Information And Periodic Affirmation
Time and price discretion for orders [FINRA Rule 3260]	ORDERS	Time And Price Discretion
Account designation changes on orders [FINRA Rule 4515]	ORDERS	Account Designation And Cancels/Rebills
Holding customer mail	FINANCIAL AND OPERATIONS PROCEDURES	Customer Confirmations And Statements - Hold Mail Instructions
Office inspections	OFFICES	Office Inspections

11 OFFICES

This chapter describes the types of offices defined by regulators and requirements for inspections and supervision of offices. **Compliance must be notified:**

- Before a new branch office or other business office is opened (including all types of offices defined in this chapter)
- When an office address changes
- Prior to a change in the types of business conducted in an office
- When an RR changes offices
- Prior to an RR commencing work from a second location, such as a primary residence
- Prior to establishing an office-sharing arrangement with an outside person or entity

11.1 Office Designations

[FINRA Rule 3110]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Information regarding offices including new offices, address changes, office sharing arrangements
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Identify each office as to type to determine regulatory requirements, maintain list of offices and types• Establish and document supervision for non-branch locations• Make required regulatory filings• Review requests for a principal to supervise more than one OSJ considering the following:<ul style="list-style-type: none">○ whether the on-site principal is qualified by virtue of experience and training to supervise the activities and associated persons in each location;○ whether the on-site principal has the capacity and time to supervise the activities and associated persons in each location;○ whether the on-site principal is a producing registered representative;○ whether the OSJ locations are in sufficiently close proximity to ensure that the on-site principal is physically present at each location on a regular and routine basis; and○ the nature of activities at each location, including size and number of associated persons, scope of business activities, nature and complexity of products and services offered, volume of business done, the disciplinary history of persons assigned to such locations, and any other indicators of irregularities or misconduct.
Record	<ul style="list-style-type: none">• List of offices including types of offices• Regulatory filings

	<ul style="list-style-type: none"> • Approval for one principal to supervise more than one OSJ and document why such a supervisory structure is reasonable
--	---

This section describes different types of offices and related requirements.

11.1.1 Branch Office

[FINRA Rule 3110(a)(3), 3110(a)(4) and 3110(f)(2)]

A branch office is any location where one or more associated persons (e.g., employees, independent contractors) regularly conduct the business of effecting any transactions in or inducing or attempting to induce the purchase or sale of any security or any location held out as such. Branch offices are required to be registered, and if the "main office" meets the definition of "branch office" (or OSJ) it is required to be registered.

Any office that is responsible for supervising associated persons at one or more non-branch locations is considered to be a branch office.

11.1.2 Non-Branch Locations

[FINRA Rule 3110(f)(2)]

There are seven exceptions from the branch office registration requirement. To qualify for an exception, all conditions must be met for the office location. All non-branch offices and their associated persons are assigned to a designated branch office for supervision.

Non-sales locations: Locations established solely for customer service and/or back office functions, not to be held out to the public as a branch office, and no sales activities are conducted from the location.

Primary residences: Any location that is the associated person's primary residence. Only one associated person, or multiple associated persons who reside at the location and are members of the same immediate family, may conduct business from the location. Requirements for primary residence offices include:

- Only one associated person, or multiple associated persons who reside at that location and are members of the same immediate family, conduct business at the location;
- The location is not held out to the public as an office and the associated person does not meet with customers at the location;
- Neither customer funds nor securities are handled at that location;
- The associated person is assigned to a designated branch office, and such designated branch office is reflected on all business cards, stationery, retail communications and other communications to the public by such associated person;
- The associated person's correspondence and communications with the public are subject to CIM Securities's supervision in accordance with this Rule;
- Electronic communications (e.g., e-mail) are made through CIM Securities's electronic system;
- All orders are entered through the designated branch office or an electronic system established by the member that is reviewable at the branch office;
- Written supervisory procedures pertaining to supervision of sales activities conducted at the residence are maintained by CIM Securities; and
- A list of the residence locations is maintained by Compliance.

Locations other than primary residences: Other locations used for securities-related activities less than 30 business days in any calendar year that meets the requirements of a primary residence office, above. This would

generally include vacation or second homes and other non-primary residences. An RR operating from this type of location will be required to maintain a record of the dates when business is conducted from such a location and submit this information monthly to Compliance. When the "30-business day" exemption is exhausted, the RR is required to cease conducting business from that location or immediately submitting a request to Compliance to register the location as a branch office.

Offices of convenience: This is a location where an associated person occasionally and exclusively by appointment meets with customers, provided the location is not held out to the public as a branch office. An associated person may not establish business hours at the location or hold out the location in any way (except for signage required at bank locations). Final approval and execution of transactions must be done through the designated supervisory branch office.

Location used primarily to engage in non-securities transactions: Locations where associated persons are primarily engaged in non-securities activities (e.g., insurance sales) and where the associated person effects no more than 25 securities transactions in a calendar year. Retail communications identifying the non-securities location must include the location of the supervising branch office. Compliance is responsible for monitoring the 25-transaction limit.

Floor of a registered national securities exchange: Any location on the floor of a registered national securities exchange where CIM Securities conducts a direct access business with public customers is exempt from the definition of "branch office."

Temporary location: Any temporary location established in response to the implementation of a business continuity plan is exempt from branch office registration.

Regardless of the above exceptions to the definition of "branch office," any location that is responsible for supervising activities of RRs at one or more non-branch locations is considered to be a branch office.

11.1.3 Offices Of Supervisory Jurisdiction (OSJ)

[FINRA Rule 3110(a)(3), 3110(a)(4), 3110(f), 3110.02 and 3110.03]

An office that includes any of the following activities will be designated as an Office of Supervisory Jurisdiction (OSJ) with a resident principal responsible for supervision:

- Order execution and/or market making
- Structuring of public offerings or private placements
- Maintaining custody of customers' funds and/or securities
- Final acceptance (approval) of new accounts
- Review and approval of customer orders
- Final approval of retail communications
- Supervision of RRs at one or more other branch offices

In addition, the following factors will be considered on determining whether an office is an OSJ:

- whether registered persons at the location engage in retail sales or other activities involving regular contact with public customers;
- whether a substantial number of registered persons conduct securities activities at, or are otherwise supervised from, such location;
- whether the location is geographically distant from another OSJ of CIM Securities;
- whether the member's registered persons are geographically dispersed; and
- whether the securities activities at such location are diverse or complex.

Excluded from the definition of OSJ is an office that solely provides final approval of research reports.

An OSJ principal will supervise only one OSJ; exceptions must be approved by Compliance.

11.1.4 Branch Offices Assigned To OSJs

Each branch office that is not an OSJ will be assigned to the supervision of an OSJ. The designated supervisor is required to visit non-OSJ branch offices on a periodic basis and record the visit in a memorandum or other record to be retained by the designated supervisor for the branch location. All business transacted by non-OSJ branch offices must be processed through the supervising OSJ. The designated supervisor is responsible for supervision of the branch office's activities and maintaining files for complaints, communications, new accounts, option accounts, advertising, and transactions originating from the branch office.

A branch office may be a "supervisory branch office" that has responsibility to supervise one or more other offices or a "non-supervisory branch office" that has no supervision over other offices.

11.2 Approval Of Persons To Operate In Non-Branch Locations

Because of the remote nature of some non-branch locations, approval is required **prior to** allowing an RR to operate from a non-branch location. The Firm's senior management will approve/disapprove at the time of new hire, taking into consideration effective supervision of non-branch location, its FINRA Membership Agreement and other factors.

11.2.1 Primary Residence Offices

[FINRA Rule 3110(f)]

On a case by case basis, an RR's request to conduct business from their primary residence may be considered provided that, at a minimum, the RR is currently employed by CIM Securities and is in good standing with both CIM Securities and supervising regulatory authorities. Compliance must approve any such arrangement. The form "Office Locations - Request For Approval" must be submitted to Compliance. The RR must submit a signed acknowledgment that he/she has read and understands this policy.

RRs approved for working from their primary residences may do so as long as the residence is not held out to the public as a branch office, and that they adhere to all relevant policies and procedures of CIM Securities. The following requirements must also be met:

- only one Firm RR may conduct business from the location (unless otherwise approved by Compliance)
- the RR does not meet with customers at the location
- customer funds and securities are not handled at the location
- the RR is assigned to a designated branch office, and such office is reflected on all business cards, stationery, advertisements, and other communications to the public
- the RR's outgoing customer communications sent from the primary residence are **pre-approved** by his/her designated supervisor
- all electronic business communications (*i.e.*, e-mails, faxes) are transmitted through Firm systems
- all customer orders are entered through the designated branch office or, if approved, via a Firm-approved system
- all required branch records are maintained at the designated branch office location

Other requirements:

- the RR may not use his/her personal e-mail accounts (*i.e.*, yahoo, gmail, *etc.*) to communicate with existing or potential clients; only Firm electronic systems may be used for customer communications

- all Firm system installations must be supervised by the Information Officer or IT department and in accordance with all Firm policies

11.3 Supervision Of Non-Branch Locations

Each non-registered location will be assigned for supervision to a designated supervisor in a registered branch office. Compliance will determine the scope of supervision and notify the designated supervisor considering factors including the number of RRs, types of business conducted, volume of business, qualification and history of on-site personnel (e.g., whether there is a registered supervisor at the location, whether RRs have disciplinary or complaint histories), and the nature and extent of RRs' outside business activities.

The designated supervisor will conduct ongoing reviews and retain records of the reviews at the designated branch location, which is subject to inspection, including records of non-branch office supervision.

11.4 Supervision Of Producing Managers

[FINRA Rule 3110(b)(6)(c) and 3110.10]

The customer account activities of managers and other supervisors are subject to supervision. Procedures are included in the chapter *SUPERVISORY SYSTEM, PROCEDURES, AND CONTROLS* in the section *Supervision Of Producing Managers' Customer Account Activity*.

11.5 Office Records

[SEC Securities Exchange Act of 1934 Rule 17a-3 and Rule 17a-4]

Each office is required to maintain or have access to certain records relating to the business conducted in the office. "Office," for records purposes, means any location where an associated person conducts business (not including a home office or the office of a customer that a RR visits regularly). "Conducting business" includes handling funds or securities or soliciting/accepting orders. Each office is required to designate someone who can explain the office records to regulators.

There are two aspects to records requirements: *retention* and *access*. Documents (paper or electronic) regarding CIM Securities's business ("books and records") must be retained for periods of time specified by regulators. Where CIM Securities's required books and records (such as order tickets, communications, *etc.*) are not retained at the office that created the records, there is a requirement that the records must be produced within a reasonable period of time upon request from a regulator that visits the office.

This section describes both types of requirements. All questions regarding books and records should be referred to Compliance.

11.5.1 Retention Of Records At The Office

Offices are required to retain the following records:

- Order records (3 years, 2 recent years in an accessible location)
- New account records (6 years after account closing, in an accessible location)
- Communications, incoming and outgoing (3 years, 2 recent years in an accessible location)
- Advertising (3 years, 2 recent years in an accessible location)

- Operations records including records of receipt/delivery of securities or funds (3 years, 2 recent years in an accessible location)
- Complaints (3 years, 2 recent years in an accessible location)

11.5.2 Forwarding Records To Home Office

The following records must be forwarded to home office for retention, as applicable:

- Order records
- New account records
- Communications, incoming and outgoing
- Advertising
- Operations records including records of receipt/delivery of securities or funds
- Copies of complaints

11.5.3 Access To Records

For records that are **not** maintained at the office location, the following records (as applicable) for the most recent two-year period will be produced at the office location promptly upon request of a regulator. **Regulators' requests should immediately be referred to Compliance for response.** "Promptly" is generally understood to mean within 24 hours of the request.

- Order records (daily trade blotters, order tickets/memoranda, including for the firm account)
- Receipts/deliveries of securities, receipts/disbursements of cash, all other debits/credits
- Employee records (U4, employment application, compensation agreements, CRD numbers, internal identifying numbers, offices where RR conducts business)
- Customer account records
- Complaints
- Transactions, by RR, including compensation earned, commission schedules, method by which compensation is determined
- Communications with the public: originals of communications received, copies of communications sent; approval of outgoing communications including correspondence, retail communications, and (if applicable) institutional communications
- Record naming the person in the office who can explain records
- Record listing the person responsible for policies and procedures
- Compliance and supervisory manuals, including updates and revisions, until three years after termination of use of the manual

11.5.4 Regulatory Requests For Records

If a regulator (SEC, SRO, state regulator, or other) requests office records (in person or by another means), Compliance should be contacted immediately. CIM Securities is obligated to provide prompt response to regulators' requests for information, therefore it is important the record retrieval process begin immediately or as soon as possible after receipt of the request.

11.6 Changes In Branch Offices

[FINRA By-Laws Article IV Section 8]

Compliance is responsible for filing the uniform branch office registration form (Form BR) with the CRD to reflect changes to existing offices or to register new offices. Compliance retains records of branch registration filings.

In addition, Compliance will verify state requirements before an office is opened and will file any necessary application or documents with state authorities which may include the secretary of state, taxing authorities, and/or broker-dealer licensing authorities.

11.7 Closing Offices

When an office is closed (and not just moved to another location), the designated supervisor is responsible for the following, as applicable:

- Obtain all access cards or keys from branch personnel and change locks until the office is completely closed.
- Secure computers and other office equipment and arrange for removal and preservation of data.
- Secure branch files and transfer to Compliance or another department for record preservation.
- Secure and transfer operations records to appropriate operations area.
- Notify customers affected by the closing.
- Finalize real estate issues such as leases.
- Maintain a record of the above closing procedures for the branch and notice to customers.

When an office is relocated, the supervisor must secure all property and records and oversee transfer to the new location. Keys/access cards for the closed office will be collected from employees and new keys/access cards issued for the new office location.

11.8 Use Of Office Space By Others

[Form BR]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Requests for office-sharing arrangements involving outsiders
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Review the potential arrangement to determine that it will be clear to the public which entity they are dealing with, considering the following:<ul style="list-style-type: none">○ Amount of customer traffic in the office○ Physical separation○ Clearance with the fidelity insurance carrier○ Posting the name of each entity on the door to their working place○ The entities' names are not listed under the same telephone number○ CIM Securities's phone number is not used on the letterhead, business cards, or on any advertising of the outside entity

	<ul style="list-style-type: none"> ○ Employees of each organization will wear a badge identifying their employer ○ Any other considerations • When space-sharing involves the dual employment of CIM Securities personnel, include policies and procedures that clearly identify the duties/functions to be performed for CIM Securities and the supervisory reporting lines • File an amendment to Form BR for approved arrangements
Record	<ul style="list-style-type: none"> • Record of review and considerations that allow or disallow the arrangement • Approval/disapproval of the arrangement • If dual employment is involved, policies and procedures to address duties and supervisory structure • Form BRs filed

Persons not affiliated with CIM Securities are generally not permitted to conduct business or maintain offices on CIM Securities premises. Office-sharing arrangements require the prior approval of Compliance.

11.9 Cybersecurity

Branch offices are required to comply with CIM Securities's requirements to protect customer and Firm information including the following. Refer to the chapter *CYBERSECURITY* and contact Compliance for further information. Branch office cybersecurity practices are subject to branch reviews. Computers and other devices that access or maintain confidential customer or Firm information must:

- be password-protected and use encryption of data where required
- be secured to prevent stealing
- be authorized Firm devices, software and cloud services
- have current required firewall, virus, malware, and other protection software

Branch personnel must immediately notify the branch supervisor of violations of Firm cybersecurity standards or material cybersecurity incidents involving loss of confidentiality, availability, or integrity of customer personally identifiable information or sensitive Firm data. Firm personnel are annually required to attest to their knowledge of and compliance with CIM Securities's cybersecurity policy.

CIM Securities has adopted the following procedures:

- Requiring branches to perform initial and recurring inventories of branch assets and update the firm regarding any changes
- Identifying sensitive customer and firm information and the location(s) where such information is stored
- Ensuring the physical security of branch assets
- Establishing processes by which branches manage and report lost or stolen assets
- Providing secured asset disposal, such as destroying hard drives of computers no longer in use
- Ensuring branch operating systems are properly supported and maintained either by CIM Securities or by vendors

11.9.1 Branch Technical Controls

Risk assessments include technical controls at the branch level, including the following:

- Limiting registered representatives' access to only their own customers' data and related exception reports
- Setting minimum password requirements and multi-factor authentication for access to firm systems and applications by firm employees, registered representatives, vendors, contractors and other insiders
- Prohibiting the sharing of passwords among firm staff

11.10 Office Inspections

[FINRA Rule 3110(c)(1), 3110(c)(2), 3110(c)(3), 3110.13 and 3110.14]

Responsibility	<ul style="list-style-type: none">• Compliance
Resources	<ul style="list-style-type: none">• Various reports/information regarding office activities
Frequency	<ul style="list-style-type: none">• Annual: inspect OSJs and any branch office supervising one or more non-branch locations• Annual: conduct risk-based review to determine inspection cycle of other offices (no less than every 3 years for branch offices)• Annual or more often as required: review compliance with cybersecurity requirements• Annual: prepare inspection schedule• Annual: assign responsibility for conducting inspections• Per inspection schedule: conduct inspections
Action	<ul style="list-style-type: none">• Conduct risk-based review to determine inspection cycle for non-supervisory offices• Prepare schedule including an explanation of the factors used in determining inspection cycles for non-supervisory offices• Assign inspection responsibility considering any potential conflicts of interest including economic, commercial, or financial interests in the associated persons or business being inspected and ensuring the person assigned is not assigned to the business unit and is not directly or indirectly supervised by, or otherwise reporting to, an associated person assigned to the unit or location. Where compliance is not possible due to CIM Securities's size or business model (only one office; business model where small or single-person offices report directly to an OSJ-manager who is also considered the office's branch office manager), document in the report both the factors used to make this determination and how the inspection otherwise complies with the requirements of Rule 3110(c)(1)• Review compliance with cybersecurity standards which may include:<ul style="list-style-type: none">○ Confirming branch examiners have sufficient cybersecurity expertise to perform reviews○ Developing a framework to capture cybersecurity risks, risk levels and related controls at each branch○ Implementing periodic exam visits or risk-based audits depending on branch risk profile

	<ul style="list-style-type: none"> ○ Implementing automated ways to verify and monitor branch controls, such as verifying patching, virus and malware protection, encryption and password protection ○ Confirming branch meets Firm cybersecurity standards and use Firm-recommended vendors or other vendors meeting Firm standards ○ Re-evaluating branches where reviews identified material deficiencies or reported material cybersecurity incidents to ensure the branch has implemented corrective action • Conduct inspections • Prepare draft and final reports and provide final report to office supervisor and senior management • Obtain response from office supervisor and follow up regarding corrective action (no later than next inspection) • For an office with significant risk profile changes or regulatory/complaint issues, review the need for an immediate "for cause" inspection or acceleration of the inspection cycle • Maintain inspection program (and revise, as needed)
Record	<ul style="list-style-type: none"> • The inspection program, schedule of inspections, reports, review of those conducting inspections, reports • Determinations of whether a branch's inspection cycle should be accelerated or a "for cause" inspection should be conducted

All OSJs, branch offices, and non-branch offices are inspected in accordance with FINRA Rule 3110(c). "Non-supervisory office" in this section refers to branch offices that do not supervise other offices and non-branch offices.

11.10.1 Risk-Based Inspection Cycle

CIM Securities will inspect non-supervisory offices based on a risk-based inspection cycle. The frequency of inspections will be determined by Compliance.

11.10.1.1 "For Cause" Inspections

At any time, a branch office may be identified for an immediate "for cause" inspection, as determined by Compliance. A "for cause" inspection may be initiated considering serious regulatory or disciplinary actions against branch personnel; serious or a pattern of complaints; thefts; fraud; suspected money laundering activities; or other malfeasance by branch personnel.

