Exhibit GG.2

Security-Based Swap Data Repository Guidebook

Table of Contents

The protocol and standards for access to, and use of, the ICE SBSDR Service consist of, collectively, this Guidebook and all other documents incorporated by reference herein. Any Applicable Law affecting the (i) duties or obligations of ICE Trade Vault or (ii) the performance of any Participant shall take precedence over this Guidebook. In the event of a conflict between Applicable Law and this Guidebook, Applicable Law shall prevail.

This Guidebook shall be made publicly available on ICE Trade Vault's website (www.icetradevault.com) per Exchange Act Rule 907(c) and reviewed and updated as necessary at least once annually, with the date of last update and review reflected, in accordance with Exchange Act Rule 907(d).

Any compliance questions and concerns regarding ICE Trade Vault or the ICE SBSDR Service may be submitted to TradeVaultChiefComplianceOfficer@theice.com.

1 Key Terms and Definitions

1.1 Administrator: An individual designated by a Participant or Regulator as its administrator with respect to use of the System and Passwords.

1.2 Affiliate: A person that, directly or indirectly, Controls, is Controlled by, or is under common Control with ICE Trade Vault or a Participant, as the case may be.

1.3 Ancillary Services: All services offered by ICE Trade Vault that are not core SBSDR functions.

1.4 API: Application Programming Interface.

1.5 Applicable Law: Any and all applicable domestic and foreign governmental laws, rules and regulations (including but not limited to Applicable SEC Regulations), judicial orders or decisions, and interpretations and protocols, as amended from time to time.

1.6 Applicable SEC Regulations: Rules promulgated by the SEC that are applicable to the ICE SBSDR Service, including, but not limited to, rules pertaining to: Security-Based Swap Data Repository Registration, Duties, and Core Principles (including Exchange Act Rules 13n-1 through 13n-12) and Regulation SBSR – Reporting and Dissemination of Security-Based Swap Information (Exchange Act Rules 900 through 909).

1.7 Appropriate Domestic Regulator: Each appropriate U.S. prudential Regulator, the Financial Stability Oversight Council; the Commodity Futures Trading Commission; the Department of Justice; and any other person that the SEC determines to be appropriate, as the case may be.

1.8 Appropriate Foreign Regulator: Any non-U.S. person that the SEC determines to be appropriate, including any foreign financial supervisors (including foreign futures authorities); foreign central banks; and foreign ministries.

1.9 Board of Directors or Board: The board of directors of ICE Trade Vault.

1.10 Chief Compliance Officer or CCO: The person designated by the Board and identified on Form SDR to serve as the chief compliance officer of ICE Trade Vault.

1.11 Clearing Agency or CA: A person that is registered with the SEC as a clearing agency pursuant to Section 17A of the Exchange Act (15 U.S.C. 78q-1) and any rules or regulations thereunder.

1.12 Confidential Information: Includes, but is not limited to, Nonpublic Personal Information, trade information, Position data, material nonpublic information, trading strategies or portfolio Positions of any person.

1.13 Confirmed: ICE Trade Vault deems the trade information it receives in respect of a Security-based swap to be "Confirmed" if the Security-based swap has been: accepted by a Clearing Agency, executed on a Platform, deemed confirmed by an electronic confirmation service, or documented in a confirmation that has

been submitted to the System to evidence the terms that were agreed upon by the Counterparties.

1.14 Control (including the terms "controlled by" and "under common control with"): The possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise. A person is presumed to control another person if the person:

(i) Is a director, general partner, or officer exercising executive responsibility (or having similar status or functions);

(ii) Directly or indirectly has the right to vote 25 percent or more of a class of voting securities or has the power to sell or direct the sale of 25 percent or more of a class of voting securities; or

(iii) In the case of a partnership, has the right to receive, upon dissolution, or has contributed, 25 percent or more of the capital.

1.15 Counterparty: A person that is a direct counterparty or indirect counterparty of a Security-based swap.

1.16 Counterparty ID: The Unique Identification Code ("UIC") assigned to a Counterparty to a Security-based swap.

1.17 Direct Electronic Access: Access, which shall be in a form and manner acceptable to the SEC, to data stored by ICE Trade Vault in an electronic format and updated at the same time as ICE Trade Vault's data is updated so as to provide the SEC or any of its designees with the ability to query or analyze the data in the same manner that ICE Trade Vault can query or analyze the data.