11.10.1.2 Change Of Risk Profile For Offices Inspected Less Frequently Than Annually

Compliance will consider whether a significant change to an office's risk profile triggers a review of the inspection schedule for that branch. Events that may trigger this review include:

- A branch RR comes under SRO/state/Firm heightened supervision requirements.
- A branch that previously did not supervise other offices now supervises another office (requiring annual inspection).
- A branch or branch employee becomes the subject of a pattern of complaints.
- A branch's level of errors or changes in accounts on orders becomes high compared to other branches.
- Branch personnel become the subject of regulatory action.
- The branch is assigned a new branch manager.
- An existing or newly-hired RR becomes or is subject to a statutory disqualification.

11.10.2 Conducting Inspections

[FINRA Rule 3110(c)(3)(B) and 3110.14]

Inspections generally include the following:

- Assignment of inspection responsibilities to a qualified person
- Pre-inspection document/information review including review of prior report(s) for the office
- Scheduling a visit on either an announced or unannounced basis
- For branch offices, scheduling reviews at the supervising office to examine records of supervision
- During a physical inspection, reviewing records and interviewing personnel in accordance with the inspection program
- Preparing a draft report of findings
- Submitting the draft to the appropriate supervisor for comment and response
- Preparing a final report incorporating the supervisor's responses
- Submission of the final report to management

Compliance, at its discretion, initiates unscheduled inspections (when potential significant problems are identified, a change in office management warrants a special review, at the request of senior management, *etc.*).

11.10.3 Temporary Relief For Remote Inspections

[FINRA Rule 3110.17; MSRB Rule G-27.01; MSRB Notice 2020-18]

CIM Securities may conduct office inspections remotely as announced by FINRA as part of COVID relief.

11.10.4 Reports

[FINRA Rule 3110(c)(2)]

Written reports of inspections will include:

- the name of the person who conducted the inspection and prepared the report
- the date(s) of the inspection
- areas reviewed which will include, at minimum (depending on types of business conducted in the office)
 - safeguarding customer funds and securities;
 - maintaining books and records;
 - supervision of supervisory personnel;
 - transmittals of funds (*e.g.*, wires or checks, *etc.*) or securities from customers to third party accounts; from customer accounts to outside entities (*e.g.*, banks, investment companies, *etc.*); from customer accounts to locations other than a customer's primary residence (*e.g.*, post office

- box, "in care of" accounts, alternate address, *etc.*); and between customers and registered representatives, including the hand-delivery of checks; and
 - changes of customer account information, including address and investment objectives changes and validation of such changes.
- for any of the above areas **not** included in the report, an explanation of why they were not included (*i.e.*, the office does not accept funds or securities, the office does not have a producing manager, *etc.*) and a statement that the office may not engage in these activities until policies and procedures for these activities are in place at that location
- observations and exceptions regarding compliance with policies and procedures
- the office supervisor's response regarding exceptions and corrective action

Final reports will be distributed to senior management and the audit committee, if a committee has been appointed.

11.11 Display Of Certificates

[SIPC By-Laws Article 10 Section 3]

Branch offices are required to display certificates on their premises, including:

- Firm Name, (Member FINRA and SIPC)
- SIPC signage

11.12 Availability Of Rules

Each office that deals with public customers will maintain copies of rules for regulators where CIM Securities is a member. Where Internet access is available, this requirement is satisfied by providing access to the rules published on the regulators' web sites.

12 INVESTMENT BANKING

12.1 Introduction

These policies and procedures outline requirements for CIM Securities's Investment Banking ("IB") activities. Questions regarding the policies and procedures outlined in this chapter should be directed to Compliance.

12.2 Information Barrier and Confidentiality Issues

12.2.1 Information Barrier Procedures

In order to control the flow of confidential and material, non-public information, CIM Securities has created Information Barriers to separate the public side employees (e.g., sales, trading and research) from private side employees (e.g., advisory and investment banking).

For more detailed information regarding CIM Securities's Insider Trading and Information Barriers policies, and the Watch and Restricted Lists policies, refer to the chapter *INSIDER TRADING*.

12.2.2 Origination Meeting Process And Information Sharing

This meeting provides a venue for IB and origination personnel to meet and discuss significant firm opportunities. To that end, open dialogue and communication is crucial, however Compliance guidelines must accompany this open forum in order to address: potential conflict situations; the flow of material, non-public information ("MNPI"); and compliance with CIM Securities's information barrier policy of sharing information only with those that have a "need to know." Separate requirements apply to dealings between IB and Research, outlined in a later section of this Policy titled *"Interaction between Research and Investment Banking."* The following compliance guidelines address information sharing issues other than interaction with Research personnel.

1. As conversations in this meeting will cross industry and product lines, participants will be privy to information that they previously have not been privy to. Senior Origination participants will be held to the same higher standard as Senior Management and above-the-barrier employees.

Participants should always use good judgment when discussing potential transactions or situations and should limit the content and context of the information they present. In the event that MNPI is shared during the meeting, the information should be limited only to essential information (*i.e.*, "need to know").

2. Unlike other forums, project code names are not required. However, if information does not need to be shared or if assistance can be gained by having conversations with colleagues in a separate, smaller venue, this route should be taken.

3. Identifying and discussing common relationships and communication strategies are permissible.

4. Participants should not hand out any materials at the meeting, except for senior management and board of director lists. To the extent that contact lists are handed out or emails are distributed, the documents should:

- have a cover sheet (as applicable),
- be clearly marked Confidential,

- use a project code name in the header or reference field (for emails), and
- be collected and shredded at the end of the meeting by the person handing the material out.

5. At a minimum the use of project code names and limited details should be used as soon as possible, e.g., after the idea comes together and the deal team proceeds with the pitch. Generally, the group should not be updated until the transaction is announced or dead.

6. All MNPI must remain confidential outside the meeting and should be used only for the business purpose it was communicated. Sharing information outside the group should be limited to those with a *"need to know."*

7. When communicating MNPI outside of the group meeting, individuals should utilize project code names in written and in oral communications when appropriate, i.e., public places, meetings outside the group, e-mail, and broadly disseminated correspondence.

8. Participants should only give their proxy information to other Senior Origination participants in the event they are unable to attend. Participants may not ask members of their industry or origination group to attend as their proxy. Given the above-the-barrier nature of the conversation, it is inappropriate for anyone other than the designated participants to attend the meeting.

12.3 Restricted And Watch Lists

IB Supervisor/Compliance maintains and monitors a "Restricted List" and a "Watch List" as described in *INSIDER TRADING*. Investment Bankers have an obligation to notify Compliance of pending deals as outlined in the policy.

12.3.1 Watch List

The Watch List is a confidential list of companies and issuers of securities maintained by Compliance for the purpose of monitoring the possession of confidential or material, non-public information obtained by CIM Securities during its normal course of business, usually when it has been retained to advise a customer regarding a transaction, to underwrite an offering, or to provide debt financing. The contents of the Watch List are highly confidential and access to the Watch List is limited to Compliance and persons granted access by Compliance. No person may discuss the contents of the Watch List or any of its information with anyone outside of the immediate deal team and senior management in the respective business unit, where appropriate, without permission of Compliance.

The Watch List is used to review the sales, trading and research activities of CIM Securities and the personal trading activities of employees without restricting such activities. The Watch List helps to ensure the integrity of the Information Barrier and is used to support and monitor compliance of these policies and procedures. For these reasons, Compliance is authorized to break trades in proprietary or employee accounts, restrict trading and research, and prohibit other activities relating to securities or issuers included on the Watch List.

12.3.1.1 Additions To The Watch List

Notification

The IB Supervisor is responsible for PROMPTLY informing Compliance when CIM Securities is reasonably likely to be engaged by a customer or they obtain information that is substantially material to the customer and/or CIM Securities. Examples include:

- M&A advisory or fairness opinion

- Underwriting or placement agent activities
- Acquisition finance involving public companies
- Conflict clearance when both the acquirer and target are customers
- Auctions
- Hostile situations

Investment Banking Commitment Committee – Not applicable at Present

The Lead Banker is responsible for notifying Compliance prior to going to the Investment Banking Commitment Committee when CIM Securities is reasonably likely to be buy-side or sell-side advisor for a private or a public company, financial or general advisor, advisor in a going-private transaction, to explore strategic alternatives, to place private equity, or to provide a fairness opinion.

IB Supervisor/Compliance will place the name of the issuer(s) involved on the Watch List and conduct a firm-wide review in an attempt to identify, manage and resolve potential conflicts of interest arising from CIM Securities's participation.

12.3.1.2 Updates To The Watch List

The IB Supervisor is responsible for informing Compliance of all material events regarding the transaction. Examples include:

- the approved additions and deletions of employees to and from deal teams
- timing and launching of transactions
- notification prior to a public announcement for an M&A transaction or rendering a fairness opinion
- notification after a shareholder vote is complete or a tender offer expires

12.3.1.3 Deletions From The Watch List

The IB Supervisor who added the security or issuer to the Watch List is responsible for PROMPTLY informing Compliance when a security or issuer should be removed from the Watch List. Generally, the removal of a security or issuer from the Watch List is warranted when the information possessed by CIM Securities is no longer deemed confidential, material or non-public in nature or when it has aged to the point where it is no longer relevant. Removal of a security or issuer from the Watch List is also warranted when the project has been abandoned or when the probability of a project occurring is no longer great enough to continue to monitor the sales, trading and research activities of CIM Securities and the activities of employee accounts.

12.3.2 Restricted List

In order to comply with securities laws, to avoid the appearance of impropriety, and to supplement the Information Barrier, CIM Securities maintains a Restricted List. The Restricted List is an internal-use-only list of companies and issuers of securities in which certain restrictions apply in handling customer orders, trading for proprietary accounts, trading for employee and employee-related accounts, and other activities.

The Restricted List is generated, maintained and distributed by IB Supervisor or Compliance for the exclusive use of CIM Securities, and its contents are for internal use only. Distribution or sharing of the list outside CIM Securities is prohibited. It is communicated through CIM Securities's intranet and is located on the Compliance website. The Restricted List identifies the type of restriction applicable to the security. Restrictions may include legal restrictions (Reg M, 14e-5, *etc.*) and policy restrictions (no proprietary trades until closing of an M&A

transaction in which CIM Securities is serving as a financial advisor) and are assessed and applied by Compliance as required.

12.3.2.1 Prohibitions And Effects Of The Restricted List

The Restricted List is most often used in the following situations to restrict the appropriate sales, trading and research activities in the applicable securities of an IB customer. IB Supervisor and/or Compliance will determine when one of the following conditions requires addition of a security to the Restricted List.

- When CIM Securities has been retained as a financial advisor in a material public transaction
- When CIM Securities is a participant in a publicly announced offering of securities
- When CIM Securities, in some cases, is a provider of debt financing
- In situations where a research analyst, salesperson, or trader is brought over-the-wall
- Prior to the initiation of Equity research coverage with a rating other than hold/market perform
- Prior to dissemination of an equity research report with a material change
- When appropriate, securities of an issuer that is on the opposite side of a material, public transaction with CIM Securities's customer

The Restricted List generally will not indicate why a particular security or issuer is restricted but will identify what activities are restricted and, conversely, permitted.

12.4 Review Of Investment Banking Business

[FINRA Rule 3110(b)(2)]

Responsibility	<ul style="list-style-type: none">• IB Supervisor
Resources	<ul style="list-style-type: none">• Proposed and pending IB deals
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Review proposed deals working with the Commitment Committee and consulting with outside counsel and others as needed• Oversee assignment of passwords and compliance with confidentiality requirements
Record	<ul style="list-style-type: none">• Deal file including review of deals, assignment of passwords and imposition of other confidentiality requirements

The supervisor of Investment Banking (IB) is responsible for oversight of IB transactions and compliance with Firm policies and securities rules, laws, and regulations. Compliance reviews IB and other transactions for compliance with insider trading and related requirements (see the chapter *SUPERVISORY SYSTEM, PROCEDURES, AND CONTROLS* and the sections *Review Of Transactions*) and *Internal Investigations*. Individual transactions by investment bankers are subject to requirements explained in the next section.

12.5 Investment Banker Personal Investments

[FINRA Rule 3110(b)(2) and 3110(d)(3)]

Responsibility	<ul style="list-style-type: none">• IB Supervisor• Compliance
Resources	<ul style="list-style-type: none">• Requests from Bankers to enter personal transactions
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Check for potential conflicts• Approve or disapprove the request• Compliance: review and monitoring of transactions, initiate an internal investigation if necessary (see section <i>Internal Investigations</i> in the chapter <i>SUPERVISORY SYSTEM, PROCEDURES, AND CONTROLS</i>)
Record	<ul style="list-style-type: none">• Records of transaction requests/approval or disapproval• Compliance records of reviews, internal investigations

Because investment bankers (Bankers) have access to MNPI, they are subject to specific requirements affecting their personal investments to avoid conflicts of interest and rule violations. Failure to comply with this Policy may result in disciplinary actions up to and including termination of employment.

Bankers are prohibited from trading in securities:

- that they cover.
- for one (1) reporting period after a publicly-announced deal is finalized (but under no circumstances for any period where there is knowledge of material, non-public information).
- in industries where the Banker is aligned.
- where the Banker has knowledge of material, non-public information (this includes a prohibition against passing on such information to others).
- when the Banker is part of a deal team (includes others supporting the deal team and having knowledge of the deal). Includes knowledge of current or proposed deals.
- that are securities of an issuer that is a customer of the Banker.
- when aware of a proposed or pending follow-on offering.
- if currently involved in an underwriting or distribution of securities for the issuer.
- if previously involved in an underwriting or distribution of securities for the issuer, less than one reporting period has elapsed since the close of the underwriting.
- if aware of an ongoing relationship with the issuer/customer of the group you are working in.
- if aware of any current or potential transactions for the issuer as a result of access to financial or other systems, write rights (the ability to view or change information) to shared folders or applications or work on specific projects.
- if aware of any pitches or other communications planned with the issuer.

Pre-clearance of Banker Transactions

Bankers are required to pre-clear all personal transactions with their supervisor or his/her designee.

12.6 Licensing And Registration

[FINRA Rule 1200; NASD Regulatory Notice 09-41]

Bankers are required to pass the SIE, Series 79 (Investment Banking Representative), and Series 63 (Uniform State Law) examinations. Registered personnel should be licensed in each state or jurisdiction (via Series 63) in which they will potentially conduct or solicit securities or investment banking business, unless a specific exemption applies as determined by Compliance.

12.7 Gifts And Entertainment

[FINRA Rule 2310(c)(2)(A), 2320(g)(4)(A), 2341(l)(5) and 3220]

All employees are subject to CIM Securities's policies on gifts and entertainment (*GENERAL EMPLOYEE POLICIES* chapter). Additional requirements that apply to Bankers are included in this section.

Deal Closing Events

Closing dinners or similar events recognizing a successful transaction are permissible, but are considered "entertainment" for the purpose of the applicable rules and are subject to CIM Securities's entertainment policy.

Customer Restrictions On Gifts, Gratuities, And Entertainment

Many institutions adopt policies and procedures restricting the receipt of gifts, gratuities and entertaining. Firm personnel should conduct business development activities consistent with such policies and procedures to the extent such policies and procedures are effectively communicated to CIM Securities.

Governmental agencies, municipalities, political subdivisions, federally insured deposit institutions, public utilities and bank holding companies typically have adopted policies and procedures or may be subject to state or federal laws and regulations that govern or limit receipt of gifts, gratuities and entertaining. Employees who cover any such customers or sectors should become familiar with the limitations imposed on the receipt of gifts, gratuities or entertainment by the customers themselves or laws applicable to the customer.

Gifts, Gratuities, And Entertainment Provided By Related People

It is not permissible to use spouses or other family members to evade the limitations of the rules. Any gift giving or entertaining of firm customers by a spouse or other family members of an employee will be subject to the rules' limitations except to the extent (i) it solely relates to business development by the spouse's or other family member's employer, or (ii) it is permissible personal gift giving or entertainment to family members and personal friends as provided above and such gift or entertainment is not directly or indirectly paid for by CIM Securities.

12.8 Participation In Compliance Meetings, Continuing Education, And Internal Audits/Reviews

[FINRA Rule 1250 and 3110(a)(7)]

Bankers are required to attend an annual compliance meeting, as required by FINRA, at which attendance is mandatory. The meeting provides a forum for education and guidance concerning legal or regulatory requirements and CIM Securities's internal policies and procedures. Bankers are also subject to continuing education requirements. Registered personnel must complete Regulatory Element continuing education (required every three years) administered by regulators and Firm Element continuing education (required annually) administered by CIM Securities. Compliance will notify employees when they are subject to the requirements; failure to

complete the requirements within specified deadlines will result in the employee ceasing business activities until continuing education is satisfied.

IB is subject to reviews to detect and deter violations of applicable legal requirements and internal policies and procedures. Reviews typically include an assessment of the supervisory structure and internal policies and procedures. Bankers and supervisors are expected to cooperate and provide requested materials promptly to auditors.

12.9 Inquiries And Investigations

CIM Securities is subject to supervisory oversight by multiple regulators. When a representative of any of these regulatory bodies contacts or requests information from an employee in IB, the employee must immediately contact Compliance. IB personnel should only communicate with regulators after consultation with Compliance and/or Legal.

12.10 Anti-Money Laundering (AML)

[FINRA Rule 3310]

Money laundering is a serious offense. SROs and federal securities and banking regulators have adopted stringent requirements to prevent and identify money laundering. Failure to comply with AML rules and regulations can result in significant charges and disciplinary action against CIM Securities and/or its employees including charges of aiding and abetting money laundering and/or direct violation of AML laws. Any irregular or suspicious activity needs to be communicated to Compliance in a timely manner. Customer actions that should be viewed with caution include (but are not necessarily limited to) the following:

- using accounts to clear large sums of money without an apparent business purpose,
- conducting transactions with no discernible purpose,
- unnecessary use of an intermediary,
- regular payment of large sums, including wire transfers, that cannot be explained in the context of the customer's normal business,
- customers whose identity proves unusually difficult or expensive to verify,
- use of an address that is not the customer's permanent business address (for example, utilization of a home address for business correspondence),
- customers who purposefully avoid needed contact with firm staff.

Each IB employee is responsible for being familiar with and complying with CIM Securities's Anti-Money Laundering policies (see the chapter *ANTI-MONEY LAUNDERING (AML) PROGRAM*).

12.10.1 Overview Of The Customer Identification Program Of The USA PATRIOT Act

CIM Securities has a Customer Identification Program (CIP) as required by AML rules and regulations. CIM Securities is required to obtain certain basic information on any **new customer** (which includes a corporation, LLC, partnership, SPV, etc.) who opens an account or otherwise establishes a formal business relationship with CIM Securities. Financial institutions including broker-dealers, industry-wide, are required to implement the following steps as part of their AML program:

1. Obtain and verify the identification of any new customer,

2. Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to us by any government agency, and
3. Provide notice to the customers that information is being requested about their identity and that the information will be used for verification purposes.

To the extent possible, the verification process has been incorporated into those systems used to open accounts/initiate business relationships, and specific procedures have been developed.

It is the responsibility of the lead or senior banker on a deal team commencing a new business relationship to ensure CIM Securities's compliance with the CIP. The following describes each component of the rule to be complied with as well as a discussion of the mechanism that will accomplish compliance and the steps that may be required of IB personnel.

Step 1: Obtain and verify the identification of any new customer.

Certain information is required in order to verify the identity of any new customer when entering into a business transaction, relationship, or engagement. Bankers should obtain the following information when a deal moves to "Pitched" status:

- Taxpayer ID number, or alternative government issued ID number for non-U.S. entities
- Full legal name
- Physical address (no P.O. Box) of principal place of business, including city, state, zip, country

When IB introduces or is otherwise involved in an engagement with an issuer's transactions originated by CIM Securities, information obtained from the issuer will be the source of information for CIM Securities's verification.

Step 2: Determine whether the person (or related persons to an organization) appears on any lists of known or suspected terrorists or terrorist organizations provided to us by any government agency.

Operations may be contacted to check customers against lists.

IMPORTANT NOTE: If for any reason an account cannot be verified through the CIP or it has a match on a terrorist listing, the account must be closed immediately.

Step 3: Provide notice to the customers that information is being requested about their identity and that the information will be used for verification purposes.

The verbiage below must be provided to any new IB customer.

Important Information About Opening Your New Account And/Or Entering into a Business Relationship with CIM Securities: To help fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify and record information that identifies each person or corporation who opens an account and/or enters into a business relationship.

It is the responsibility of the IB Supervisor and Sales Rep executing an engagement letter on behalf of CIM Securities to ensure the required disclosure is incorporated in the engagement letter or other similar engagement documents executed with issuers and borrowers.

12.11 Communications

IB personnel are subject to CIM Securities's communications policies (see the chapter *COMMUNICATIONS WITH THE PUBLIC*). Only firm-sponsored communications networks and computers may be used for public communications. CIM Securities is required to review and retain electronic communications. Electronic communications of any type should be considered the equivalent of written communications for purposes of creating a record of communications and should not be considered "conversations" or phone calls.

The following are included in the definition of communications with the public.

- Press Releases
- Single and Multiple Tombstone Advertisements
- Underwriting proposals to issuers
- Pitchbooks, marketing materials
- Research reports
- Recommendations List
- Offering sheets, fact sheets, or prospectus summaries
- Seminar texts
- Any material designed to be published in the public media
- Electronic communications such as e-mail and Bloomberg
- Communications via electronic networks such as instant messaging
- Facsimile ("Fax")

Communications that refer to CIM Securities as a legal entity (in contracts, *etc.*), must state the full legal name of CIM Securities and CIM Securities's capacity in relation to the product or service offered. Any brand name may be used for marketing purposes, but may not be used in place of the legal entity. If a firm affiliate is mentioned, the relationship between CIM Securities and its affiliate must be clear. If an individual is named in a communication containing the names of CIM Securities and an affiliate, the nature of the relationship of the individual with CIM Securities should be clear.

12.11.1 Prohibited Communications Between Bankers And Customers

Except for Emerging Growth Companies ("EGCs") as discussed in a following section, prior to the effective date of a registered offering, communications mentioning the offering are prohibited including press releases, advertisements, and written communications. There should be **no** written communications (including email or fax) between Bankers and customers during the offering period. Private placements, by their nature, may not be announced prior to the transaction via press releases, advertisements and other media with broad distribution.

"Internal Use Only" material should not be disseminated externally and should be marked "Confidential" to prevent copying or forwarding.

12.11.2 Communication With Other Business Units

This section is intended only to provide general guidelines regarding appropriate levels of communication between IB and other firm business units (other than Research which is discussed in the next section). **If there is any question related to whether or not something can be discussed or shared with other business units, contact Compliance.**

In the event that an employee believes that he or she may have inadvertently signaled that a confidential commitment or project is underway, or may have communicated confidential information about a project to a

person not entitled to such information, the employee should immediately contact the senior business person on the transaction, who should then contact Compliance to determine what, if any, actions are advisable or necessary as a consequence of these communications.

12.11.3 "Public Side" Employees (Sales and Trading, etc.)

In the ordinary course of business, IB will possess non-public and potentially material information regarding corporations whose securities are traded by the public side of CIM Securities, specifically Trading and Sales. It is the responsibility of Bankers to prevent such information from being shared with the public side of CIM Securities. However, there exists a great deal of information received by IB that is public and of interest to employees on the public side of CIM Securities. To facilitate the sharing of such information the following list of items is pre-approved by Compliance for distribution to the public side of CIM Securities and is considered public information:

- Annual Reports, Press Releases, or other company prepared material which is made available to the public;
- Publicly registered documents, 10Ks, 10Qs, and Credit Agreements filed with the SEC;
- Information from publicly available industry media sources; and
- Publicly distributed research published by other institutions.

Written information **not pre-approved** in the above categories must be reviewed by Compliance before being distributed to the public side of CIM Securities.

12.11.4 Interactions Between Research Analysts And Investment Bankers – Not Applicable at Present (Sections 12.11.4 – 12.11.4.3.2)

[FINRA Rule 2241]

Communications and interaction between IB and Research are subject to restrictions by regulatory rules. No Research Analyst may be subject to the supervision or control of any member of CIM Securities's IB groups. IB will have **no** input into company-specific coverage decisions made by the Research Department (*i.e.*, whether or not to initiate or terminate coverage of a particular company).

No Banker may, directly or indirectly, retaliate against or threaten to retaliate against any research analyst employed by CIM Securities or its affiliates as a result of an adverse, negative, or otherwise unfavorable research report or public appearance written or made by the research analyst that may adversely affect CIM Securities's present or prospective IB relationship with the subject company of a research report.

There are some Emerging Growth Company exceptions regarding investment banker/research analyst interactions which are discussed in a section that follows.

12.11.4.1 Chaperoning

Most permissible communications between IB and Research require "chaperoning." Chaperoning means that any written or electronic communication between the research analyst and the Banker must be made through Compliance or in a transmission copied to Compliance. Oral communications must be made through Compliance acting as intermediary or in the presence of Compliance; provided that, Bankers may engage in un-chaperoned communications with research administrative personnel and research analysts may engage in un-chaperoned communications with IB administrative personnel only to the extent necessary to schedule an oral communication for which chaperoning is required.

12.11.4.2 Joint Due Diligence

Joint due diligence (*i.e.*, confirming the adequacy of disclosure in offering or other disclosure documents for a transaction) by the research analyst in the presence of investment banking department personnel prior to the selection by the issuer of the underwriters for the investment banking services transaction is prohibited.

12.11.4.3 Prohibited Activities

The following are additional prohibited research/investment banking activities.

12.11.4.3.1 No Solicitation Of Investment Banking Business

A research analyst **must not** participate in any efforts to solicit investment or corporate banking business. Accordingly, the analyst **must not** participate in any "pitches" for investment or corporate banking business to prospective customers, or have other communications with companies for the purpose of soliciting investment or corporate banking business.

By the same token, IB personnel must not direct or ask a research analyst to engage in any "pitches" or other communications with companies for the purpose of soliciting investment or corporate banking business. This means that Bankers should **not** ask an analyst to visit a customer or business prospect, or join them on a customer visit or phone call. An analyst may, however, visit or speak with a prospective or current customer as the analyst deems appropriate for purposes of conducting due diligence on a transaction.

Pitch materials may include the fact of coverage and the name of the research analyst if it does not imply favorable coverage. Restrictions on pitches do not apply to Emerging Growth Companies with the prior approval of Compliance.

12.11.4.3.2 No Participation In Deal-Related "Road Shows"

Research analysts **must not** participate in "road shows" related to a public offering or other investment banking transaction. To that end, an analyst may **not** review or comment on "dry run" road show presentations or materials prepared in connection with a road show related to a public offering or other investment banking transaction. By the same token, Bankers must not direct an analyst to engage in marketing or selling efforts to investors with respect to any investment banking transaction.

12.11.5 Emerging Growth Companies (EGCs)

[JOBS Act, Title I; SEC JOBS Act Frequently Asked Questions: <http://www.sec.gov/divisions/corpfin/guidance/cfjobsactfaq-title-i-general.htm>]

The Federal JOBS Act creates a category of issuers known as EGCs that have had total annual gross revenues of less than \$1 billion during its most recently completed fiscal year. An issuer remains an EGC until the earliest of:

1. The last day of the fiscal year during which it had total annual gross revenues of at least \$1 billion;
2. The last day of the fiscal year following the fifth anniversary of the issuer's initial public offering;
3. The date on which it has issued more than \$1 billion in non-convertible debt during the previous three-year period; or
4. The date it becomes a "large accelerated filer."

EGCs receive the following treatment under the Act:

- Confidential filing and review of initial public offerings;
- Permitted publication of research reports at the time of a proposed public offering;
- Permitted broker-dealer public appearances following an IPO and after the expiration of a "lock-up" agreement;
- Limited communications between research analysts and potential investors;
- Limited participation by a research analyst in meetings with management and others regarding securities offerings; and
- Permitted oral and written communications (including offers), both before and after the filing of a Securities Act registration statement, with potential investors that are QIBs or accredited investors.

EGCs also have certain disclosure advantages regarding IPO audited financial statements, less financial information to be filed for IPOs, and fewer disclosures under the Act as well as fewer corporate governance requirements than are imposed on non-EGC issuers.

Compliance must be contacted for review of the potential EGC prior to engaging in activities permissible for EGCs but not permissible for other issuers and prior to involvement with research analysts (if applicable). Compliance will notify the banker and appropriate supervisors whether the issuer meets EGC status and whether any restrictions apply.

12.12 Prohibition Against Offering Favorable Research To Induce Investment Banking Business – NOT APPLICABLE AT PRESENT

[FINRA Rule 2241(b)(2)(K) and 2242.01; FINRA Regulatory Notice 11-41]

CIM Securities may not agree to provide favorable research to an issuer to obtain the issuer's investment banking business. Pitch materials may not include information about CIM Securities's research in a manner that suggests, directly or indirectly, that CIM Securities may provide favorable research coverage. FINRA has indicated that the publication in a pitch book or related materials of an analyst's industry ranking will imply the potential outcome of future research because of the manner in which such rankings are compiled. CIM Securities is permitted to include in pitch materials the fact of coverage and the name of the research analyst. Pitch materials and responses to requests for proposals (RFPs) will include disclaimer language that CIM Securities is not, and is unable to, make any promises about research coverage. An example of an inducement would be a CEO of an issuer to requiring candidates for the company's next offering to demonstrate their ability and willingness to follow the company and articulate why investors should own their stock.

If an issuer expresses its expectation, directly or implicitly, that the awarding of investment banking business is conditioned on CIM Securities providing favorable research, the following steps must be taken:

- Notify the IB supervisor or Compliance of the issuer's communication;
- Expressly repudiate to the issuer any expectation with respect to the content of research coverage and document the repudiation;
- Heightened supervision will be implemented regarding solicitation activities, including pitch meetings and materials and other communications with the issuer; and
- Increased oversight of the preparation and content of research on the subject company.

12.13 New Issues

[FINRA Rule 5131(b)]

Firms are prohibited from engaging in "spinning" which is a prohibited practice. Following is the policy regarding spinning as it appears in the chapter *CORPORATE SECURITIES UNDERWRITING*. The IB Manager is responsible for ensuring IB personnel do not participate in allocation of new issues or attempt to influence employees responsible for allocations.

FINRA rule prohibits firms from allocating shares to obtain the investment banking business of a customer. CIM Securities and its employees are prohibited from allocating shares of a new issue to any account where an executive officer or director of a public company or a covered non-public company, or a person materially supported by such executive officer or director, has a beneficial interest:

- If the company is currently an investment banking services customer of CIM Securities or the firm has received compensation from the company for investment banking services in the past 12 months;
- If the person responsible for making the allocation decision knows or has reason to know that CIM Securities intends to provide, or expects to be retained by the company for, investment banking services within the next 3 months; or
- On the express or implied condition that such executive officer or director, on behalf of the company, will retain CIM Securities for the performance of future investment banking services.

These prohibitions do not apply to allocations to any account exempt under FINRA Rule 5130(c) listed in the section *Restrictions On Purchase And Sale of IPOs Of Equity Securities - Exemptions* in the chapter *CORPORATE SECURITIES Underwriting* **with the exception** of the de minimis exemption if beneficial interest does not exceed 10%. The spinning exception applies to persons materially supported by them in aggregate do not exceed **25%** of such account.

In addition, spinning prohibitions do not apply to allocations of securities that are directed in writing by the issuer, its affiliates, or selling shareholders, so long as CIM Securities has no involvement or influence, directly or indirectly, in the allocation decisions of the issuer, its affiliates, or selling shareholders with respect to such issuer-directed securities. [FINRA 5131.01]

The New Issue Certification includes inquiry whether the potential purchaser is an executive officer or director or person materially supported by them.

12.14 New Product Approval Process

New products must be presented to the IB Supervisor and/or Compliance for review and approval prior to offering the new product. A new product or activity can be identified as one that:

- Requires a change or new system or procedure because existing systems or procedures cannot process it;
- Necessitates a new pricing or risk measurement methodology;
- Has unique regulatory, legal, reputation or credit risk characteristics.

Marketing, sales and/or trading activities in the new product may not be commenced until the IB Supervisor and/or Compliance has given its approval. Refer to the section *New Products* in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*.

12.15 Pitch Materials

[FINRA Regulatory Notice 11-41 and 07-04]

12.15.1 Definition

"Pitch materials" are defined as any written (electronic or hard-copy) communication prepared in whole or in part by origination professionals that is delivered to the "public" (*i.e.*, customers) for the solicitation of business. This includes "short form" and "follow-up" materials prepared by origination professionals that are sent to customers via hard copy and/or email.

12.15.2 Approval Of Pitch Materials

Pitch materials require the supervisor's approval **prior to use**.

12.15.3 Other Disclosures And Guidelines

- Sources for all charts, graphs, *etc.* are cited (*i.e.*, Bloomberg, FactSet, *etc.*).
- Information is factual and correct to the best of the preparer's ability.
- Presentation is fair and balanced.
- If research or analyst commentary is included in the pitch material, it must be approved by the Equity Research supervisor and **MAY NOT** include firm research. Quotes must be complete and not out of context, and sources must be cited.
- Pitch materials and response to requests for proposals (RFPs) will include disclaimer language that CIM Securities is not, and is unable to, make promises about research coverage.
- Testimonials from customers regarding the quality of CIM Securities's advisory/execution capabilities must adhere to the following:
 - Inclusion of the following: *"This testimonial may not be representative of the experience of other customers and is not indicative of future performance or success."*
 - If an amount is paid for the testimonial, the fact that it is a paid testimonial must be included.
 - If the testimonial concerns a technical aspect, the person providing the testimonial must have the experience/knowledge necessary to form a valid opinion.
 - **NOTE: This provision does not pertain to case studies listing only the names and contact numbers of customers as references.**
- Offers of Free Service. Reports, analyses or other services offered as "free" must be furnished entirely free and without condition or obligation.

12.15.4 Pitch Materials: Non-Permissible Items

Pitch Materials may **not** include the following:

- Any item not adhering to the guidelines listed above.
- Pitch materials may not include information about CIM Securities's research in a manner that suggests, directly or indirectly, that CIM Securities may provide favorable research, if applicable. Also see the section *Prohibition Against Offering Favorable Research To Induce Investment Banking Business* in this chapter.

- Claims and Opinions - Specifically defined as: "Promises of specific results, exaggerated or unwarranted claims, misleading statements, unwarranted superlatives, opinions for which there is no reasonable basis or forecasts of future events that are unwarranted or that are not clearly labeled as forecasts."
- Hedge Clauses - Specifically defined as: "Cautionary statements or caveats that are misleading or inconsistent with the content of the material."
- "Internal Use Only" Material - not permitted in full or in part.

If applicable to the Firm's business lines, research analysts may not participate in pitches, assist with the preparation of specific pitch materials, or review pitch materials prior to use.

Any questions regarding whether pitch material content can be considered as "approved" or as "non-permissible" should be brought to the attention of the appropriate supervisor and Compliance, **prior to the pitch material's use.**

12.15.5 Document Retention

Pitch materials must be retained for three years. Retained materials must include who prepared the material; other business units/individuals who contributed to the materials; and who approved the material, and when.

12.16 Commitment Committee

If applicable, the Commitment Committee's primary responsibility is to review and approve underwritings (currently handled by the IB Supervisor) of all private or public offerings of taxable and tax-exempt securities in which CIM Securities is the lead or co-manager.

The requirements for presenting proposed issues to the Commitment Committee, if applicable, or IB Supervisor apply to both negotiated and competitive underwritings.

The banker rep must submit each advisory assignment, fixed income, equity, and equity-linked products deals to be undertaken by the Firm to the Commitment Committee, if applicable, or IB Supervisor for approval prior to entering into any engagement. The Committee proposal must include:

- Summary of issuer's background and business
- Summary of issuer's historical financials
- Summary of the structure of the issue
- Key credit strengths and weaknesses
- Size and name of issue
- Name of the investment banker submitting the deal
- Any conditions attached to the issue

The Committee, if applicable, or IB Supervisor will notify the banker rep of its action, whether approved, disapproved, or a request for more information.

12.17 Commitments

When an investment banking customer has agreed to have CIM Securities represent it in an investment banking transaction, a signed agreement detailing the terms and conditions of the commitment will be obtained and signed by all parties. Copies will be provided to the customer and retained by CIM Securities in the deal file.

12.17.1 Representing Two Sides Of A Banking Transaction

In general, CIM Securities will not represent both sides of an investment banking transaction. In those cases where this may be appropriate, the following is required:

1. The proposed dual engagements must be submitted to and approved by the Commitment Committee, if applicable, or IB Supervisor.
2. The proposed dual engagements must be reviewed and approved by in-house or outside counsel as well as the designated supervisor prior to engagement.
3. Each side must be represented by separate investment banking teams separated physically and separated in their electronic and other communications. Each team will be notified in writing and acknowledge in writing that their activities are separate from the other team, and their activities are confidential and may not be communicated to the other team.
4. The written agreement with the customer must include clear disclosure that CIM Securities is representing both sides of the transaction, and the customer must separately acknowledge in writing their understanding and acceptance of this arrangement.

The IB supervisor is responsible for ensuring that these requirements are satisfied and for retaining records documenting them.

12.18 Fairness Opinions

[FINRA Rule 5150]

Responsibility	<ul style="list-style-type: none">• IB supervisor• Review committee, if applicable
Resources	<ul style="list-style-type: none">• Fairness opinion• Fairness Opinion Review/Approval forms
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• Manager:<ul style="list-style-type: none">○ Review and approve opinion and forward to committee○ Confirm that required changes are made to the opinion• Committee: Review and approve opinion or refer back to manager for changes
Record	<ul style="list-style-type: none">• Fairness opinions• Fairness Opinion Review/Approval forms

FINRA Rule 5150 outlines requirements when CIM Securities issues a fairness opinion. The rule requires that investors-shareholders be informed about potential conflicts of interest between CIM Securities and the issuer and addresses specific procedures when issuing fairness opinions. This includes fairness opinions issued to the board of directors and/or any special committee or subset or committee of the board.

Specific requirements are explained below. In summary:

- Required disclosures must be included in the fairness opinion.

- The Fairness Opinion Review/Approval form must be completed.
- The IB supervisor must approve the opinion and forward it, with the form, to the review committee.
- The review committee will review the opinion and notify the manager of approval or required changes.
- Revised opinions must be re-submitted to the committee for review and approval.

12.18.1 Disclosures

Disclosures include "significant" payment or compensation. FINRA does not assign a quantitative number to "significant" but defines it as a payment or compensation that a reasonable person who reads a fairness opinion would have an interest in knowing in order to assess whether CIM Securities has a potential conflict of interest. The receipt of *de minimis* fees (such as trading fees or other small incremental fees from account assets or activity) are not required to be disclosed. Disclosures may be descriptive rather than quantitative.

The fairness opinion must disclose if CIM Securities:

- has acted as financial advisor to any party to the transaction that is the subject of the fairness opinion.
- will receive compensation, contingent on the successful completion of the transaction, for issuing the fairness opinion and/or serving as advisor. *[Includes significant payments or compensation from related transactions (e.g., stapled financings) if such transactions are contingent upon the completion of the transaction for which the fairness opinion was issued.]*
- will receive any other significant payment or compensation contingent upon the successful completion of the transaction.
- has had any material relationships that existed during the past two years or that are mutually understood to be contemplated in which any compensation was received or is intended to be received as a result of the relationship between CIM Securities and any party to the transaction that is the subject of the fairness opinion. *[Includes material relationships between CIM Securities and all parties to the transaction, not just the party requesting the fairness opinion. A fairness opinion issued to a target's board of directors would have to include disclosure of any relationship with the acquirer.]*
- has independently verified information provided by the company requesting the opinion where that information is used for a substantial basis of the fairness opinion. *[If verified, must include a description of the information or categories of information verified and the process or standards for independent verification. Where no information provided by the company is verified, include a blanket statement that no independent verification took place.]*
- has approved the fairness opinion through a fairness committee or whether approval is required. *["Fairness committee" is deemed by FINRA to include any committee or group that approves a fairness opinion in accordance with Rule 5150(b).]*
- expresses an opinion about the fairness of the amount or nature of the compensation to any of the company's officers, directors or employees, or class of such persons, relative to the compensation to the public shareholders of the company. *[Disclosure is required as to whether or not such an opinion is expressed.]*

12.18.2 Approval

Fairness opinions must be approved prior to issuance.