1.18 Director: Any member of the Board or Directors.

1.19 Exchange Act: The U.S. Securities Exchange Act of 1934, as amended from time to time.

1.20 Form SDR: The application for registration with the SEC as an SBSDR, as such application is amended from time to time.

1.21 Historical Security-Based Swap: Any Pre-Enactment Security-Based Swap or Transitional Security-Based Swap.

1.22 ICE: Intercontinental Exchange, Inc., a publicly traded company.

1.23 ICE SBSDR Service: The SBSDR service offered by ICE Trade Vault.[1]

1.24 ICE Trade Vault: ICE Trade Vault, LLC.

[1] For clarity of purpose, the ICE eConfirm Service is an electronic platform for the matching of previously executed trades among counterparties and brokers. The ICE eConfirm Service is a distinct service and it is not part of the ICE SBSDR Service.

1.25 Life Cycle Event: With respect to a Security-based swap, any event that would result in a change in the information reported to a registered Security-based swap data repository under Exchange Act Rule 901(c), (d), or (i), including: an assignment or novation of the Security-based swap; a partial or full termination of the Security-based swap; a change in the cash flows originally reported; for a Security-based swap that is not a clearing transaction, any change to the title or date of any master agreement, collateral agreement, margin agreement, or any other agreement incorporated by reference into the Security-based swap contract; or a corporate action affecting a security or securities on which the Security-based swap is based (e.g., a merger, dividend, stock split, or bankruptcy). Notwithstanding the above, a life cycle event shall not include the expiration of the Security-based swap, a previously described and anticipated interest rate adjustment (such as a quarterly interest rate adjustment), or other event that does not result in any change to the terms of the Security-based swap.

1.26 Non-Mandatory Report: Any information provided to the ICE SBSDR Service by or on behalf of a Counterparty that is not required by Exchange Act Rules 900 through 909.

1.27 Nonpublic Personal Information: Includes (i) Personally Identifiable Information that is not publicly available information; and (ii) any list, description, or other grouping of market participants (and publicly available information pertaining to them) that is derived using Personally Identifiable Information that is not publicly available information.

1.28 Non-U.S. Person: A person that is not a U.S. person.

1.29 Participant: An entity that has validly enrolled to use the ICE SBSDR Service. A Participant may be:

(1) A Counterparty to a Security-based swap that is reported to ICE Trade Vault to satisfy an obligation under Exchange Act Rule 901(a) and that meets the criteria of Exchange Act Rule 908(b);

(2) A Platform that reports a Security-based swap to ICE Trade Vault to satisfy an obligation under Exchange Act Rule 901(a); or

(3) A Clearing Agency that reports a Security-based swap to ICE Trade Vault, whether or not it has accepted a Security-based swap for clearing pursuant to Exchange Act Rule 901(e)(1)(ii).

1.30 Parent: A legal person that controls a Participant.

1.31 Personally Identifiable Information: Any information: (i) that a Participant provides to ICE Trade Vault to obtain ICE SBSDR Service; (ii) about a Participant resulting from any transaction involving a service between ICE Trade Vault and the Participant; or (iii) ICE Trade Vault obtains about a Participant in connection with providing the ICE SBSDR Service to that market participant.

1.32 Platform: A national securities exchange or an SBSEF that is registered or exempt from registration.

1.33 Position: The gross and net notional amounts of open Security-based swap transactions aggregated by one or more attributes, including, but not limited to,

the (i) underlying instrument, index, or reference entity; (ii) Counterparty; (iii) asset class; (iv) long risk of the underlying instrument, index, or reference entity; and (v) short risk of the underlying instrument, index, or reference entity.

1.34 Pre-Enactment Security-Based Swap: A Security-based swap executed before July 21, 2010 (the date of enactment of the Dodd-Frank Act (Pub. L. No. 111-203, H.R. 4173)), the terms of which had not expired as of that date.

1.35 Product ID: The UIC assigned to a group of Security-based swap contracts each having the same material economic terms except those relating to price and size.

1.36 Public Data: SBSDR Information that ICE Trade Vault disseminates publicly pursuant to Applicable SEC Regulations.

1.37 Regulator: An Appropriate Domestic Regulator or an Appropriate Foreign Regulator, acting within the scope of its jurisdiction.