- Opinions will be approved by a committee comprised of three or more individuals including representation from non-investment banking areas such as Compliance, Operations, or Sales, and representation from Investment Banking personnel who are not involved on the deal team to the transaction. At least two

persons must be from non-investment banking departments. All committee members must be sufficiently experienced or knowledgeable in investment banking matters to render approval.

- The deal team must present the complete fairness opinion, including required disclosures and an explanation of valuation analyses used in the fairness opinion. The IB supervisor is responsible for confirming that all required disclosures are included.
- The committee is responsible for reviewing the opinion (including a determination of whether the valuation analyses used in the opinion are appropriate) and approving or disapproving the opinion. The approval or disapproval and comments regarding necessary changes or other comments will be forwarded to the IB Supervisor.
- The IB Supervisor is responsible for confirming that changes are made consistent with the instructions of the committee. If the fairness opinion is revised, it must be re-submitted to the committee for review.
- The IB Supervisor/Compliance will retain records of who is serving on the committee, its reviews, and its actions.

12.19 Origination, Record Retention, Closed Deal Files

12.19.1 Due Diligence

The Securities Act of 1933 can impose substantial civil liability on various parties, including the issuer, the underwriters, and the accountants involved in the preparation of a registration statement or offering document. In particular, these participants are subject to potential liability if any part of the effective registration statement contains an untrue statement of material fact or omits to state a material fact. Moreover, failure to conduct proper due diligence can result in the revocation by the SEC of a broker-dealer's registration.

An underwriter may avoid liability if it can affirmatively demonstrate that it, after a reasonable investigation or "due diligence," had grounds to believe and did believe that the registration statement or offering document did not contain a material misstatement or omission.

12.19.2 Investment Banking's Responsibility

Although the product origination groups have the primary due diligence responsibility, Bankers should work closely with their product origination partners to help ensure a thorough due diligence review has been conducted and documented. Contact Compliance or Legal with any questions.

12.19.3 Required Document Retention

Because an underwriter has the burden of proving its due diligence defense under the securities laws, it is essential that the investigation conducted by CIM Securities be documented. One central "deal file" should be maintained and controlled by the IB Supervisor. All other files shall be either merged into the central file or destroyed once the offering has been completed.

The central closed deal file should contain only clean, final copies of deal documents which may include, but not be limited to:

- Final closing documents (any preliminary drafts and all copies with other extraneous records such as handwritten notes should be discarded)
- Investment Committee deal package (where applicable)

- Rating Agency Presentation (where applicable)
- Computational materials provided to investors (where applicable)
- Due diligence questionnaire
- Regulatory filings
- Pitchbooks or other marketing materials
- Other pertinent correspondence

All documentation related to a securities underwriting must be maintained for a period of three years; two years in an easily accessible place.

12.19.4 M&A Closed Deal Files – Not applicable at Present

To comply with federal securities regulations, an M&A Closing File Checklist is designed to assist in collecting and retaining important documents relating to the engagement of CIM Securities as financial advisor to customers in connection with M&A transactions.

This list of documents is not intended to be exhaustive. Given storage space constraints, CIM Securities wishes to keep **final** copies of the **formal** documentation that is necessary to reflect CIM Securities's relationship with the party or parties to the engagement and our work product. CIM Securities does not want to retain copies of documents that are readily available from other sources, are merely drafts or contain information that is available in other documents that are being retained. Space constraints and the increasing lists involved in the retention of large transaction files make it desirable to retain only those items reflected on the list below or deemed by the deal team leader to be an important record that is in keeping with firm policies.

Promptly upon closing of a transaction or after the expiration or termination of CIM Securities's engagement, an associate on the deal team, with the guidance of the deal team leader, will compile the documents listed below, as applicable. Upon compilation of the file, the supervisor who supervises the deal team will review the file and include in the file a signed statement signifying that the file is ready for storage. The file will consist of paper documents. Copies of the file may also be kept in "pdf" format in addition to, but not in lieu of, paper documents. Any other electronic copies of documents should be deleted or redacted to remove transaction-specific or confidential information and should be stored in the forms library.

These files will be maintained in a readily accessible central location for a period of three years, with the most recent two years readily accessible.

Compliance and the appropriate supervisor will periodically review these files to ensure that all (and only) appropriate documents are being properly maintained, and that the supervisor has reviewed the files.

Materials required to be maintained (if applicable):

1. **Commitment Committee Materials.**
 - Memorandum.
 - Engagement letter.
2. **Fairness Opinion Materials** (presentation materials vs. engagement letters, contracts or other exhibits).
3. **All board presentations during the engagement (only final).**
4. **Contractual Agreements with Customer and other Parties.**
 - Engagement Letters.
 - Confidentiality Agreements.
 - Indemnity Agreements.
 - Right of Refusal Letters.
 - Amendments or Terminations.
 - Approvals of Marketing Materials or Potential Purchasers, *etc.*
5. **SEC Filings** that refer to CIM Securities and include copies or descriptions of our fairness or adequacy opinions.

- Proxy statements, information statements, Schedules 14D-9 and TO.
- 6. **Marketing Materials approved by Customer.**
- 7. **Substantive Letters to SEC or Other Governmental Agencies from CIM Securities or its counsel.**
 - Consents of CIM Securities.
- 8. **Financing Commitments** (related to the transaction, *i.e.*, to either buyer or seller from CIM Securities or its affiliates [if shared with deal team]).
- 9. **Opinion Letters or Formal Advice from outside counsel to CIM Securities.**
- 10. **Working Group Lists.**
- 11. **Other Pertinent Correspondence.**

13 PRIVATE PLACEMENTS AND OFFERINGS

[FINRA Rule 5122 and 5123; FINRA Frequently Asked Questions: <https://www.finra.org/rules-guidance/guidance/faqs/private-placement-frequently-asked-questions-faq>; Securities Act Regulation D Rule 504, Rule 506(b) and Rule 506(c)]

This chapter explains the requirements when offering private placements and engaging in private offerings. Private placements and offerings are subject to strict requirements that are imposed on the issuer and those who sell the issue. The requirements for offering a specific private placement will be announced at the time the private placement becomes available for sale. It is important to understand and comply with the requirements for each offering.

13.1 Introduction

This section provides general information about private placements and the regulations that govern their offer and sale. A general understanding of private placements is helpful when considering whether to offer a specific issue to a customer.

There are several general areas of requirements and limitations that affect most private placements.

- No general solicitation of purchasers other than those permitted under Rule 506(c) and 144A
- Limits as to the size of the offering
- No advertising or general public meetings about specific private placements other than those permitted under Rule 506(c) and 144A
- Issuers must provide information to potential investors
- Securities purchased are generally restricted as to resale
- Number of purchasers is restricted

13.1.1 Private Securities Offerings Principal

Principals solely responsible for supervising specified activities relating to private securities offerings may register as Private Securities Offerings Principals, instead of registering as General Securities Principals. Individuals can qualify for registration as a Private Securities Offerings Principal in several ways.

Individuals registering as Private Securities Offerings Principals are required to satisfy the Private Securities Offerings Representative prerequisite registration which includes passing the SIE and the General Securities Principal (Series 24) qualification examinations.

13.1.2 Definition Of Terms

The following are common terms included in this chapter.

Accredited investor	An investor who meets certain criteria that are indicative of sophistication (see the section <i>Accredited Investors</i>)
Letter of Non-Distributive Intent	A letter or form signed by the purchaser of a private placement, affirming that the investor is purchasing the securities for their own account and are not to be resold unless registered or subject to an available exemption.

Non-Disclosure Agreement	An agreement signed by the offeree stating that proprietary information learned about the issuer will not be divulged to third parties.
Offer	An attempt to sell a security to a potential purchaser
Offeree	A prospective purchaser to whom an offer is made
Purchaser questionnaire	A questionnaire completed by an offeree to establish the offeree's suitability/Reg BI eligibility to purchase the investment
Purchaser representative	A person (not affiliated with the issuer or the broker-dealer selling the issue) who acts on the purchaser's behalf to evaluate the investment for the purchaser
Subscription agreement	The document signed by the purchaser and evaluated by the issuer prior to the purchase

13.1.3 "Private Placement" Defined

Private placements are unregistered, non-public securities offerings that rely on an available exemption from registration with the SEC under either Sections 3 or 4 of the Securities Act. Most private offerings are sold pursuant to one of three "safe harbors" under Rules 504, 506(b), and 506(c) of Regulation D. Private placements sold by FINRA member firms to individuals generally must file offering documents with FINRA.

13.1.3.1 Section 4(2) Of The Securities Act Of 1933

Some private placements are offered under Section 4(2) which provides an exemption for "transactions by an issuer not involving any public offering." While the section does not specifically outline the requirements for establishing an exemption, the following is a summary of requirements gleaned from SEC interpretations and court decisions.

- There may be no general solicitation of purchasers other than those permitted under Rule 506(c) and 144A.
- Offerees and purchasers must have access to information about the issuer and must be able to comprehend and evaluate the information.
- The issuer, broker-dealer, and others acting for the issuer must conduct due diligence to reasonably insure information given to offerees and purchasers is complete and accurate.
- Offerees must have access to meaningful information concerning the issuer and be able to comprehend and evaluate the information.
- Purchasers must acquire the securities for investment and not for resale.

13.2 Blue Sky Requirements

State securities laws ("blue sky" laws) that apply to private placements vary from state to state. Some states have differing definitions for accredited investors; some states require registration of a securities issue that is otherwise exempt under Federal securities laws.

CIM Securities and its sales personnel are required to comply with any blue sky requirements that apply to a specific private placement issue. Requirements may differ depending on where the issue originates and where it is sold.

13.3 The Firm's Participation In Private Placements

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • Information provided by the issuer and/or issuer's counsel
Frequency	<ul style="list-style-type: none"> • As required - process the private placement • Within 15 calendar days of the date of first sale - provide submissions to FINRA
Action	<ul style="list-style-type: none"> • Execute an agreement with the issuer • Conduct due diligence or engage counsel or other qualified person to conduct due diligence • Document the file regarding due diligence • Provide information to CIM Securities's New Product or Underwriting Committee or appropriate senior manager for review and approval to proceed with the deal • Determine limitations on the offering, including integration issues and obtain representation letter from issuer if needed • Determine what information to provide to sales personnel • Authorize the sale of the offering • Within required timeframes, submit private placement memorandum, term sheet or other document (including material amendments) to FINRA or notify FINRA no offering documents were used • Consider conducting a post-closing assessment to ascertain whether offering proceeds were used in a manner consistent with the offering memorandum
Record	<ul style="list-style-type: none"> • The deal file will include due diligence information; approval/disapproval from the appropriate committee or senior manager; the issuer agreement; issuer representation letter; offering materials; authorization to sell; post-closing assessment, if applicable • Record of submissions to FINRA and when submitted

13.3.1 Due Diligence

Due diligence will be conducted for each private placement issue to be offered by CIM Securities and is documented in the file for the private placement. Outside counsel or another third party may be engaged to assist in due diligence and other aspects of the private placement offering. If the counsel or third party is affiliated with or somehow associated with the issuer, CIM Securities will conduct additional independent due diligence. Due diligence may include the following reviews (which may include engaging attorneys or other third parties to conduct some or all reviews), as appropriate for the particular potential offering:

- Financial reports
- Written company assurances as to the accuracy of records and financial statements
- Determination of the issuer's creditworthiness
- Evaluate the validity and integrity of the issuer's business model and how it fits into its business sector
- Review information available from financial and other publishers
- Independent verification of management's representations (contact with issuer's customers; lenders, vendors, lower-level employees, etc.)

- Independent verification of information key to the performance of the offering such as unrealistic costs projected to execute the business plan coupled with aggressively projected timing and overall rate of return for investors
- Identify conflicts of interest such as firm affiliates or issuers whose control persons were also employed by CIM Securities and address conflicts (such as by confirming that the issuer prominently and comprehensively discloses these conflicts in offering documents or mitigating them by removing financial incentives to recommend a private offering or other more appropriate investments)
- Reviewing news articles and industry publications regarding the issuer, its market, and competition
- Review the company's internal documents such as operating plans, product literature, corporate records, financial statements, contracts and lists of distributors and customers
- Physical inspection of the company's facilities
- Contact with the issuer's auditor and other experts knowledgeable about the company
- Contact with outside directors
- Interviews of key personnel or customers
- Determination of the plausibility of expected rates of return as compared to industry benchmarks, particularly considering complex fee structures associated with many of these types of investments
- Identifying red flags such as questionable business plans or unlikely projections or results, and conflicts of interest and following up
- Updating due diligence as needed until effectiveness of the offering

13.3.2 Agreement With The Issuer

CIM Securities will execute an agreement with the issuer to define the terms of CIM Securities's role in the offering and the issuer's obligations as well as other covenants of the offering.

13.3.3 Dollar Amount Of The Offering And Integration Issues

The IB supervisor is responsible for ensuring the issue is not oversold relative to the dollar amount disclosed in the offering document compared to the limitations provided in the rules. The supervisor should consider any "integration" of similar offerings by the same issuer for substantially identical purposes for determining whether the issuer meets the dollar limitation under the exemption within a 12-month period of time. The supervisor's review for integration may include one of the following or another procedure determined adequate by the supervisor:

- Reviewing the issuer's financial statements for the past 12 months and/or contact directly with the issuer
- Obtaining a representation letter from the issuer that states that no other offerings were distributed during the 6-month period prior to the current private placement offering or will be distributed in a succeeding 6-month period that would cause the exemption to be lost

13.3.4 Form D

For issues sold under Regulation D, the issuer is required to make a Form D filing electronically on EDGAR within fifteen days after the first sale of securities in the offering. For ongoing offerings lasting longer than one year, the issuer is required to electronically file an amendment annually.

Some states also require filing of Form D. The issuer (or issuer's counsel) is responsible for Form D filings.

13.3.5 Submissions To FINRA

[FINRA Rule 5123; FINRA Regulatory Notice 13-26 and 12-40]

For private placements sold by CIM Securities (other than those exempt under Rule 5123), filings will be made electronically with FINRA within 15 calendar days of the date of first sale including the private placement memorandum, term sheet or other offering document (including any material amendments). If no offering documents were used, FINRA will be notified.

13.4 Sales Of Private Placements

13.4.1 Regulation Best Interest (BI)

A primary objective when selling a private placement is that all securities placed with retail investors be consistent with Regulation BI. The RR recommending a private placement is responsible for determining that the recommendation is appropriate for the offeree based on information known about the potential offeree. The RR must consider minimum investor requirements and other suitability standards for each private placement offering.

Recommendations to retail customers who are natural persons are subject to Regulation Best Interest (BI). Reg BI includes recommendations for orders; types of accounts; and investment strategies, including recommendations to prospects. It is important to be familiar with those requirements which are included in the chapter *REGULATION BEST INTEREST (BI)*.

13.4.1.1 Accredited Investors

[Securities Act Rule 215; Securities Act Regulation D Rule 501]

An accredited investor is defined in Rule 501 as someone who meets certain financial criteria which may include minimum net worth, minimum income levels and other standards set by federal or state laws and regulations. It also includes natural persons holding professional certifications or designations or other credentials; knowledgeable employees of private funds; rural business investment companies; limited liability companies that meet certain criteria; other entities meeting an investments owned test; family offices and family clients; and spousal equivalents. The Rule should be consulted for specific criteria. Typically, accredited investors are not counted toward the limitation on the number of purchasers of a private placement.

Information about each private placement (and where it is sold) must be consulted to determine who qualifies as an "accredited investor" for a particular issue.

13.4.1.2 Non-Accredited Investors

Private placements sometimes may be offered to purchasers who do not meet the criteria of accredited investors. The number of allowable non-accredited purchasers will be limited, to preserve the registration exemption and meet requirements specified under federal and state law.

13.4.2 Restricted Nature Of Private Placement Securities

Private placement securities are considered "restricted securities," other than those purchased in Rule 504 offerings. Certificates will typically include a legend and securities cannot be resold unless registered or the securities qualify for sale under an exemption.

Purchases must be for investment purposes and not for the purpose of resale. Subscription documents typically include an affirmation that the purchaser is buying the private placement for investment purposes and understands they may not be resold (Letter of Non-Distributive Intent).

RRs must consider the illiquidity of most private placements when making suitability/Reg BI determinations. For example, a private placement would not be a suitable investment for a purchaser who expects to invest his funds on a short-term basis.

13.4.3 Retail Communications

[FINRA Rule 2210; FINRA Regulatory Notice 20-21 and 13-18]

This section includes requirements for retail communications about private placements. FINRA Regulatory Notice 20-21 should be referenced for more detail and guidance.

- Under Rule 2210(d) all communications must be fair, balanced, and not misleading;
- Any promotion of potential awards must be balanced by disclosure of the associated risks;
- Communications must be accurate and provide a sound basis to evaluate the facts with respect to the products or services discussed; and
- Retail communications must be approved by a registered principal.

This also applies to communications prepared by third parties and used by CIM Securities. If a retail communication is included in the same electronic file with an issuer-prepared private placement memorandum and distributed by CIM Securities, it is considered a Firm communication in its entirety subject to FINRA Rule 2210. Retail communications must balance any discussions of benefits with a discussion of related risks and must be in the same retail communication (*i.e.*, cannot be in a separate document or different section of the website).

Retail communications may not contain any prediction or projection of performance, subject to certain exceptions, as well as any exaggerated or unwarranted claim, opinion, or forecast. Reasonable forecasts of issuer operating metrics, along with a sound basis for evaluating the facts and related risks, would be permitted. FINRA Regulatory Notice 20-21 provides more detailed guidance when including forecasts.

Regulatory Notice 13-18 provides guidance for public and non-public REITs including principles relating to distribution rates which refers to issues where a portion of distributions are funded through return of principal or loan proceeds. Refer to the Notice for details of necessary disclosures.

Internal Rate of Return (IRR) is a measure of performance commonly used in connection with marketing private placements of real estate, private equity and venture capital. A drawback of IRR calculations is an inherent assumption that investors will be able to reinvest distributions at the IRR rate, which is unlikely to occur. In addition, calculations may include holdings that have not yet been sold (or liquidated or matured) resulting in subjective factors and assumptions. IRR may not be used in retail communications regarding privately placed new investment programs with no operations or that operate as a blind pool. IRR may be used for completed investment programs (holdings matured or all sold).

13.4.4 Filing Requirements For Private Placement Of Securities

[FINRA Rule 5123(a)]

The IB supervisor is responsible for the following filings with FINRA within fifteen calendar days of the date of first sale or notify FINRA that no such documents were used:

- private placement memorandum
- term sheet or other such document
- any retail communication (defined in FINRA Rule 2210) that promotes or recommends the member private offering
- amendments to the above within 10 days of providing to any investor or prospective investor

Excluded from this requirement are private offerings sold only to institutional investors [defined in FINRA Rule 4512(c)]; qualified purchasers [defined in the Investment Company Act of 1940]; investment companies [defined in the Investment Company Act] and qualified institutional buyers [defined in Rule 144A].

13.4.5 Filing Requirements For Private Placement Of Securities Issued By A Member Firm

[FINRA Rule 5122(b)(2)]

The IB supervisor is responsible for the following filings with FINRA at or prior to the first time the document is provided to any prospective investor:

- private placement memorandum
- term sheet or other such document
- any retail communication (defined in FINRA Rule 2210) that promotes or recommends the member private offering
- amendments to the above within 10 days of providing to any investor or prospective investor

Excluded from this requirement are private offerings sold only to institutional investors [defined in FINRA Rule 4512(c)]; qualified purchasers [defined in the Investment Company Act of 1940]; and qualified institutional buyers [defined in Rule 144A].

13.4.6 Purchaser Questionnaires

Where necessary, the potential investor will be requested to complete a Purchaser Questionnaire which confirms that the investor meets certain minimum requirements to participate in the private offering.

When Purchaser Questionnaires are required, the RR is responsible for obtaining the completed Questionnaire from the potential purchaser and submitting it for review and approval within the timeframe established for the offering.

13.4.7 Purchaser Representatives

If a purchaser is not sufficiently sophisticated to effectively evaluate the investment opportunity, he or she may have a "purchaser representative" (chosen by the investor and **not** an affiliate of the issuer or broker-dealer) who assists in evaluating the investment. The purchaser representative will be required to sign the offering documents attesting to his or her role acting as purchaser representative.

13.4.8 Offering Memorandum

An offering memorandum is prepared for each private placement, depending on the specific issue. The offering memorandum includes disclosures of information obtained from the issuer including the nature, character, and risk factors relating to the offering.

An offering memorandum must be provided to all offerees. Offering memorandums may be numbered or listed on an internal spreadsheet, to enable CIM Securities to maintain a record of offerees who received them.

RRs must provide information regarding the offeree at the time the memorandum is provided to the prospective purchaser.

If it is necessary to update or correct information in the private placement memorandum prior to closing of the issue, the revised information will be provided to offerees, in writing.

13.4.9 Oral Representations

RRs must not deviate from written private placement memorandum information or other pre-approved information when discussing private placements with potential investors. Written notes of conversations with offerees (and their purchaser representatives) should be made, dated and placed in the customer's file.

13.4.10 Offeree Access To Information

Most private placement memoranda state that it was prepared by counsel from information provided by the issuer. Offerees are invited to meet with representatives of the issuer to make an independent investigation and verification of information in the memorandum.

13.4.11 Solicitation

[Securities Act Regulation D Rule 506(b) and Rule 506(c); SEC Compliance & Disclosure Interpretations (C&Ds) on verification methods, see 255.48, 255.49, 260.35, 260.36, 260.37, 260.38: <http://www.sec.gov/divisions/corpfin/guidance/securitiesactrules-interps.htm#255.48>; SEC explanation of 506(b): <https://www.sec.gov/smallbusiness/exemptofferings/rule506b>; SEC explanation of 506(c): <https://www.sec.gov/smallbusiness/exemptofferings/rule506c>; SIFMA Guidance on Rule 506(c) verification: <http://www.sifma.org/issues/item.aspx?id=8589949595>; SEC Compliance and Disclosure Interpretations 256.23-256.33 8/6/15 re solicitations]

Responsibility	<ul style="list-style-type: none">• IB Supervisor
Resources	<ul style="list-style-type: none">• Rule 506 offerings
Frequency	<ul style="list-style-type: none">• As required
Action	<ul style="list-style-type: none">• For offerings under Rule 506(b):<ul style="list-style-type: none">○ Ensure there are no media (including internet) or public event announcements of the offering○ If there is to be solicitation of investors with a pre-existing, substantive relationship, confirm those to be solicited meet SEC guidance○ If other exemptions apply, confirm compliance with requirements• For offerings under Rule 506(c):

	<ul style="list-style-type: none"> ○ Confirm that the issuer has determined that purchasers qualify as accredited investors or conduct verification of purchasers ○ File forms and pay fees as required
Record	<ul style="list-style-type: none"> • Record of confirming accredited investor status of all purchasers • Record of confirming the pre-existing substantive relationship to satisfy Rule 506(b) requirements or other SEC guidance requirements • Records of filing forms/paying fees

Solicitation of private placement offerings under Rules 506(b) and 506(c) differ as explained below.

13.4.11.1 Offerings Under Rule 506(b)

Companies conducting an offering under Rule 506(b) may raise an unlimited amount of money and may sell to an unlimited number of accredited investors. 506(b) offerings are subject to the following:

- no general solicitation or advertising to market the securities
- may not be sold to more than 35 non-accredited investors subject to the following:
 - must provide disclosure documents; if information is provided to accredited investors, the same must be provided to non-accredited investors
 - must provide financial statement information
 - should be available to answer questions from prospective purchasers

Purchasers receive restricted securities. Notice to the SEC on Form D is required within 15 days after the first sale of securities in the offering. Some states may require notice filings and fees.

506(b) offerings are subject to "bad actor" disqualification provisions (see *Disqualification Of Felons And Other "Bad Actors"* in this chapter).

13.4.11.2 Offerings Under Rule 506(c)

Under Rule 506(c) issuers may broadly solicit and generally advertise an offering subject to the following restrictions:

- All purchasers must be accredited investors as defined under Rule 501.
- The issuer is obligated to take reasonable steps to verify that purchasers are accredited investors under Rule 501 of Regulation D. Depending on CIM Securities's role, CIM Securities may be responsible for verification.
- Certain other conditions in Regulation D are satisfied.

Purchasers receive restricted securities. The issuer must file notice to the SEC on Form D within 15 days after the first sale of the securities in the offering. Some states may require notice filings and fees.

The SEC has provided a non-exclusive list of methods that issuers (or someone acting on behalf of the issuer) may use to satisfy the verification requirement for individual investors, including:

- Reviewing copies of any IRS form that reports the income of the purchaser and obtaining a written representation that the purchaser will likely continue to earn the necessary income in the current year.

- Receiving a written confirmation from a registered broker-dealer, SEC-registered investment adviser, licensed attorney, or certified public accountant that such entity or person has taken reasonable steps to verify the purchaser's accredited status.

The verification rule does NOT apply if there is no advertising or general solicitation.

13.4.12 Investment Seminars Or Meetings

Responsibility	<ul style="list-style-type: none"> • IB Supervisor
Resources	<ul style="list-style-type: none"> • Requests to conduct meetings or seminars
Frequency	<ul style="list-style-type: none"> • As required
Action	<ul style="list-style-type: none"> • Request a written outline of the information to be presented, including any written materials to be provided to those attending • Request information about how the seminar or meeting will be publicized • Review the outline, written materials, and method of publication • Approve or disapprove, providing any revisions necessary • Require that all invitees receive copies of the offering memorandum
Record	<ul style="list-style-type: none"> • Include copies of the outline, list of invitees, written materials, and the approver's initials and date of approval/disapproval in the deal file.

Rule 504 offerings may be solicited without limitation. There may be general solicitation for Rule 506 and 144A offerings though the issuer is subject to requirements to verify that purchasers are accredited investors (Rule 506) or QIBs (Rule 144A). See the sections *Solicitations* and *Rule 144A Transactions* for more information.

- Seminars or meetings on specific private placements must be approved by the designated supervisor prior to conducting the seminar or meeting. Prior to approval provide the supervisor with:
 - a written outline of information to be presented and any graphic or written materials to be provided to attendees.
 - a description of how the seminar or meeting will be publicized to prospective attendees.
- Attendees must be provided with an offering memorandum. No other written material may be provided, unless previously approved by CIM Securities.

13.4.13 Subscription Agreements

Each potential purchaser will be required to complete the necessary subscription agreement to purchase a private placement. The agreement must be accompanied by a check, if applicable for the purchase.

Note: CIM does not handle checks. Investors in offerings will deposit funds directly with the issuer as instructed in subscription agreements.

Subscription agreements are processed as follows:

- The RR obtains the signed subscription agreement (and other required offering documents) and a check for payment from the offeree and submits them to the designated supervisor.
- Subscription agreements and checks received are logged into the Sales Blotter for the private placement.

- The designated supervisor reviews the agreement and check for acceptability.
- The check is forwarded to the escrow agent or the issuer, together with the purchaser's name, address, social security number, and number of shares/units, as required.
- Rejected agreements/checks are returned to the RR with an explanation for the rejection.
- Accepted agreements are signed/initialed by the supervisor, a copy retained by CIM Securities, and the original forwarded to the issuer.
- The issuer reviews and accepts or rejects the agreement.
- A confirmation is sent to accepted purchasers when the purchase is effective.

RRs should be aware that **purchasers are not accepted until the issuer accepts them**. Final acceptance rests with the issuer who is responsible for ensuring conditions of the offering are satisfied to qualify under the operative exemption.

13.5 Regulation D

[SEC Securities Act of 1933 Regulation D; FINRA Regulatory Notice 10-22]

Regulation D is a series of six rules, Rules 501-506, that include exemptions from the registration requirements of the 1933 Act. The specific exemptions are included in Rules 504-506 and differ as to the size of the offering and conditions imposed to qualify for the exemption. The following chart summarizes the three exemptions available under Regulation D. This is only a very general summary of requirements and does not include legal definitions and technicalities that may apply to certain types of private placements.

	Rule 504	Rule 506
Who may invest	Anyone suitable for the investment	Qualified investors
Number of investors	Unlimited	35 non-accredited, unlimited accredited investors
Size of offering sold in any consecutive 12 months	\$5,000,000	Unlimited
Restricted securities?	No	Yes
Public solicitation/advertising allowed?	Yes	Yes
Disclosure document required?	No	Yes*
Opportunity to ask questions of issuer?	No	Yes

* Under the rule, disclosure documents are not required to be given to accredited investors though a note to Rule 502(b) states that an issuer should consider providing such information to accredited investors in view of anti-fraud statutes.

The reference to "unlimited accredited investors" in the section "Number of investors" above does not imply that a private placement will, in fact, have an unlimited number of accredited investors. The issuer and CIM Securities will consider limitations on accredited investors, as appropriate, to preserve the exemption as a private placement and avoid the appearance of a broad solicitation of the issue.

13.5.1 Disqualification Of Felons And Other "Bad Actors"

[SEC Regulation D Rule 506(d)(1)]

Rules 504 and 506 are frequently-used exemptions from registration under Regulation D. The exemptions are NOT available if the issuer or any person covered by the disqualification rule had a "disqualifying event." Disqualifying events include certain criminal convictions; SEC and CFTC actions; and other events. Refer to the rule cited above for a list of covered persons and disqualifying events.

There is an exception from disqualification if the issuer can show it did not know, and in the exercise of reasonable care, could not have known that a covered person with a disqualifying event participated in the offering.

13.5.2 Due Diligence

This section includes due diligence guidelines provided by FINRA. CIM Securities will conduct due diligence appropriate for the particular Regulation D offering and document its reviews and investigations in the deal file.

When engaging in a Regulation D offering, due diligence will include, at minimum, reasonable investigation of:

- the issuer and its management;
- the business prospects of the issuer;
- the assets held by or to be acquired by the issuer;
- the claims being made; and
- the intended use of proceeds of the offering (including whether investors' money is likely to be applied according to the stated use of proceeds, and whether the stated use of proceeds is reasonable in light of the issuer's business purpose and prospects).

The scope of investigation may depend on a number of specific factors included in FINRA guidance, described below.

BD affiliation with the issuer. If there is affiliation with the issuer, a BD must not compromise its independence in performing a thorough and independent investigation and must resolve any conflict of interests impairing that responsibility.

BD that prepares the private placement memorandum or other offering document. The BD has a duty to investigate the securities offered and representations made by the issuer. Where a BD assists with preparation of a memorandum or document, the BD is subject to FINRA communications rules. **Retail communications are subject to FINRA rule requirements whether or not the BD assisted in their preparation.**

"Red flags" (such as an issuer's refusal to provide information for the BD to meet its obligation to investigate or inaccurate financial statements) must be reviewed and simple reliance on representations by the issuer's management is not sufficient to meet the BD's investigatory obligations.

The use of counsel or experts to perform an investigation on the BD's behalf must be done by firms and individuals that the BD is satisfied are qualified and competent. When CIM Securities is a member of a syndicate or selling group, it may rely upon the reasonable investigation by the syndicate manager if the BD believes the syndicate manager has the expertise and absence of conflicts to conduct the investigation. Reliance may be substantiated by meeting with the manager; obtaining a description of the manager's reasonable investigation efforts; and inquiry regarding the independence and thoroughness of the investigation.

13.5.3 Investigation Practices

The following are FINRA guidelines for what may be included in a reasonable investigation of a Regulation D offering. CIM Securities will conduct investigation into the issuer as appropriate for the proposed offering.

A. Issuer and Management

Reasonable investigations of the issuer and its management concerning the issuer's history and management's background and qualifications to conduct the business might include:

- For Rule 506 offerings, determine whether the issuer or any covered person under Rule 506(d)(1) has been the subject of a disqualifying event precluding the use of the Rule 506 exemption.
 - Examining the issuer's governing documents, including any charter, bylaws and partnership agreement, noting particularly the amount of its authorized stock and any restriction on its activities. If the issuer is a corporation, a BD might determine whether it has perpetual existence.
 - Examining historical financial statements of the issuer and its affiliates, with particular focus, if available, on financial statements that have been audited by an independent certified public accountant and auditor letters to management.
 - Looking for any trends indicated by the financial statements.
 - Inquiring about the business of affiliates of the issuer and the extent to which any cash needs or other expectations for the affiliate might affect the business prospects of the issuer.
 - Inquiring about internal audit controls of the issuer.
 - Contacting customers and suppliers regarding their dealing with the issuer.
 - Reviewing the issuer's contracts, leases, mortgages, financing arrangements, contractual arrangements between the issuer and its management, employment agreements and stock option plans.
 - Inquiring about past securities offerings by the issuer and the degree of their success while keeping in mind that simply because a certain product or sponsor historically met obligations to investors, there are no guarantees that it will continue to do so, particularly if the issuer has been dependent on continuously raising new capital. This inquiry could be especially important for any blind pool or blank-check offering.
 - Inquiring about pending litigation of the issuer or its affiliates.
 - Inquiring about previous or potential regulatory or disciplinary problems of the issuer. A BD might make a credit check of the issuer.
 - Making reasonable inquiries concerning the issuer's management. A BD might inquire about such issues as the expertise of management for the issuer's business and the extent to which management has changed or is expected to change. For example, a BD might inquire about any regulatory or disciplinary history on the part of management and any loans or other transactions between the issuer or its affiliates and members of management that might be inappropriate or might otherwise affect the issuer's business.
 - Inquiring about the forms and amount of management compensation, who determines the compensation and the extent to which the forms of compensation could present serious conflicts of interest. A BD might make similar inquiries concerning the qualifications and integrity of any board of directors or similar body of the issuer.
 - Inquiring about the length of time that the issuer has been in business and whether the focus of its business is expected to change.
- When a new client is signed up by CIM will ensure that it is receiving bad actor reports (BARs) for the Covered Persons in a REG D offering. The Firm make sure it receives a Govt Issued ID from each covered person and do a Microsoft Teams or Zoom Video Conference Call with each Covered Person so it can match the physical identity of that Covered Person in conjunction with having our Third Party Vendor Crowd Check provide us with their BAR on each Covered Person. This should ensure that the Firm is/are ONLY getting BARs on the correct persons a company puts forth and that no "proxy" person should slip through the cracks to ensure the Firm does not engage in Reg D offerings with Bad Actors.

B. Issuer's Business Prospects

Reasonable investigations of the issuer's business prospects, and the relationship of those prospects to the proposed price of the securities being offered, might include:

- Inquiring about the viability of any patent or other intellectual property rights held by the issuer.
- Inquiring about the industry in which the issuer conducts its business, the prospects for that industry, any existing or potential regulatory restrictions on that business and the competitive position of the issuer.

- Requesting any business plan, business model or other description of the business intentions of the issuer and its management and their expectations for the business, and analyzing management's assumptions upon which any business forecast is based. A BD might test models with information from representative assets to validate projected returns, break-even points and similar information provided to investors.
- Requesting financial models used to generate projections or targeted returns.
- Maintaining in the BD's files a summary of the analysis that was performed on financial models provided by the issuer that detail the results of any stress tests performed on the issuer's assumptions and projections.

C. Issuer's Assets

Reasonable investigations of the quality of the assets and facilities of the issuer might include:

- Visiting and inspecting a sample of the issuer's assets and facilities to determine whether the value of assets reflected in the financial statements is reasonable and that management's assertions concerning the condition of the issuer's physical plants and the adequacy of its equipment are accurate.
- Carefully examining any geological, land use, engineering or other reports by third-party experts that may raise red flags.
- Obtaining, with respect to energy development and exploration programs, expert opinions from engineers, geologists and others are necessary as a basis for determining the suitability of the investment prior to recommending the security to investors.

13.6 Private Investment In Public Equity (PIPE)

This section describes PIPE transactions.

13.6.1 Introduction

A PIPE is defined as a privately negotiated sale (*i.e.*, private placement) of securities of an already public company. In a PIPE transaction, a public company sells its unregistered securities (*e.g.*, common stock, preferred stock or convertible securities) in a private placement to a select group of sophisticated individuals or institutions and subsequently files a resale registration statement with the SEC at the completion of the private placement to enable the investors to resell the securities into the public market. CIM Securities's role in a PIPE transaction is to act as the placement agent for the issuer.

13.6.2 Underwriting

PIPE transactions will be managed by Investment Banking (IB) which is also responsible for:

- Obtaining transaction approval from the Investment Banking Supervisor;
- Working with other appropriate personnel/departments, as needed (*e.g.*, Compliance, Legal), to execute an engagement letter; and
- Maintaining a Master Log, which includes among other things an investor log and list of firm employees brought "over the wall."

Non-IB employees approached by an issuer to participate in a PIPE should contact Compliance and/or their supervisor immediately and must handle such information as confidential unless advised otherwise by Compliance or Legal.

13.6.3 Compliance Notification

All PIPE offerings in which CIM Securities is involved, including offerings that are reasonably likely to occur or that CIM Securities is actively pursuing, must promptly be added to CIM Securities's Restricted/Watch List. Consistent with CIM Securities's Information Barrier Policy, the IB manager is responsible for immediately contacting Compliance when there is a reasonable likelihood of receiving a PIPE mandate. Once a company has been added to the Restricted/Watch List, IB must notify Compliance of any significant developments with respect to the transaction, including intended pricing and announcement dates.

13.6.4 Registration Statement Integration

In order to avoid potential registration statement integration (a risk whenever a public and private offering of an issuer's securities are conducted concurrently or within a short period of time to each other), a PIPE offering must be completed before the related resale registration statement is filed. In the event a registration statement covering the same (and/or similar) securities that will be sold in the PIPE offering has been filed but is not yet effective, the issuer must withdraw the registration statement before the PIPE offering can commence. Note the foregoing restriction is not applicable to offerings structured as a registered direct issuance off of an existing/effective registration statement. IB should work with Compliance to ensure compliance with these rules.

13.6.5 Eligible Investors

In general, companies are prohibited from selling unregistered securities unless an exemption is available under SEC rules. With respect to the private placement phase of a PIPE transaction, issuers normally rely on the exemption from registration contained in Section 4(2) of the Securities Act of 1933, as amended (the "Securities Act"), and the safe harbor provisions of Regulation D. As a general matter, in its role as placement agent, CIM Securities may only offer and sell PIPEs to investors whom CIM Securities reasonably believes to be "accredited investors." Generally, CIM Securities may only solicit potential investors who qualify as accredited investors.

Regulation D does not limit the number of accredited investors who may purchase securities in a private placement.

13.6.6 Marketing Restrictions

This section outlines restrictions on marketing pipe offerings.

13.6.6.1 Prohibition On General Solicitation And Advertising

The federal private placement exemption prohibits the issuer of a PIPE and any person acting on its behalf (including placement agents such as CIM Securities) from offering or selling the securities by any form of general solicitation or general advertising. Contacting potential investors with whom CIM Securities has a **pre-existing, substantive relationship** does not constitute a general solicitation. As a general matter, CIM Securities may only contact investors with whom CIM Securities has such a relationship, and generally, initial contact should be made directly with the customer (*i.e.*, contact must be with the ultimate investor with investment discretion).