1.38 Reporting Side: The party to a Security-based swap identified in Exchange Act Rule 901(a)(2) as required to report the information specified in the Applicable SEC Regulations to a registered SBSDR, which includes a direct Counterparty to the Security-based swap and any guarantor of the direct Counterparty' obligations and, with respect to clearing transactions, the Clearing Agency.

1.39 SBSDR or Security-Based Swap Data Repository: A person that is registered with the SEC as a security-based swap data repository pursuant to section 13(n) of the Exchange Act (15 U.S.C. 78m(n)) and any rules or regulations thereunder.

1.40 SBSDR Information: Any information that ICE Trade Vault receives from Participants or maintains on their behalf as part of the ICE SBSDR Service.

1.41 SBSEF: A Security-based swap execution facility.

1.42 SEC: The U.S. Securities and Exchange Commission.

1.43 Security-based swap: A Security-based swap as defined from time to time by the SEC and the Commodity Futures Trading Commission.[2]

1.44 System: The ICE Trade Vault system as it may exist from time to time and any hardware, software, systems and/or communications links furnished by ICE Trade Vault to Participants from time to time.

1.45 Transaction ID: The UIC assigned to a specific Security-based swap transaction and used to identify that particular Security-based swap transaction throughout its existence.

1.46 Transitional Security-Based Swap: A Security-based swap executed on or after July 21, 2010, and before the first date on which trade-by-trade reporting of Security-based swaps in that asset class to a registered Security-based swap data repository is required pursuant to Exchange Act Rules 242.900 through 242.909.

[2] See the agencies' joint final rule, available at http://www.sec.gov/rules/final/2012/33-9338.pdf.

1.47 Unique Identification Code or UIC: A unique identification code assigned to a person, unit of a person, product, or transaction.

1.48 U.S. Person: Has the same meaning as in Exchange Act Rule 3a71-3(a)(4).

2 General Provisions

2.1 Overview of Regulatory Requirements

Section 13(m)(1)(G) of the Exchange Act requires that each Security-based swap (whether cleared or uncleared) be reported to a registered SBSDR. The fundamental purpose of an SBSDR is to provide transparency to the Security-based swaps market and publicly disseminate trade information. An SBSDR is required to register with the SEC, comply with all core principles applicable to an SBSDR under Applicable SEC Regulations and Applicable Law, meet compliance requirements by reporting primary SBSDR Information and secondary SBSDR Information of a Security-based swap transaction and reporting and recording Life Cycle Events related to that transaction, manage data reporting obligations, and maintain policies and procedures to ensure data security. An SBSDR also interacts directly with a range of market participants and is required to engage in the following core duties: (i) acceptance and confirmation of data; (ii) recordkeeping; (iii) public reporting; (iv) maintaining data privacy and integrity; and (v) permitting access to Regulators. In accordance with Exchange Act Rule 13n-8, ICE Trade Vault will report to the SEC information that the SEC determines to be appropriate to perform its duties. ICE Trade Vault, will upon request, provide to the SEC information or reports of the timeliness, accuracy, and completeness of data reported pursuant to Exchange Act Rule 900 through Rule 909.

2.2 System Availability and Support; Hours of Operation

In accordance with Exchange Act Rule 904(a)-(e), the ICE SBSDR Service shall continuously receive and disseminate SBSDR Information seven days per week, twenty-four hours per day. ICE Trade Vault reserves the right to take the services offline on an ad hoc basis between the hours of 9:00 PM ET and 11:59 PM ET on any weekday and from 9:00 PM ET on Friday through 7:00 PM ET on Sunday. ICE Trade Vault will, to the extent reasonably possible under the circumstances, provide Participants with advanced notice of any unavailability (for example, for scheduled maintenance), in accordance with Exchange Act Rule 904. All data submitted during System down time is stored and shall be processed and disseminated in accordance with Exchange Act Rule 902(a) once availability of the System and the ICE SBSDR Service has resumed. If, due to the nature of the downtime, the System was unable to receive and queue messages, ICE Trade Vault will immediately upon re-opening send a message to all Participants that it has resumed normal operations. Any Participant that had an obligation to report trade information to the ICE Trade Vault but could not do so during the downtime must promptly report the trade information to ICE Trade Vault.