The general guideline for establishing that a potential investor has had a pre-existing, substantive relationship with CIM Securities is that such potential investor:

- Has invested in other PIPE offerings where CIM Securities acted as placement agent; or
- Has maintained an investment advisory account with CIM Securities (or an affiliate) or a brokerage account or similar relationship with CIM Securities (or an affiliate) for at least 30 days prior to the distribution of information to such investor concerning the offering; and
- Was not solicited to become a customer of CIM Securities in contemplation of the offering.

Failure to observe restrictions that may be imposed on CIM Securities's activities in connection with an offering may have severe consequences, including, depending on the timing of the violation, a forced delay in the ability to market or close the offering or civil and criminal penalties and rescission rights for investors. Any questions concerning whether an activity is appropriate in light of the private nature of a PIPE transaction should be directed to Compliance.

After the **final** closing, "tombstone" advertisements and public statements as to the PIPE offering may be permitted. Compliance should review each such advertisement and statement prior to its publication or use.

13.6.6.2 Written Presentation Content

PIPE transactions are generally marketed via an oral presentation. Any written materials used during the presentation must adhere to the content standards specified below and must be collected from attendees at the end of the presentation.

Written materials created for the purpose of marketing a PIPE transaction should never be based on anything other than the issuer's existing publicly available information (typically the 10K) accompanied by the following:

- Offering summary;
- Key investment highlights; and
- Business summary.

Further, the written presentation:

- Must also contain customary legal legends and disclaimers including preamble language related to: (1) forward looking statements; and (2) confidentiality and Regulation FD obligations (to be reviewed by issuer counsel).
- Should always be accompanied by a disclaimer letter from CIM Securities to prospective investors (to be reviewed by issuer's counsel).
- Should never reference CIM Securities, except to refer to its role as placement agent, and, when appropriate, to disclose potential conflicts of interest to prospective investors (e.g., a firm employee serving on the issuer's board of directors or a material firm ownership position of securities of the issuer).
- Should never be on firm letterhead or other formats containing the firm logo.
- Should never contain forward-looking projections unless such projections have been publicly disclosed. During the marketing process, if prospective investors ask about projections, they should be directed to existing, publicly available research reports and information.

13.6.6.3 FINRA Filings

IB should discuss the specific facts and circumstances of each PIPE transaction with Compliance, Legal and/or external counsel, as necessary, to determine whether to file documents and information with FINRA or whether the offering is clearly exempt from filing.

13.6.6.4 Regulation M

Upon receiving a PIPE mandate, Compliance should be contacted to preliminarily determine if the proposed transaction is subject to Regulation M. Based on the issuer's float, trading volume and a determination of whether the PIPE transaction constitutes a distribution, the issuer's securities may be subject to restrictions on engaging in transactions and quotation activity with respect to the issuer's stock for the applicable restricted period (*i.e.*, 0, 1 or 5 trading days) as required by Regulation M.

If subject to Regulation M, the IB supervisor or Compliance will make required submissions to FINRA. Upon receiving the UAR from FINRA, IB Supervisor will consult with Compliance to determine the appropriate firm market maker status (if applicable) (passive or active) and the applicable Regulation M restricted period. If co-agents are involved,

After the subject transaction has priced, but no later than the market open on the day following pricing, IB Supervisor or Compliance will file the required Reg M forms in FINRA Gateway.

13.6.7 Information Flow

This section outlines information flow for PIPE transactions.

13.6.7.1 Treatment Of Confidential And Inside Information

Prior to the time that an issuer makes a public announcement of a PIPE transaction, information surrounding the offering is confidential information. As PIPE issuers typically see a drop in their share price following the public announcement of the transaction due to the dilution that results from the issuance of additional shares, a PIPE offering will generally constitute a material transaction for an issuer. Accordingly, knowledge of a PIPE transaction prior to a public announcement by the issuer of the transaction may constitute material nonpublic information ("inside information"). As placement agent for an issuer customer, CIM Securities has an obligation not to breach the customer's trust by misusing any information furnished during the course of an engagement. Thus, firm employees with knowledge of a PIPE transaction must:

- Not act on or give this information to others;
- Not trade or advise others to trade based upon the information, misappropriate the information or tip other customers or third parties; and
- Immediately notify Compliance and take appropriate steps to protect the information.

Persons guilty of misusing inside information may be subject to civil and criminal penalties (including imprisonment), SEC administrative actions, disciplinary action by various self-regulatory organizations, and dismissal by CIM Securities.

13.6.7.2 Sharing Transaction Details With Potential Investors

Before a firm employee reveals an issuer's name to a prospective investor, commences discussions concerning the details of a PIPE offering, or otherwise furnishes an investor with material nonpublic information regarding an issuer, such employee should mention that the offering constitutes a private transaction and must ask the prospective investor if he/she is interested in learning more about the PIPE transaction. Firm employees, moreover, should obtain from the prospective investor an agreement that the investor will keep such information confidential, and an acknowledgment that the investor understands how such confidential information must be

treated under the securities laws. As soon as is practicable and typically within one (1) business day after receipt of a prospective investor's positive response, CIM Securities will send such prospective investor a follow-up email confirming such prospective investor's receipt of material, nonpublic information and acknowledging such prospective investor's agreement to hold such information in confidence. In addition, the email will remind such prospective investor of his/her obligation not to use any such information in contravention of applicable securities laws.

Investor logs must be maintained by IB/IB Supervisor during the marketing process and must contain, among other things: (1) the identity of the investors contacted; (2) such investor's level of interest in the subject transaction; and (3) the date that the management presentation was given (in person or via conference call) to such investor. Upon completion of the marketing process, IB Supervisor must forward to Compliance a copy of the investor log.

13.6.7.3 Sharing Information With Sales And Trading Personnel (If applicable)

Any decision to bring sales personnel "over the wall" must be discussed and approved by the designated sales supervisor in consultation with the IB manager and Compliance. Sales personnel brought "over the wall" may continue to conduct their normal sales activities but may not communicate information related to the PIPE transaction to customers. To the extent that sales personnel are asked to assist in the marketing of the PIPE transaction, sales personnel should make the marketing calls off of the trading floor in an area where their conversation cannot be overheard.

Any decision to bring trading personnel "over the wall" must be discussed and approved by the manager of Trading (NASDAQ or Listed) in consultation with the IB Supervisor and Compliance. Trading personnel brought "over the wall" may not trade or make markets in the securities of the issuer subject to the PIPE transaction. The Trading manager should assign trading responsibilities for such securities to another trader without divulging the details of the PIPE transaction. Trading personnel brought "over the wall" may continue to trade and make markets in other securities pursuant to their normal responsibilities but are prohibited from disclosing information regarding the PIPE transaction to anyone that is not already "over the wall."

13.6.7.4 Sharing Information With Research Analysts – Not applicable at Present

Any decision to bring a firm research analyst "over the wall" must be discussed and approved by the Research manager and Compliance.

13.7 Conservation Donation Transactions (CDTs) – If applicable

[Report on FINRA's Examination and Risk Monitoring Program: <https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program>]

CDTs commonly involve private placement offerings where investor returns are based on a share of tax savings from a charitable donation. In practice, CDTs involve unrelated investors acquiring an interest in a pass-through entity (*i.e.*, a partnership or limited liability company) owning unimproved land.

Before year-end, the pass-through entity either grants a conservation easement - which forever limits future development of the land - or outright donates the land to a land trust. In exchange, the pass-through entity receives charitable donation tax deductions, which serve as a return on investment to investors and often have values based solely on land appraisals that are predicated on an alternative plan to develop the land, oftentimes the equivalent of four to more than 10 times the price paid to acquire the land. Common CDTs involve syndicated conservation easement transactions [SCETs] or substantially similar fee simple donations of land.

Recommendations must comply with the requirements of Reg BI.

13.8 Private Equity Funds

Private equity funds pool investments from individuals and institutions and invest in businesses. Investors are usually limited partners in a limited partnership controlled by a general partner that determines the investing of funds. There is no public market for private equity funds but there may be a secondary market for interests.

Private equity funds may offer a high rate of return with a corresponding high rate of risk of loss. In a growing economy funds may exit the earliest portfolio investments providing distributions to limited partners, but a slowing economy may restrict the fund's ability to liquidate investments. Most investors are institutions that have the ability to develop a diversified portfolio of private equity funds or that invest through a fund of funds to provide a diversified portfolio.

Features of private equity funds include the following:

- Entry requires a substantial initial investment (which may be \$1,000,000 or more) allowing the fund's manager discretion over the first few years of the fund.
- Funds may provide for obligatory capital contributions throughout the life of the fund obligating the limited partners to make additional contributions. Failure to meet capital calls may result in the defaulting limited partner forfeiting interest in the fund.
- These are illiquid investments that are not publicly traded. An investor's capital is locked up in a long-term investment which may last ten years or more with no redemption rights. Distributions are made only as investments are converted to cash.
- Limited partners typically have a passive role with no say in the actions of the general partner.
- The general partner may not find suitable investments for the fund resulting in the investors' funds remaining uncommitted
- Funds are high risk; the investor may lose all of the investment.

Recommendations are subject to Reg BI and RRs must obtain necessary partnership agreements and any customer eligibility documents required for the investment and submit them to the appropriate supervisor for review.

14 CYBERSECURITY

[SEC Regulation S-P Rule 30; SEC Release No. 34-50781; DOJ Cybersecurity Unit report on best practices re victim response and reporting: http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf; FINRA Notice to Members 05-49; FINRA web page: Customer Information Protection <http://www.finra.org/industry/cybersecurity>; Fair and Accurate Credit Transactions Act of 2003 Section 216; FTC Safeguards Rule; SIFMA cybersecurity web page: <http://www.sifma.org/issues/operations-and-technology/cybersecurity/overview/>; Safeguards Rule 16 CFR Part 314; SIFMA cybersecurity guidance for small firms: <https://www.sifma.org/resources/general/cybersecurity-guidance-for-small-firms/>; FINRA Small Firm Cybersecurity Checklist: <https://www.finra.org/compliance-tools/cybersecurity-checklist>; Center for Internet Security: <https://www.cisecurity.org/>

This chapter outlines CIM Securities's program for addressing cybersecurity risks. These procedures are modeled after the NIST Framework for Improving Critical Infrastructure Cybersecurity and are guidance for CIM Securities. It also includes guidance and practices from SEC and FINRA exam priorities and cybersecurity reports. Procedures are subject to CIM Securities's business model and technology infrastructure. Some of these procedures will be conducted by CIM Securities's clearing firm, if applicable, and will be subject to the section on third party vendors. Procedures in this chapter also apply to branch offices, as appropriate. See the section *Cybersecurity* in the chapter *OFFICES* as well as the *Cybersecurity Policy* in the chapter *GENERAL EMPLOYEE POLICIES AND PROCEDURES*.

14.1 Assignment Of Responsibility

Cybersecurity oversight is the responsibility of the following:

- Chief Executive Officer or Equivalent
- Chief Compliance Officer

Where appropriate, responsibilities will be segregated and/or supervised to prevent unauthorized activities.

14.2 Identification Of Risks

Risks in CIM Securities's systems will be identified, reviewed annually, and updated when necessary, including the following.

- Identification of mission critical systems (email, data storage, etc.)

14.3 Risk Assessments

Risk assessments will be conducted periodically.

- Frequency is determined by the designated supervisor who will maintain a schedule and update as necessary.

14.3.1 Asset Inventory

The risk assessment will include an asset inventory to identify critical assets and their vulnerability to attack. CIM Securities will also identify sensitive customer and Firm information and the location(s) where such information is stored. CIM Securities will provide secured asset disposal, such as destroying hard drives of computers no longer in use.

14.3.1.1 Branch Assets

Branch asset review procedures will include the following:

- Establishing processes by which branches manage and report lost or stolen assets, if applicable.

14.4 Insider Threat

[SIFMA Best Practices for Insider Threats: <https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf>]

"Insiders" include individuals who currently have or previously had authorized access to Firm systems and data because of their function or role and include individuals such as full and part-time employees, contract or temporary employees, consultants and interns, and employees or contractors of third-party vendors and sub-contractors.

Insider's threats are addressed as follows:

- Training for all insiders

14.4.1 Identifying Potentially Malicious Activity

Malicious insider threats are challenging because these individuals know CIM Securities and its systems and weaknesses. Indicators of potential risk, if known, may include notification or evidence of illegal activity; threats of retaliatory acts or violence; significant debt and recurring financial irresponsibility; time and attendance fraud; falsifying reports or records; unexcused or unauthorized absences; and other indicators of the employee's dissatisfaction that may lead to malicious activity.

To mitigate the potential for malicious activity, CIM Securities has adopted the following practices:

- Designating a senior executive or manager with responsibility for the firm's insider threat controls

14.5 Third Party Vendors

[Statement on Standards for Attesting Engagements (SSAE) No. 16; System and Organization Controls (SOC): <https://www.aicpa.org/soc>, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html>; Cybersecurity and Infrastructure Security Agency's (CISA) Risk Considerations for Managed Service Provider Customers: https://www.cisa.gov/sites/default/files/publications/cisa-insights_risk-considerations-for-msp-customers_508.pdf]

Third party vendors that will have access to CIM Securities's systems or devices will be reviewed, prior to engagement and periodically, to:

- Evaluate the vendor's cybersecurity safeguards prior to approving engagement with particular review of firewalls and other security systems
- Include cybersecurity assurances in CIM Securities's contract with the third party including notifying CIM Securities of a breach of customer data
- Notify RRs and supervisors of approved third party vendors and limitation of use to only approved vendors
- Periodically (at least annually) review security systems including cloud-based storage and protection of data

14.5.1 Vendor Selection and Due Diligence

Due diligence conducted to select vendors may include:

- Confirming vendors have a sound knowledge of cyber risks, current attack techniques and appropriate tools to emulate the actions of an attacker

14.6 Encryption Of Data

Data regarding private customer information transmitted to laptops or remote devices will be encrypted. Such data stored on laptops and other remote devices will also be encrypted.

14.7 Identity Access Management (IAM) and User Entitlements

[FINRA Information Notice: Cybersecurity Background - Authentication Methods: Information Notice 10/15/20 (finra.org)]

CIM Securities has adopted the following practices to control access to CIM Securities's systems and data:

- Disabling or changing the use of generic IDs (such as vendor-provided "default user" and "administrator" IDs and passwords used for the first time system install) to require individual IDs for each user and strong passwords

14.7.1 Privileged User Controls

The Firm has adopted the following practices to control access:

- Monitoring of privileged user system access activities

14.8 Security Information and Event Management (SIEM) and User and Entity Behavioral Analytic (UEBA) Tools

SIEM tools collect and aggregate and correlate log information from numerous sources, including but not limited to: firewalls, Intrusion Detection and Prevention systems, servers, and network devices. Firms use the aggregated

log to monitor various user activities and events. A SIEM system may identify and generate alerts regarding risky activities and potential attacks so that the firm can respond to and prevent sensitive information from going outside the firm's network. In some advanced cybersecurity programs, firms use machine learning in conjunction with SIEM tools to learn and model baseline and irregular behavior, which improves the system's ability to identify potentially malicious behavior, including risky insider activities.

UEBA tools can also enhance a firm's capability to detect anomalous behaviors. Such tools focus on analyzing individual user and entity behaviors, and typically include a learning element that enables the tool, over time, to identify normal and abnormal behaviors and to flag the latter for further review.

The Firm has adopted the following practices regarding SIEM and UEBA:

- Establishing risk-based approaches to identify high risk events, provide timely alerts and escalate events according to agreed procedures

14.9 Data Loss Prevention (DLP)

A strong DLP program creates preventative controls that can help to detect and mitigate insider (and other) threats. DLP controls can prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method. CIM Securities may maintain DLP software internally or use vendors to support these efforts.

CIM Securities has adopted the following practices to prevent data loss:

- Establishing rules to control printing of sensitive data and documents

14.10 Penetration Testing (PEN)

Penetration testing (or a pen test) is an important element of CIM Securities's cybersecurity program. A pen test simulates an attack on a firm's internally- or externally-facing computer network to determine the degree to which malicious actors may be able to exploit vulnerabilities in the network and evaluate the effectiveness of the firm's protective measures. Pen tests may take the perspective of an outside attacker attempting to infiltrate a firm's system or an insider attacker trying to gain access to assets to which they should not have access.

CIM Securities has adopted practices for penetration testing (PEN) which may include:

- Adopting a risk-based approach to penetration testing including identifying higher risk systems such as online trading; high risk systems that include or access sensitive data; operationally important systems; and the presence of known vulnerabilities

14.11 Retirement Of Equipment Containing Data

Computers or other data-retaining equipment that will be disposed of will be subject to clearing of hard drives and other repositories of data prior to disposal. If a computer will be re-assigned to someone who is not authorized to view data stored on that computer, the hard drive will be cleared prior to reassignment. Flash drives and other portable data devices that will no longer be used or will be reassigned will be destroyed or cleared of all data prior to disposal or re-use.

14.12 Detection Of Unauthorized Activity

Procedures to detect unauthorized activity on networks and devices include the following:

- Software is used to detect malicious code on the firm's networks and mobile devices and to prevent loss of data.

14.12.1 Cloud-Based E-mail Account Takeovers (ATOs)

[FINRA Regulatory Notice 21-18; FINRA Information Notice 10/2/19: Cybersecurity Alert: Cloud-Based Email Account Takeovers: <https://www.finra.org/rules-guidance/notices/information-notice-100219>]

Attackers may use compromised e-mail accounts to take over e-mail to defraud firms by requesting fraudulent wire requests or stealing confidential firm information or non-public personally identifiable information. This includes attacks taking over administrative privileges which may result in a broader attack. The Notice should be referenced for an explanation of attack techniques.

14.12.1.1 Responding To An Attack

CIM Securities's response will include the following:

- determining whether any customer information was breached and notification required under federal or state law

14.12.1.2 Preventing ATOs

CIM Securities has procedures to prevent and respond to ATOs which may include the following:

- Multi-factor authentication (MFA) - Implement MFA for all e-mail account log-in activity outside of the Firm's network for general users (e.g., for registered representatives and, internal administrators). On the Office 365 (O365) platform, implement MFA for Microsoft Partners and use the Microsoft Authenticator application on users' mobile devices or a dynamically generated personal identification number (PIN) sent via SMS text to provide the second factor.
- E-mail Archiving - Retain and archive all e-mails in a separate location from the e-mail server to provide the Firm with an additional copy of all inbound and outbound e-mails including alerts to appropriate firm personnel if there were interruptions in e-mail archiving services.

14.13 Cybersecurity Incident Response Program

[FINRA Regulatory Notice 21-18]

If an intrusion is identified, the designated cybersecurity supervisor will coordinate CIM Securities's response which may include:

- Limiting access to affected systems or devices
- Diverting computer resources to a safe system
- Engaging a third party to process data until CIM Securities's system is safe

- Engaging a third party to assess the intrusion
- Assessing data loss and reviewing potentially impacted customer accounts
- Notifying the AML Compliance Officer and/or Chief Compliance Officer
- Notifying regulators and customers including filing of SARs
- Evaluating potential financial losses
- Taking corrective action to prevent a future intrusion
- Reporting fraud, where appropriate, to authorities including FINRA, the SEC, the FBI, the Internet Crime Complaint Center, and local state securities regulators. [Contact information is included in Regulatory Notice 21-18.]

14.14 Recovery

CIM Securities has procedures for data backup and recovery of data. Refer to the *Business Continuity Plan* for further information.

14.15 Business Continuity/Pandemic Responses

[FINRA Information Notice 3/26/20 Cybersecurity Alert]

This section includes guidelines from FINRA Information Notice dated 3/26/20.

14.15.1 Measures for Associated Persons

Office and Home Networks

- Use a secure network connection to access your Firm's work environment (e.g., through a company-provided Virtual Private Network (VPN) or through a secure Firm or third-party website (which begin with "https")).
- Secure Wi-Fi connections using a stringent security protocol (e.g., WPA2).
- Check for and apply software updates and patches to routers on a timely basis.
- Change the default user names and passwords on home networking equipment, such as Wi-Fi routers.