The ICE Trade Vault help desk is available to receive customer calls in the United States from 8:00 AM ET to 6:00 PM ET, on all local business days, and in the United Kingdom from 8:00 AM GMT to 6:00 PM GMT, on all local business days. To reach the help desk, contact: TradeVaultSupport@theice.com or 1.770.738.2102.

2.3 Service, Commitment and Continuity

If ICE Trade Vault intends to cease operation of the ICE SBSDR Service for any reason, it shall notify all Participants using the ICE SBSDR Service at least three months in advance or, if ICE Trade Vault intends to cease operations in fewer than three months, as soon as practicable. In such event, in accordance with Applicable SEC Regulations, ICE Trade Vault will continue to

preserve, maintain, and make accessible the trade information and historical Positions in the manner, and for the duration, required by Applicable Law.

2.4 ICE SBSDR Service Pricing

In accordance with Exchange Act Rule 13n-4(c), any dues, fees or other charges imposed by, and any discounts or rebates offered by, ICE Trade Vault in connection with the ICE SBSDR Service and any other supplemental or ancillary services shall be (i) fair and reasonable and not unreasonably discriminatory and (ii) applied consistently across all similarly situated Participants. ICE Trade Vault dues, fees, other charges, discounts, or rebates shall be applied consistently across all similarly situated Participants. Please refer to "Exhibit M.2 - ICE Trade Vault SBSDR Pricing Schedule", available on the ICE Trade Vault website (www.icetradevault.com), for further details.

2.5 Emergency Authority

2.5.1 Authority

ICE Trade Vault is authorized to determine, in its sole discretion, whether an emergency exists with respect to, or otherwise threatens, the System or the ICE SBSDR Service (an "Emergency") and whether emergency action is warranted to mitigate such circumstances. ICE Trade Vault may also exercise emergency authority if ordered to do so by the SEC or other regulatory agency of competent jurisdiction.

2.5.2 Circumstances Requiring Invocation of Emergency Authority

Circumstances requiring the invocation of emergency authority include: (i) any occurrence or circumstance that ICE Trade Vault determines to constitute an Emergency; (ii) any "Physical Emergency" (such as a fire or other casualty, bomb threats, terrorist acts, substantial inclement weather, power failures, communications breakdowns, computer system breakdowns, or transportation breakdowns); (iii) any occurrence or circumstance that threatens or may threaten the proper functionality of the System or the ICE SBSDR Service; (iv) any occurrence or circumstance that may materially affect the performance of the System or the ICE SBSDR Service; (v) any action taken by any governmental body or any Regulator that may have a direct impact on the System or the ICE SBSDR Service; and (vi) any other circumstance that may impact ICE Trade Vault, the System or the ICE SBSDR Service in a materially adverse manner.

2.5.3 Emergency Authority Procedures

If the President of ICE Trade Vault, or any individual designated by the President or the Board of Directors, determines that an Emergency is likely to arise or has arisen, the President or such designee, as the case may be, may, consistent with conflict of interest policies detailed herein, declare an Emergency with respect to the System, the ICE SBSDR Service or the facilities of ICE Trade Vault and take or place into immediate effect a temporary emergency action or protocol. Any such action or protocol may remain in effect for up to 30 business days, after which time, and for each 30-business day period thereafter, it must be reissued by the Board of Directors to remain in effect. The CCO will be consulted in the event any emergency action or protocol may raise potential conflicts of interest. Any such action or protocol may provide for, or may authorize ICE Trade Vault, the Board of Directors or any committee thereof to undertake, actions deemed necessary or appropriate by the President or its designee to respond to the Emergency, including, but not limited to, the following:

- modifying or suspending any relevant provision of the Guidebook;

- changing the operating hours of the ICE SBSDR Service;
- temporarily limiting or denying access to the System or the ICE SBSDR Service; or
- requiring re-submission of any data lost or otherwise affected due to such Emergency.

Any such action placed into effect in accordance with the preceding paragraph may be reviewed by the Board of Directors at any time and may be revoked, suspended or modified by the Board of Directors.

If, in the judgment of the President of ICE Trade Vault, or any individual designated by the President and approved by the Board of Directors, the physical functions of the System are, or are threatened to be, materially adversely affected by a Physical Emergency, such person may take any action that he or she may deem necessary or appropriate to respond to such Physical Emergency, including preventing access to the System or suspending the ICE SBSDR Service.

In the event that any action has been taken pursuant to this Section 2.5, any person who is authorized to take such action may order the removal of any restriction ultimately imposed upon a determination by such person that the Emergency that gave rise to such restriction has sufficiently abated to permit the System and the ICE SBSDR Service to operate in an orderly manner; provided that any order pursuant to this paragraph will be subject to review, modification or reversal by the Board of Directors.

ICE Trade Vault will notify the SEC as soon as practicable of any action taken, or proposed to be taken (time permitting), pursuant to this Section 2.5.3. The decision-making process with respect to, and the reasons for, any such action will be recorded in writing. ICE Trade Vault will also notify Participants via email as soon as practicable of any action taken (time permitting), or proposed to be taken, pursuant to this Section 2.5.3.

2.6 Conflicts of Interest

2.6.1 Definitions

For purposes of this Section 2.6, the following definitions shall apply in addition to the key terms and definitions in Section 1:

The term “Family Relationship” shall mean the person's spouse, former spouse, parent, stepparent, child, stepchild, sibling, stepbrother, stepsister, grandparent, grandchild, uncle, aunt, nephew, niece or in-law.

The term “Named Party in Interest” shall mean a person or entity that is identified by name as a subject of any matter being considered by the Board of Directors or a committee thereof.

2.6.2 Prohibition

No member of the Board of Directors or of any committee thereof that has authority to take action for, and in the name of, ICE Trade Vault shall knowingly participate in such body's deliberations or voting in any matter involving a Named Party in Interest where such member (i) is a Named Party in Interest; (ii) is an employer, employee, or guarantor of a Named Party in Interest or an Affiliate thereof; (iii) has a Family Relationship with a Named Party in Interest; or (iv) has any other significant; ongoing business relationship with a Named Party in Interest or an Affiliate thereof.

2.6.3 Disclosure

Prior to consideration of any matter involving a Named Party in Interest, each member of the deliberating body shall disclose to the CCO, or his designee, the existence of any of the relationships listed in Section 2.6.2 with respect to such member with a Named Party in Interest.

2.6.4 Procedure and Determination

The CCO shall determine whether any member of the deliberating body is subject to a prohibition under Section 2.6.2. Such determination shall be based upon a review of the following information: (i) information provided by the member pursuant to Section 2.6.3, and (ii) any other source of information that is maintained by or reasonably available to ICE Trade Vault or the CCO.

3 Access, Connectivity and Use of Data

3.1 Fair and Open Access Policy

Consistent with Applicable Law, ICE Trade Vault provides access to the ICE SBSDR Service and to the data maintained by the ICE SBSDR Service on a fair, open and not unreasonably discriminatory basis. Access to, and usage of, the ICE SBSDR Service is available to all market participants that engage in Security-based swap transactions and to all market venues from which data can be submitted to the ICE SBSDR Service. Except for Ancillary Services that ICE Trade Vault is required to provide, access to, and use of, the ICE SBSDR Service does not require the use of any Ancillary Service offered by ICE Trade Vault

Participants shall only have access to their own data and data that ICE Trade Vault is required to disseminate publicly (i.e., Public Data).

3.1.1 Participant Access

Access to the ICE SBSDR Service is provided to parties that have a duly executed Participant Agreement in effect with ICE Trade Vault.

When enrolling with ICE Trade Vault, Participants must designate an Administrator with respect to Participant's use of the System. The Administrator will create, permission and maintain all user names and passwords for the Participant. Please refer to "Exhibit U.2 - ICE Trade Vault Security-Based SDR Participant Agreement" for further details.

3.1.2 Regulator Access

Any Regulator requiring or requesting initial access to the ICE SBSDR Service should contact the Chief Compliance Officer (via email: TradeVaultChiefComplianceOfficer@theice.com) to request access and the necessary documentation and certify that it is acting within the scope of its jurisdiction. ICE Trade Vault shall promptly notify the SEC regarding any request received from a Regulator for access to the Security-based swap data maintained by ICE Trade Vault.

Following notification to the SEC of the request for data access for a Regulator and due execution of necessary documentation, ICE Trade Vault shall provide access to the requested Security-based swap data consistent with Applicable Law. Each Regulator's designated Administrator will manage the Regulator's access to the ICE SBSDR Service. Such access may include, where applicable, proper tools for the monitoring, screening and analyzing of Security-based swap trade information, including, but not limited to, web-based services and services that provide automated transfer of data to Regulators. The ICE SBSDR Service shall provide Regulators the ability to view individual Participants' data and aggregated data sets.