Computers and Mobile Devices

- Check for and apply updates and patches to the operating system and any applications on a timely basis.
- Install and operate anti-virus (AV) and anti-malware software.
- For any files on a personal device, check your Firm's policy about file storage and back-up, especially if the files contain customer personally identifiable information (PII).
- Lock your screen if you work in a shared space and plan to be away from your computer.

Common Attacks

- Be sensitive to the growing variety of scams and attacks that fraudsters are using to exploit the current situation, such as:
 - phishing scams that reference COVID-19, the coronavirus or related matters;
 - fake, unsolicited calls from a "Helpdesk" requesting passwords or wanting to walk you through your home preparedness; and
 - malicious links in e-mails, online sites and unofficial download sites, especially those offering "free software."

Incident Response

- Understand your role in CIM Securities's incident response plan and whom to contact in the event of a cybersecurity incident (e.g., data breach, loss or exposure of customer PII, successful e-mail attack, ransomware, lost or stolen mobile device).

14.15.2 Measures for Firms

Network Security Controls

- Provide staff with a secure connection to the work environment or sensitive applications (e.g., VPN, secure sessions remote desktop with multi-factor authentication).
- Evaluate privileges to access sensitive systems and data.

Training and Awareness

- Provide staff with training on:
 - how to connect securely to the office environment or office applications from a remote location; and
 - potential scams and other attacks described above.
- Alert CIM Securities's IT support staff, or others involved in managing or supporting staff using CIM Securities's systems, to be diligent in vetting incoming calls because fraudsters may use the increase in remote work to engage in social engineering schemes, such as making bogus calls requesting password resets or reporting lost phones or equipment. FINRA is aware of successful social engineering attacks where fraudsters contacted a Help Desk, for example under the guise of requesting a password reset, and subsequently used information about critical technical or business operations gained during this conversation to steal funds from CIM Securities.

14.16 Reports To Senior Management

Cybersecurity risk assessments to the extent applicable will be included in the Annual Report to the CEO or equivalent.

14.17 Training

Data breaches may occur because well-intentioned employees or other users make preventable mistakes. Developing a firm culture that focuses on cybersecurity awareness and providing regular cybersecurity training can help address this problem. CIM Securities provides ongoing training as necessary or applicable on:

- Appropriate handling of customers' requests for user name and password changes, money transfers and identity verification, particularly those involving large amounts of money transferred to an overseas location or third parties
- Sound practices regarding the opening of email attachments and links, including using simulated phishing campaigns where the firm notes and re-tests the individuals who failed the exercise
- Identifying social engineering activities from hackers

14.18 Other Policies

The following other policies in this manual address issues involving cybersecurity:

- Privacy Policy (GENERAL EMPLOYEE POLICIES)
- Electronic Communications Policy (GENERAL EMPLOYEE POLICIES)
- Mobile Devices (GENERAL EMPLOYEE POLICIES)
- Computer Records, Equipment And Software (GENERAL EMPLOYEE POLICIES)
- Cybersecurity Policy (GENERAL EMPLOYEE POLICIES)
- Identity Theft Prevention Program (Red Flags Rule) (ANTI-MONEY LAUNDERING [AML] PROGRAM)
- Electronic Communications Systems And Devices (COMMUNICATIONS WITH THE PUBLIC)
- Protection Of Customer Information And Records (FINANCIAL AND OPERATIONS PROCEDURES)
- Business Continuity Plan (FINANCIAL AND OPERATIONS PROCEDURES)
- Cybersecurity (OFFICES)

15 REGULATION BEST INTEREST (BI)

[SEC final rule: <https://www.sec.gov/rules/final/2019/34-86031.pdf>; SEC small entity compliance guides: <https://www.sec.gov/info/smallbus/secg/regulation-best-interest> and <https://www.sec.gov/info/smallbus/secg/form-crs-relationship-summary>; SEC release announcing adoption of Reg BI with a link to the entire regulation: https://www.sec.gov/news/press-release/2019-89?mod=article_inline; FINRA Reg BI and Form CRS Checklist: <https://www.finra.org/sites/default/files/2019-10/reg-bi-checklist.pdf>; FINRA Regulatory Notice 19-26; FINRA website re Reg BI: <https://www.finra.org/rules-guidance/key-topics/regulation-best-interest>]

Regulation BI is an SEC regulation that requires a broker-dealer (BD) and its associated persons (RRs in this chapter) to act in the best interest of the retail customer at the time the recommendation is made, without placing the financial or other interest of the broker-dealer or RR ahead of the interest of the retail customer. Definitions and cross references to other chapters appear at the end of this chapter.

15.1 Summary Of Key Requirements

1. Regulation BI applies only to recommendations to natural persons who are retail customers. Reg BI **also** applies to recommendations to natural persons who are considered "institutional accounts" under FINRA rules.
2. Recommendations include those for orders; types of accounts (e.g., brokerage vs. advisory, whether or not tied to a securities transaction); and investment strategies. Also included are recommendations to prospects.
3. The "best interest" standard goes beyond suitability requirements for recommendations; it requires acting in the customer's best interest and not the RR's or BD's interest including consideration of available alternatives and cost/risk rewards.
4. Compliance with Reg BI requires meeting four obligations: disclosure, care, conflict of interest, and compliance.
5. If the BD agrees to monitor a customer's account, Reg BI applies to explicit and implicit recommendations to hold. Reg BI does not impose a duty to monitor customer accounts.
6. Form CRS must be provided to customers when an account is opened (including additional accounts for existing customers) and when a recommendation is made (as defined in this chapter). Form CRS is posted on the Firm's website and updates must be provided to customers within 60 days of material updates.
7. BDs and their professionals are not permitted to use the titles "advisor" or "adviser" unless CIM Securities is dually registered as a broker-dealer and investment adviser and the RR is employed by a registered investment adviser and authorized by Compliance to use such a title.
8. Incentive programs (sales contests, non-cash compensation, etc.) may not be limited to certain securities or types of accounts over a period of time.
9. Communications for education purposes (listed below) that do not include a recommendation of a particular security or strategy involving securities are not considered recommendations:
 - o General financial and investment information which encompasses basic investment concepts.
 - o Descriptive information about an employer-sponsored retirement or benefit plan.
 - o Certain asset allocation models based on generally accepted investment theory accompanied by necessary disclosures.

15.2 General Obligations

Compliance with each of the following four component obligations is necessary to comply with Regulation BI.

15.2.1 Disclosure

[SEC FAQs on Form CRS: <https://www.sec.gov/investment/form-crs-faq>]

Responsibility	IB Supervisor, VA Supervisor, if applicable
Resources	<ul style="list-style-type: none">• New product reviews and information• Form CRS• Other disclosures regarding securities and accounts
Frequency	<ul style="list-style-type: none">• Form CRS: when a recommendation is made and when updated• When new products/services are proposed and at least annually:<ul style="list-style-type: none">◦ Review products and services to confirm necessary disclosures are provided to retail customers including possible standardized disclosures◦ Consider the need for specific training• As soon as practicable but no later than 30 days after a material change - update disclosures• Other disclosures: as required
Action	<ul style="list-style-type: none">• Identify necessary disclosures and other requirements for new securities or services (Also see <i>New Products</i> in the chapter <i>FINANCIAL AND OPERATIONS PROCEDURES</i>)• Identify necessary disclosures as part of a review of current products and services• Update disclosures if there have been any material changes• Provide Form CRS and other necessary disclosures to retail investors at time of a recommendation/account opening and within 60 days of material changes• Include review of disclosures in annual review of firm's procedures
Record	<ul style="list-style-type: none">• Reviews of products and services and actions taken for disclosure• Tracking of providing disclosures including version, date provided, to whom provided including Form CRS• Various other methods of disclosure (confirmations, monthly statements, account agreements, prospectuses, <i>etc.</i>)

The obligation to provide full and fair disclosure should give sufficient information to enable a retail investor to make an informed decision with regard to a recommendation.

The disclosure obligation requires a BD or RR, prior to or at the time of the recommendation, to provide the retail customer, in writing, full and fair disclosure of:

- All material facts relating to the scope and terms of the relationship with the retail customer, including:
 - That the BD or associated person is acting as a BD or an associated person with respect to the recommendation;
 - The material fees and costs that apply to the retail customer's transactions, holdings, and accounts;
 - The type and scope of services provided to the retail customer, including any material limitations on the securities or investment strategies involving securities that may be recommended to the retail customer; and

- Material facts relating to conflicts of interest that are associated with the recommendation. "Material facts" are facts a retail customer would consider important in making an investment decision. For example, material facts relating to conflicts of interest including, but not limited to, how RRs are compensated and the benefits to a BD from recommending a proprietary product.
- Other material facts relating to the scope and terms of the relationship with the retail customer which include:
 - The general basis for a recommendation (*i.e.*, what might commonly be described as investment approach, philosophy, or strategy); and
 - Risks associated with recommendations in standardized terms.
- If necessary, other material facts relating to the scope and terms of the relationship.

Disclosures are provided in a variety of ways, including (but not necessarily limited to) the following:

- Electronic mailings to those who have consented to receive electronic delivery
- Form CRS Relationship Summary
- Account opening documents and account agreements
- Firm's website
- Standardized disclosures
- Disclosures specific to certain securities or products (e.g., risk, conflicts of interest, material limitations)
- Fee schedules
- Prospectuses

While disclosures must be in writing, in certain circumstances oral disclosures (no later than the time of the transaction) to supplement facts not reasonably known at the time written disclosure is made (a record of oral disclosures) must be maintained with the order record.

15.2.2 Care

Responsibility	IB Supervisor
Resources	<ul style="list-style-type: none"> • Customer account information • Information about securities • Available reports
Frequency	<ul style="list-style-type: none"> • When recommendations are made • Other: as required
Action	<ul style="list-style-type: none"> • Communicate risks, costs, and other necessary information to RRs • Review recommendations of transactions and opening of accounts • Consider whether to use a risk-based approach to identify certain type of recommendations that should be documented, and the type of documentation (<i>e.g.</i>, categorizing recommendations as "high risk" or "complex")
Record	<ul style="list-style-type: none"> • Order records • Account records • Reviews of orders and accounts with supervisor's record of supervision and actions taken, if any

	<ul style="list-style-type: none"> Records of risk-based recommendations and documentation of recommendations, if applicable
--	---

The care obligation is broader than the existing suitability standard because it: (1) explicitly requires that the recommendation be in the customer's best interest and that the BD and RRs do not place their interests ahead of the customer; (2) explicitly requires that cost be a consideration; (3) applies the quantitative suitability requirement (recommending a series of transactions, avoiding excessive activity); and (4) requires the BD and RRs to consider "reasonably available alternatives" as part of having a "reasonable basis to believe" that the recommendation is in the best interests of the customer.

The RR must exercise reasonable diligence, care, and skill to:

- understand the risks, rewards, and costs associated with the recommendation;
- have a reasonable basis to believe the recommendation is in the customer's best interest; and
- have a reasonable basis to believe that recommended transactions are in the customer's best interest based on the customer's investment profile and doesn't place the interests of the BD ahead of the customer. This includes avoiding transactions that are excessive.

In particular, the BD and RR must have an understanding of complex products, and recommendations of complex investments should be documented, particularly where a recommendation may seem inconsistent with a retail customer's objectives on its face. The care obligation applies to a series of recommended transactions (quantitative suitability) whether or not the BD exercises actual or *de facto* control over the account.

15.2.2.1 Factors To Consider

When making recommendations, the following non-exclusive list of factors (depending on the particular product or strategy recommended) may be considered:

- What are the characteristics (including any special or unusual features) of the security or strategy?
- What are the initial and subsequent costs (if any, e.g., surrender or redemption costs) of the security or strategy?
- How liquid is the security?
- What are the risks, volatility, and likely performance in a variety of market conditions (normal or stressed)?
- What is the expected return of the security?
- What are the financial incentives to recommend the security or investment strategy?
- Are there alternative investments or strategies, at lower cost, that may meet the customer's needs? More costly products may be recommended provided there is a reasonable basis to believe they are in the best interest of the customer. There is no obligation to recommend the "best" of all possible alternatives.

15.2.2.2 Recommending Types Of Accounts

RRs must have a reasonable basis for recommending accounts (margin, brokerage or advisory, IRAs, etc.). This includes the following considerations:

- services and products provided in the account;
- projected cost of the account;
- alternative account types available;
- services the retail customer requests; and

- the retail customer's investment profile. Profile elements include age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, risk tolerance, and any other information disclosed by the customer.

Additional considerations when recommending IRAs (including rollovers or transfers of assets in a workplace retirement plan account to an IRA) include:

- customer's current financial situation and liquidity needs;
- fees and expenses;
- level of services available;
- ability to take penalty-free withdrawals;
- application of required minimum distributions;
- protections from creditors and legal judgments;
- holdings of employer stock; and
- any special features of the existing account.

15.2.2.3 Costs

The RR should understand and consider the potential costs associated with the recommendation and have a reasonable basis to believe that the recommendation does not place the financial or other interest of CIM Securities or RR ahead of the interest of the retail customer. While cost must be considered, it should never be the only consideration. Cost is only one of many important factors to be considered regarding the recommendation and that the standard does not necessarily require the "lowest cost option." RRs need to consider costs in light of other factors and the retail customer's investment profile.

15.2.2.4 Alternatives

Alternatives should be considered before making recommendations to a particular retail customer. This does not mean customers must be offered all alternatives or necessarily the lowest-cost alternative or the "single best" alternative. Reasonably available alternatives include considerations of, for example:

- An RR's customer base (including the general investment objectives and needs of the customer base)
- Investments and services available to the RR to recommend (including limitations due to the RR's licensing)
- Specific limitations on the available investments and services with respect to certain retail investors (e.g., product or service income thresholds; product geographic limitations; or product limitations based on account type, such as those only eligible for IRA accounts)

15.2.2.5 Quantitative Suitability

R Rs may not make recommendations that result in transactions excessive for the customer considering the customer's investment objectives (also known as "churning"). A series of recommended transactions must be in the customer's best interest. The customer may be contacted by CIM Securities to confirm that active trading is appropriate.

15.2.2.6 Material Limitations

If CIM Securities materially limits its product offerings to certain proprietary or other limited menus of products or third-party arrangements, its limited menu does not justify a product recommendation that is not in the customer's best interest.

15.2.3 Conflict Of Interest

[FINRA website on conflicts of interest: <https://www.finra.org/rules-guidance/key-topics/conflicts-of-interest>]

A conflict of interest is an interest that might incline a BD or an RR - consciously or unconsciously - to make a recommendation that is not disinterested. Conflicts may exist between the BD and the retail customer; between the RR and the retail customer; and between the BD and the RR. Additional conflicts may exist between customers (e.g., IPO allocations or proprietary research or advice among different types of customers).

CIM Securities has an obligation to avoid or mitigate conflicts of interest where possible and provide disclosure where conflicts may exist.

CIM Securities will identify conflicts and, where appropriate, identify material limitations placed on the investment product or strategy and any conflicts associated with such limitations (e.g., limited product menu, proprietary products only, etc.) and make necessary disclosures.

Incentive programs (whether provided by CIM Securities or a third party) such as sales contests, sales quotas, bonuses, non-cash compensation, etc., within a limited period of time are prohibited if they are based on:

- a specific product; or
- types of securities.

RRs have an obligation to avoid conflicts of interest when dealing with retail customers; some examples are listed below.

1. Recommending proprietary products because they result in higher compensation without considering the customer's needs and alternative investments.
2. Recommending other products or services based on compensation/incentives from CIM Securities or third parties.

15.2.4 Compliance

CIM Securities conducts ongoing and annual reviews and training to achieve compliance with Regulation BI. It is the responsibility of RRs to be familiar with these requirements and act in the customer's best interest at all times. Questions should be referred to Compliance.

15.3 Form CRS

[SEC Form CRS instructions: <https://www.sec.gov/rules/final/2019/34-86032-appendix-b.pdf>; SEC FAQs on Form CRS: <https://www.sec.gov/info/smallbus/secg/form-crs-relationship-summary>; SEC Form CRS Relationship Summary Small Entity Compliance Guide: <https://www.sec.gov/info/smallbus/secg/form-crs-relationship-summary>]

Responsibility	CCO
Resources	<ul style="list-style-type: none">• Information about securities and types of accounts and services offered by CIM Securities• New product and services reviews
Frequency	<ul style="list-style-type: none">• When recommendations are made (as defined in this chapter)• Update and file with CRD as required
Action	<ul style="list-style-type: none">• Provide Form CRS to retail customers when a recommendation is made and within 60 days of a material change to the Form• Post Form CRS to CIM Securities's website and update as necessary• File Form CRS with the CRD and update within 30 days when required• Include Form CRS in reviews/audits to confirm the form is being kept up to date; posted to the website; filed with the CRD; and sent to customers when there are material changes
Record	<ul style="list-style-type: none">• Website postings• Providing Form CRS to customers including when delivered; version provided; consent to e-delivery if delivered electronically• Records of updates, changes provided to customers, updates to website• CRD filings• Records of reviews/audits

Form CRS is a relationship summary intended to clarify the relationship between the BD and the customer. Firms without retail customers (as defined under Regulation BI) are not required to provide the form to customers or submit it to regulators. Form CRS must be provided before or at the time of a recommendation. The form is required upon **the first event that triggers the requirement** which includes when:

- An order is placed for the retail customer
- A new account is opened for a new customer
- A new account is opened for an existing customer
- A securities transaction or investment strategy is recommended
- A rollover is recommended from a retirement account into a new or existing account or investment
- An RR recommends or provides a new advisory service or product that does not necessarily involve opening a new account or would not be held in an existing account, for example, the first-time purchase of a direct-sold mutual fund or insurance product that is a security through a "check and application" process, *i.e.*, not held directly within an account
- A retail investor requests a copy (provide within 30 days)

The Form will be updated and filed with the CRD within 30 days of material changes. Updated summaries will be provided to customers within 60 days after material updates with changes highlighted. Updates may be provided electronically to customers who have consented to electronic delivery.

Dual registrants (BD and IA) are required to deliver a relationship summary to retail investor customers of both the investment advisory and brokerage businesses.

15.4 Training

Responsibility	CCO
Resources	<ul style="list-style-type: none">• In-house training materials• Outside vendors or materials
Frequency	<ul style="list-style-type: none">• Annual; when new RRs are hired; and as appropriate
Action	<ul style="list-style-type: none">• Provide training on acting in a customer's best interest, CIM Securities's culture, the Code of Conduct, and conflicts of interest in their mitigation and management
Record	<ul style="list-style-type: none">• Record of subjects included in training, who attended, and when administered

RRs will receive training on "best interest" requirements and communicating Firm culture, specific requirements of CIM Securities's code of conduct and its conflicts management framework.

15.5 Monitoring Accounts

CIM Securities may provide monitoring of retail customer accounts under the following circumstances:

- Voluntarily and without any agreement with the customer to review the account for purposes of deciding whether to make an investment recommendation.
- Agreed-upon limited monitoring on a periodic basis for purposes of providing buy, sell, or hold recommendations.

CIM Securities does not charge a separate fee or separately contracts for this service or receive any special compensation. Such monitoring is solely incidental to CIM Securities's securities business. Account monitoring is disclosed on Form CRS.

If CIM Securities offers monitoring for compensation or under other circumstances not solely incidental to its securities business, it will register as an Investment Adviser and comply with those requirements.

15.5.1 Monitoring

It is the firm's policy not to monitor accounts. Reg BI does not impose a duty to provide ongoing advice and monitoring.

15.6 Dual Registrants

Dual registrants and affiliates (as defined at the end of this chapter) are required to provide a Form CRS for both the broker-dealer and advisory relationships; the forms may be combined. Broker-dealers have an obligation to file Form CRS with FINRA's CRD and advisers are required to file with IARD.

If two separate relationship summaries are provided, they will reference and facilitate access to the other with equal prominence and at the same time, without regard to whether the particular retail investor qualifies for those retail services or accounts.

CIM Securities does not have an affiliated investment advisor.