In accordance with Exchange Act Rules 907(e) and 13n-8, ICE Trade Vault will provide reports evidencing the timeliness, accuracy, and completeness of data when requested by the Regulator.

3.2 Revocation of Access

Determinations to revoke access to the System, the ICE SBSDR Service or data maintained by ICE Trade Vault shall be made by the CCO. Unless circumstances require immediate action, prior to implementing a limitation or revocation of access to the System, the ICE SBSDR Service or SBSDR Information, the President and General Counsel of ICE Trade Vault shall review the basis for the limitation or revocation for compliance with Applicable Law, this

Guidebook and any other policies and procedures related to the ICE SBSDR Service, and the CCO shall provide notice to the Participant of such limitation or revocation.

If the President and General Counsel determine that revocation of access pursuant to this Section 3.2 is the result of unreasonable discrimination, the President and General Counsel shall take such actions as are necessary to restore access to such service or data.

3.3 Review of Revocation of Access

A party whose access has been revoked pursuant to Section 3.2 may seek reinstatement of access or modification of such revocation by submitting a petition for review ("Petition") to the President and General Counsel in such form and accompanied by such information as ICE Trade Vault may prescribe from time to time. Any such Petition shall be considered by the President and General Counsel and, thereafter, may be rejected or granted, in whole or in part, by the President and General Counsel, in their discretion, after review of the basis for revocation and the relevant Petition.

A Petition described in this Section 3.3 shall be reviewed by the President and General Counsel if submitted by the party seeking review promptly after the commencement of such revocation. The President and General Counsel may, in their discretion, review a Petition submitted after such a twenty-day period has elapsed.

A decision of the President and General Counsel ("Decision") concerning a Petition shall be issued promptly and shall constitute final action on the part of ICE Trade Vault.

3.4 Connectivity

Participants and Regulators may access the System through a web-based front-end that requires systems to (a) satisfy ICE Trade Vault minimum computing system and web browser requirements, (b) support HTTP 1.1 and 128-bit or stronger SSL data encryption, (c) the most recent version of Internet Explorer or Chrome, and (d) support the most recent version of Adobe Flash Player. The SEC may connect to the ICE SBSDR Service through Direct Electronic Access.

3.5 Use of Data

Access to SBSDR Information by ICE Trade Vault employees and others performing functions on behalf of ICE Trade Vault is strictly limited to those with the direct responsibility for supporting the System, the ICE SBSDR Service, Participants and Regulators. ICE Trade Vault employees and others performing functions on behalf of ICE Trade Vault are prohibited from using SBSDR Information other than in the performance of their job responsibilities.

In accordance with Applicable SEC Regulations, ICE Trade Vault may disclose, for commercial purposes, certain SBSDR Information. Any such disclosures shall be made solely on an aggregated basis in a manner that ensures that the disclosed SBSDR Information cannot reasonably be attributed to individual transactions or Participants.

4 Acceptance of Data and Reporting Procedures

4.1 Asset Classes

The ICE SBSDR Service accepts data in respect of all Security-based swap trades in the credit derivatives asset class and promptly records such data upon receipt.

4.2 Trade Data and Data Processing

4.2.1 General

Participants reporting trade information to the ICE SBSDR Service will be required to comply with reporting obligations under Applicable SEC Regulations and any other applicable reporting requirements promulgated from time to time by the SEC. In order to fulfill its obligations under Exchange Act Rule 13n-5(b)(1), ICE Trade Vault requires all Participants to report complete and accurate trade information and to review and resolve all error messages generated by the System.

4.2.2 Reporting Side

Exchange Act Rule 901 requires each Security-based swap, other than Security-based swaps executed on Platforms that will be submitted for clearing, to designate a Reporting Side, as determined by the hierarchy specified in Exchange Act Rule 901(a), to report certain information as required under Applicable SEC Regulations. The Reporting Side shall report primary trade information (set forth in Exchange Act Rule 901(c)), secondary trade information (set forth in Exchange Act Rule 901(d)) and Life Cycle Events (set forth in Exchange Act Rule 901(e)), each within the timeframe specified in the Applicable SEC Regulations. Primary trade information, secondary trade information, and Life Cycle Events are described in this Guidebook in further detail. A Platform on which a Security-based swap was executed and will be submitted to a Clearing Agency shall report to an SBSDR certain information as required under Applicable SEC Regulations.

A Platform and a Reporting Side (other than a Clearing Agency) that has a duty to report a Security-based swap that has been submitted to a Clearing Agency shall promptly provide that Clearing Agency with the Transaction ID of the submitted Security-based swap and the identity of the SBSDR to which the transaction will be reported.

For Security-based swaps not executed on a Platform and when both Counterparties have the same designation, these Counterparties must come to a mutual determination as to which Counterparty will serve as the Reporting Side.

In accordance with Exchange Act Rule 906(c), each Participant that is a Security-based swap dealer, Security-based major swap participant, Clearing Agency or Platform shall establish, maintain, and enforce written policies and procedures that are reasonably designed to ensure that it complies with any obligations to report information to the ICE SBSDR Service in a manner consistent with Applicable SEC Regulations. Each such Participant shall review and update its policies and procedures at least once annually in accordance with Exchange Act Rule 906(c).

4.2.3 Non-Reporting Side

The non-Reporting Side has an obligation to submit to the System any missing UIC information not provided by the Reporting Side. In accordance with Exchange Act Rule 906(a), ICE Trade Vault will generate a report whereby Participants are able to view trades missing UIC

information. ICE Trade Vault provides functionality allowing a Participant that is the non-Reporting Side to report missing UICs via a tab delimited file upload to ICE Trade Vault.

4.2.4 Required Submissions

4.2.4.1 Submission Methods

In accordance with Exchange Act Rules 901(h) and 907(a)(2), Participants must submit trade information in the data format required by ICE Trade Vault. The System will accept tab delimited file uploads via web access and API submissions in the Financial products Markup Language ("FpML") format. Information regarding FpML can be found on the website: http://www.fpml.org/. For the avoidance of doubt, only Participants may submit trade information to the System.

4.2.4.2 Primary Trade Information

In accordance with Exchange Act Rules 901(c) and 907(a)(1), Participants must report all primary trade information, and this information must be submitted to the System consistent with "Exhibit N.5 - ICE Trade Vault - SBSDR Fields and Validations ("Exhibit N.5")", which is publicly available at www.icetradevault.com.

Exhibit N.5 enumerates the required fields and acceptable values for the submission of trade information into the ICE Trade Vault System. The System will perform validations in accordance with Exhibit N.5 to ensure the trade information submitted adheres to the enumerated fields and values contained in this exhibit. For the submission of trade information that does not adhere to the standards enumerated in Exhibit N.5, the System will generate a corresponding error message for each invalid submission of trade information. The Reporting Side is required to properly amend and resubmit non-conforming trade information. In accordance with Exchange Act Rule 901(j), all primary and secondary trade information must be submitted within twenty-four hours after execution or submission of trade information to a Clearing Agency. Furthermore, ICE Trade Vault shall make systematically available standard data values as denoted in Exhibit N.5 to the SEC and Participants.

Primary trade information must be reported in accordance with the requirements of Exhibit N.5 and includes:

(1) The Product ID (or complete set of required underlying fields pursuant to Exhibit N.5); if the Security-based swap has no Product ID or the Product ID field does not include the following information, the Reporting Side shall report:

i. Information that identifies the Security-based swap, including the asset class of the Security-based swap and the specific underlying reference asset(s), reference issuer(s), or reference index;

ii. The effective date (the value submitted for this field cannot commence prior to the execution date);

iii. The scheduled termination date (the value submitted for this field cannot commence prior to the effective date);

iv. The terms for standardized fixed or floating rate payments, and the frequency of such payments; and

v. A flag indicating that the Security-based swap is customized and does not provide all of the material information necessary to identify such customized

Security-based swap or does not contain the data elements necessary to calculate the price.

(2) The execution date and time should be expressed using the Coordinated Universal Time format;

i. Compliance reporting will be based on the time zone selected by a Participant. As such, Participants should be observant of the time zone selected in the System in order to submit trade information with the appropriate value for the time zone that corresponds to the associated execution time.

ii. The value submitted for the execution time should use the ISO-8601 Standard.

iii. The value submitted for the execution time cannot be greater than the submission time.