15.6.1 Recordkeeping

[Exchange Act Rule 17a-3(a)(35); SEC Use of Electronic Media: <https://www.govinfo.gov/content/pkg/FR-1996-05-15/pdf/96-12176.pdf>]

Responsibility	IB Supervisor, CCO
Resources	<ul style="list-style-type: none">• Provision of Form CRS to prospects, customers
Frequency	<ul style="list-style-type: none">• As required under Form CRS requirements, obtaining consent
Action	<ul style="list-style-type: none">• Obtain recipient's informed consent for electronic delivery• Track delivery of Form CRS which may include electronic return-receipt or by confirmation that information was accessed, downloaded, or printed and/or disseminating information through facsimile methods• Include reviewing providing Form CRS in audit/review programs
Record	<ul style="list-style-type: none">• Consents for e-delivery• Tracking records of delivery• Records of Form CRS and updates to the form• Record of filing with FINRA CRD• Record of audits/reviews of providing Form CRS

Records of all information collected from and provided to the retail customer are maintained in accordance with recordkeeping rules. Records are not required to evidence best interest determinations on a recommendation-by-recommendation basis. CIM Securities also is not required to provide information regarding the basis for each particular recommendation. Records of Form CRS will be retained for six years after the earlier of the date that the account was closed or the date on which the information was collected, provided, replaced or updated.

15.7 Definitions

Affiliate: Any persons directly or indirectly controlling or controlled by CIM Securities or under common control with CIM Securities.

Best interest: The term "best interest" is explained through SEC guidance and interpretations and is not expressly defined. Whether a broker-dealer has acted in the retail customer's best interest in compliance with Regulation BI

will turn on an objective assessment of the facts and circumstances of how the specific components of Regulation BI - including its Disclosure, Care, Conflict of Interest, and Compliance Obligations - are satisfied at the time that the recommendation is made (and not in hindsight).

Conflict of interest: A conflict of interest is an interest that might incline a BD or RR, consciously or unconsciously, to make a recommendation that is not disinterested.

Dually licensed financial professional: A natural person who is both an associated person of a broker-dealer registered under section 15 of the Exchange Act, as defined in section 3(a)(18) of the Exchange Act, and a supervised person of an investment adviser registered under section 203 of the Advisers Act, as defined in section 202(a)(25) of the Advisers Act.

Dual registrant: A firm that is dually registered as a broker-dealer under section 15 of the Exchange Act and an investment adviser under section 203 of the Advisers Act and offers services to retail investors as both a broker-dealer and an investment adviser. There are exceptions; for example, if a BD dually registered offers investment advisory services to retail investors, but offers brokerage services only to institutional investors, the BD is not a dual registrant for purposes of Form CRS.

Full and fair: Sufficient information to enable a retail customer to make an informed decision with regard to a recommendation.

Implicit or explicit recommendations: For accounts where there is agreed-upon account monitoring, if the BD makes no recommendation in a periodic review, it is an implicit "hold" recommendation subject to Regulation BI just as would an explicit "hold" recommendation. Absent an agreement to monitor an account, Regulation BI does not apply to implicit hold recommendations.

Legal Representative: includes the non-professional legal representatives of a natural person, *e.g.*, a non-professional trustee that represents the assets of a natural person. Regulation BI would not apply when the legal representative is acting in a legal capacity as a regulated financial services industry professional retained to exercise independent professional judgment. Therefore, recommendations to registered IAs and BDs or corporate fiduciaries would not trigger Regulation BI. On the other hand, recommendations to non-professional trustees, executors, conservators and persons holding power of attorney that represent natural persons are covered. The definition does not apply to financial industry professionals.

Material facts (under Regulation BI): Information is material if there is a substantial likelihood that a reasonable shareholder would consider it important.

Monitoring accounts: An agreement between the BD and the customer to provide account monitoring services. Monitoring may be incidental reviews of accounts to make recommendations and does not require IA registration. Through Form CRS firms are required to advise customers if they provide account monitoring services. BDs do not have a duty to provide account monitoring.

Non-cash compensation: Non-cash compensation includes any form of compensation, including but not limited to merchandise, gifts and prizes, travel expenses, meals and lodging.

Personal, family, or household purposes: The phrase "primarily for personal, family or household purposes" covers any recommendation to a natural person for his or her account, other than recommendations to a natural person seeking these services for commercial or business purposes. Regulation BI would not cover, for example, an employee seeking services for an employer or an individual seeking services for a small business or on behalf of another non-natural person entity, such as a charitable trust.

Receives and Uses: The SEC has stated that "use" means when, as a result of the recommendation: (a) the retail customer opens a brokerage account with the BD regardless of whether the BD receives compensation; (b) the retail customer has an existing account with the BD and receives a recommendation from the BD, regardless of whether the BD receives or will receive compensation, directly or indirectly, as a result of the recommendation; or (c) the BD receives or will receive compensation, directly or indirectly, as a result of that recommendation even if that retail customer does not have an account at the firm.

Recommendation: Interpreted in a manner consistent with current BD regulation under federal securities laws and FINRA rules.

Relationship summary: A written disclosure statement (Form CRS) that must be provided to retail investors when a recommendation is made (as defined in Reg BI).

Retail customer: A natural person (regardless of their financial status, including those previously qualifying as "institutional accounts" under FINRA's suitability rule) or the legal representative of such person who: (a) receives a recommendation for any securities transaction or investment strategy from a broker-dealer or associated person (whether or not the recommendation results in a securities transaction); and (b) uses the recommendation primarily for personal, family, or household purposes.

15.8 Cross References To Sections In This Manual

Subject	CHAPTER/Section
Suitability	<p>Sections in the following chapters:</p> <p>ORDERS CORPORATE FIXED INCOME SALES AND TRADING CORPORATE SECURITIES UNDERWRITING MUTUAL FUND AND OTHER INVESTMENT COMPANY PRODUCTS OPTIONS MUNICIPAL SECURITIES DIRECT PARTICIPATION PROGRAMS AND REITS BANK BROKER DEALERS INSURANCE PRODUCTS PRIVATE PLACEMENTS AND OFFERINGS</p>
Cash and Non-cash compensation	<p>ORDERS:</p> <ul style="list-style-type: none"> • Cash And Non-Cash Compensation Policy <p>CORPORATE SECURITIES UNDERWRITING</p> <ul style="list-style-type: none"> • Non-Cash Compensation <p>MUTUAL FUNDS</p> <ul style="list-style-type: none"> • Non-Cash Compensation <p>INSURANCE PRODUCTS</p> <ul style="list-style-type: none"> • Sales Guidelines
Sales contests, incentive programs	<p>ORDERS:</p> <ul style="list-style-type: none"> • Sales Contests <p>MUTUAL FUNDS</p> <ul style="list-style-type: none"> • Sales Contests And Incentive Programs

	MUNICIPAL SECURITIES <ul style="list-style-type: none">• Sales Contests
New Accounts	ACCOUNTS

16 INSURANCE PRODUCTS

This chapter describes policies and procedures that apply to the sale of insurance products.

16.1 Approved Insurance Products

RRs are permitted to sell only those products approved by the Insurance Department. The Insurance Department is responsible for evaluating and selecting products which may include, among other considerations:

- the insurance company's rating by a nationally recognized rating service
- when available, the number and substance of material complaints against the company and existence of criminal judgments against the company or its senior management
- availability of similar products from other insurance companies
- pricing of the product, including premium rates, compared with competitors' products
- sales support provided by the insurance company

The designated supervisor is responsible for reviewing proposed products and maintaining a record of information reviewed and approval of the product as well as the contract executed with the insurance company.

16.2 Licenses and Appointments

To offer insurance products, the RR must have a state license for the type of insurance product. The RR must also have a non-resident license for the customer's state of residence, if different from the RR's resident state. In addition, the RR must be "appointed" with the insurance company whose product is being sold.

An RR engaged in the sale of insurance products requires the following:

- Licensing with the state insurance regulator as an insurance agent for the type of insurance business (ordinary life, variable annuity, *etc.*). Some states require successful completion of an examination for the type of license requested.
- Licensing in the state where the RR resides as well as the state of domicile of the customer.

Appointment with the insurance company whose product is being sold. Insurance business cannot be dated prior to the RR's insurance company appointment in certain states.

☐ Continuing education, depending on the state where licensed.

RRs may not engage in the sale of insurance products or receive commissions from such sales unless properly licensed and appointed.

16.2.1 Requests for Licenses

RRs should contact the Insurance Department to request insurance licensing and appointment. The RR will be notified when insurance licenses are effective. Licenses are sent to the RR's home by the state licensing agency; a copy should be forwarded to the Insurance Department as soon as possible after receipt.

16.2.2 Non-Resident Licenses

There are some states where CIM is unable to conduct insurance sales activities. In other states, RRs may obtain non-resident licenses. The Insurance Department should be contacted to clarify requirements before offering insurance products to out-of-state customers.

16.2.3 Unsolicited Insurance Transactions

If an unlicensed RR receives an unsolicited order to purchase an insurance product, the transaction must be referred to a properly licensed insurance agent. Commissions will not be transferred to an unlicensed RR.

16.2.4 Additions to Existing Annuity Policies

If a customer wishes to make an additional contribution to an existing annuity policy, the RR must be licensed in the state where the customer currently resides.

16.3 Sales Guidelines

There are differences between insurance and securities products; it is important to understand these differences when discussing insurance products with customers. The following sections discuss sales guidelines for offering insurance products.

16.3.1 General Guidelines

- All insurance product purchases and sales **MUST** be conducted through CIM, *i.e.*, RRs are not permitted to accept any direct commission payments from insurance companies.
- Discussion of benefits of an insurance product should include disclosure of fees and charges.
- Focus on tax advantages must be balanced with disclosure of tax consequences.
- Avoid excessive focus on gross interest rate or investment performance rate without disclosure of product expense charges that serve to effectively reduce the return rate. Life insurance products may have significant front-end and/or back-end load structures; they are designed as long-term vehicles.
- Encourage customers to review their periodic statements received from the insurance company.
- Make a prior determination that a recommended purchase or sale of an insurance product is appropriate for the customer depending on the customer's financial circumstances and reasons for considering the insurance product.

16.3.2 Life Insurance and Other Non-Annuity Products

- Do not refer to life insurance as an "investment" or "investment product."
- One primary need satisfied by life insurance is providing death benefit protection (including income to heirs directly for day-to-day living expenses or providing funds to pay estate taxes).

Another use of life insurance is to accumulate cash value on a tax-advantaged basis.

- The RR should ensure the customer fully understands the difference between guaranteed and nonguaranteed elements of life insurance.

- Illustrations of return are projections only and not guaranteed.
- Positioning life insurance as a way to get tax-free income through policy cash value should be carefully evaluated. Other financial products may be a better source of tax advantaged cash flow.
- Life insurance purchased for pension or educational funding planning purposes must be disclosed as life insurance.
 - replacing an existing policy (or reducing its value to raise funds) to purchase a new policy must be considered carefully for its suitability and the costs that will be incurred by the customer. Refer to the section *Replacements* for the policies and procedures that apply to such transactions.

16.3.3 Annuities

- Some primary needs satisfied by annuities include tax deferral; providing income that cannot be outlived; and enhanced death benefit features.
- Annuities are designed for customers with long-term investment objectives, typically as a source of retirement income.
- Surrender charges and tax penalties generally make annuities unsuitable for short term investors. Customers should have adequate sources of liquidity apart from the money paid into the contract.
- While it may seem that most customers have a need for tax deferral, taxable investments may be more appropriate for customers in lower tax brackets, depending on the contract's mortality/expense fees and other charges.
- Guarantees on death benefits cannot be represented as applying to investment return or principal value of the account.
- Discussion of investment features and insurance features should be balanced, *i.e.*, do not neglect either feature.
- Illustrations of return are projections only and not guaranteed.
- Once a contract is annuitized, it is generally irreversible. Accordingly, there should be an income objective and no need for access to principal.
- Replacing an existing policy (or reducing its value to raise funds) to purchase a new policy must be considered carefully for its suitability and the costs that will be incurred by the customer. Refer to the section *Replacements* for the policies and procedures that apply to such transactions.

16.3.3.1 Equity-Indexed Annuities May Not Be Offered

[FINRA Notice to Members 05-50]

Insurance companies (and sometimes others) offer equity-indexed annuities (EIAs) which are financial instruments that generally offer a combination of interest income, some protection from loss of principal, and an opportunity to earn additional interest based on the performance of a securities market index. Some EIAs are registered securities and others are unregistered.

CIM does not offer Equity-Indexed Annuities (EIAs) and RRs are not permitted to offer them to customers or anyone else.

16.4 Sales to Military Personnel on Military Installations

[Military Personnel Financial Services Protection Act]

The following requirements and guidelines apply when offering life insurance products (including annuities) to military personnel and their dependents on military installations:
Referral fees upon securities sales or solicitations are prohibited unless the fee recipient is a licensed agent of the issuer of the policy or annuity.

- Life insurance products must not be marketed as investment products.
- Products that provide very low death benefits for very high premiums that are frontloaded in the first few years are inappropriate for most military personnel.
- Written disclosures must be provided that:
- state that the federal government provides subsidized life insurance to service members under the Servicemembers' Group Life Insurance (SGLI) program, and the amount and cost of the

SGLI coverage available; state that the federal government does not sanction, recommend, or encourage purchase of the life insurance product being sold;

- fully disclose any terms and circumstances under which amounts accumulated in a savings fund or savings feature under the life insurance product that is the subject of the disclosure may be diverted to pay, or reduced to offset, premiums due for continued coverage under the product;
- state that no one has received any referral fee or incentive compensation for offering to sell the product, unless the person is a licensed agent of the person issuing the product;
- are in plain and readily understandable language; and
- for sales or solicitations on federal land or facilities located outside the U. S., list the address and phone number at which consumer complaints are received by the state insurance regulator.

16.5 Purchases

The following is a summary of how insurance contracts are purchased and processed. Refer to the section *Replacements* for other procedures if the value of one policy is used to purchase a new policy.

16.5.1 Life Insurance and Other Non-Annuity Products

RRs may offer insurance products available from designated wholesalers. CIM must have a sales agreement with the insurance carrier prior to effecting sales. The RR may call approved wholesalers directly for the following:

- Quote on the requested product
- Appointment of the RR with the insurance company
- Applications and forms to purchase the policy
- Brochures on products available

16.5.2 Annuities

CIM must have a signed selling agreement with the insurance company to permit sales of products of that company. The Insurance Department should be contacted to obtain a list of approved insurance companies or verify whether a particular company has an agreement with CIM.

The following are steps for purchasing annuities:

- Both the customer and the RR must sign the application and the RR sends the application to the Insurance Department.
- The Insurance Department will review for availability of funds and required licensing and appointment of the RR.
- If funds are available and licensing/appointment is in effect, the customer's account at CIM will be debited and the proceeds wired to the individual insurance carrier.

16.6 Replacements

Responsibility	<input type="checkbox"/> VP – Insurance Products
Resources	<input type="checkbox"/> Insurance applications and order records Replacement Letters
Frequency	<input type="checkbox"/> Daily or as required
Action	<input type="checkbox"/> Review insurance transactions to identify potential replacements (Simultaneous or contemporaneous purchases and surrenders) <input type="checkbox"/> Require Replacement Letters where required <input type="checkbox"/> Review for patterns of an RR's customers exercising "free looks" or surrenders of contracts closely timed with the initial purchase <input type="checkbox"/> Identify RRs whose customers have a high rate of variable annuity replacements or rollovers and determine whether replacements or rollovers are appropriate for the customers <input type="checkbox"/> Conduct suitability review of each 1035 exchange effected by a customer buying an annuity contract considering the customer's age, the cost of the exchange, and what benefit the exchange is to the customer <input type="checkbox"/> Review proposed replacement and, if appropriate, sign Letter indicating approval <input type="checkbox"/> Notify RR the replacement was not approved and cancel purchase and sale, if necessary.
Record	<input type="checkbox"/> Replacement Letters are retained by the Insurance Department with records of the transaction.

The term "replacement" generally refers to the activity of a customer surrendering or altering existing insurance coverage in order to purchase a new insurance policy. Recommendation of a replacement should be suitable for the customer and justified based on the reasons for the replacement. Considerations include the age of the customer, the cost involved, and what benefit is derived from the replacement.

If the RR is aware of a replacement, certain procedures must be followed, as explained in the following sections.

16.6.1 Definition

Replacement occurs when an existing life insurance or annuity has been or is to be:

- Terminated;
- Converted to reduced paid-up insurance, continued as extended term insurance, or otherwise reduced in value by the use of nonforfeiture benefits or other policy values;
- Amended to effect either a reduction in benefits or in the term for which coverage would otherwise remain in force or for which benefits would be paid;

- Reissued with any reduction in cash value; or,
- Pledged as collateral or subjected to borrowing, whether in a single loan or under a schedule of borrowing over a period of time for amounts in the aggregate exceeding 25% of the loan value of the policy.

Common transactions that constitute replacements include Internal Revenue Code section 1035 exchanges; loans on existing life insurance policies used to fund new purchases; and note transactions involving the same insurer (commonly known as internal replacements), depending on state law.

16.6.2 Suitability of Replacements

The RR must have a reasonable basis for determining the suitability of recommending a replacement. A replacement may not be in the customer's best interest. For example, a customer may incur new fees, extended surrender charge periods, a possible higher insurance risk rating due to ill health, and new suicide and incontestability periods. There may also be unfavorable tax consequences. RRs should carefully consider whether a replacement is suitable for the customer and take into consideration the following:

Has surrender charge period in the old annuity expired?

- What is the composition of the customer's overall portfolio? Will a new variable annuity represent a significant asset in the portfolio?
- Will the customer need the money soon? What is the length of the surrender charge period in the new annuity? To what extent does the new annuity provide access to funds without penalty?
- Is disclosure to the customer clear that all investment risk in a variable contract is borne by the customer?
- What is the customer's age? Older customers may have greater liquidity need.

If new life insurance provides a higher death benefit for truly the same or lower premium cost than under old life insurance policy consider:

- Surrender charges, if any, under old policy
- Surrender charges, and duration, in new policy
- Imposition of new contestability/suicide period. Has there been a change in the customer's health?
- Premium payment period of new policy compared to old policy
- Possible variability of future premium payments

16.6.3 Replacement Procedures

If a replacement is to be effected, the RR must:

- Be appointed with the new insurance company and licensed in the state of the customer's residence prior to effecting the replacement.
- Complete the appropriate insurance original application.
- Check with the Insurance Department to determine whether the insurance carrier requires its own surrender form or state replacement form.
- Complete a state replacement form where required (check with the Insurance Department regarding states requiring their own replacement form).

- Obtain the surrendering carrier's original policy or complete a lost policy statement, signed by the customer.
- Complete CIM's Replacement Letter including signatures of the customer, the RR, and the RR's supervisor
- Send all original paperwork to the Insurance Department for processing.

16.6.4 1035 Exchanges

A 1035 Exchange refers to a section of the IRS Code that allows for the non-taxable exchange of nonqualified funds from one insurance carrier to another. The tax code states that the old insurance contract must be exchanged for a new contract; the policyholder cannot receive a check and apply the proceeds to the purchase of a new insurance or annuity contract. The tax code also states that the policyholder may make a tax-free exchange from: 1) a life insurance contract to another life insurance contract or an annuity contract, or 2) from one annuity contract to another annuity contract. 1035 exchanges are not allowed for liquidations from annuity contracts to purchase life insurance contracts.

When a customer exchanges an annuity or life insurance contract to purchase an annuity contract, in addition to the requirements listed in the prior section, a specific 1035 exchange form may be required. The Insurance Department should be contacted regarding questions on 1035 exchanges.

16.6.5 Prohibited Replacement Activities

- It is an unfair practice to persuade an insurance policyholder, through misrepresentation or improper recommendations, to cancel an existing policy and buy a new one ("twisting").

It is inappropriate to recommend the purchase of multiple insurance contracts, resulting in higher cost to the customer, when one contract will meet the customer's needs.