(3) The price that includes the associated currency, and value of any up-front payments;

(4) The notional amount and associated currency;

(5) If the Counterparties to the Security-based swap include a registered Security-based swap dealer, an indication to that effect;

(6) Whether Counterparties intend that the Security-based swap to be submitted for clearing; and

(7) The flags listed in Section 4.7 ("Duty to Apply and Monitor Flags") of this Guidebook.

4.2.4.3 Secondary Trade Information

In accordance with Exchange Act Rules 901(d) and 907(a)(1), Participants must report secondary trade information. As with primary trade information, secondary trade information must be submitted pursuant to Exhibit N.5, and the System will perform validations based on Exhibit N.5 to ensure the secondary trade information submitted adheres to the enumerated fields and values contained in this exhibit. If submitted secondary trade information does not adhere to the standards enumerated in Exhibit N.5, the System will generate a corresponding error message for each invalid submission of secondary trade information. New data elements will be added via a System release, which will be announced to Participants and updated in Exhibit N.5. The Reporting Side is required to properly amend and resubmit non-conforming secondary trade information. In accordance with Exchange Act Rule 901(j), all primary and secondary trade information must be submitted within twenty-four hours after execution or submission of trade information to a Clearing Agency.

Secondary trade information must be reported in accordance with the requirements of Exhibit N-5 and includes, as applicable and to the extent not previously submitted as primary trade information:

(1) The Counterparty ID or the Execution Agent ID of each Counterparty;

(2) The Branch ID, Broker ID, Execution Agent ID, Trader ID, and Trading Desk ID of the direct Counterparty on the Reporting Side;

(3) The terms of any fixed or floating rate payments, or otherwise customized or non-standard payment streams, including the frequency and contingencies of any such payments;

(4) For a Security-based swap that is not a clearing transaction, the title and date of any master agreement, collateral agreement, margin agreement, or any other agreement incorporated by reference into the Security-based swap contract;

(5) Any additional data elements included in the agreement between the counterparties that are necessary for a person to determine the market value of the transaction;

(6) The name of the Clearing Agency to which the Security-based swap will be submitted for clearing;

(7) The direct Counterparties do not intend to submit the Security-based swap to clearing, whether they have invoked the exception in Section 3C(g) of the Exchange Act;

(8) If the direct Counterparties do not submit the Security-based swap to clearing, a description of the settlement terms, including whether the Security-based swap is cash-settled or physically settled, and the method for determining the settlement value; and

(9) The Platform ID, if applicable.

(10) The Security-based swap arises from the allocation, termination, novation, or assignment of one or more existing Security-based swaps, the Transaction ID of the allocated, terminated, assigned, or novated Security-based swap(s), except in the case of a clearing transaction that results from the netting or compression of other clearing transactions.

(11) To report trade allocations, Participants should submit the pre-allocated Security-based swap with the "Allocation Trade" field set to "Pre." Once the Security-based swap is allocated, the pre-allocation Security-based swap will be canceled upon the submission of the new post-allocation Security-based swaps which have the field "Allocation Trade" set to "Post." The submission of the new post-allocation Security-based swap will require the submission of the following fields: "Buyer or Seller Agent" information and the "Pre Allocation USI".

4.2.4.4 Historical Security-Based Swap Reporting

In accordance with Exchange Act Rule 901(i), Participants must submit a value of "Y" for the "Flag for Historical Security-Based Swap public dissemination exemption" field. Furthermore and as applicable, Participants should submit values "Y" or "N" for the "Flag for Historical Security-Based Swap Life Cycle Event public dissemination" field to update SBSDR Information associated with Historical Security-Based Swaps.

4.2.4.5 Exotic Security-Based Swap Reporting

ICE Trade Vault supports the reporting of highly customized and bespoke Security-based swaps which are commonly referred to as "exotic swaps". In order to support the reporting of exotic Security-based swaps, Participants are required to upload a file to the System that contains that trade information and the corresponding confirmed terms. For Security-based swaps that were executed as ad-hoc spread or package transactions, Participants should make best efforts to submit trade information in accordance with the appropriate product identifiers prior to submitting this information as exotic Security-based swaps. Specifically, Participants should attempt to separate the components of ad-hoc spread or package transaction before submitting this trade information to the System as an exotic Security-based swap.

4.2.4.6 Verification of Trade Data

Participants must verify that all trade information submitted to the ICE SBSDR Service is complete and accurate. If any trade information is found to be incorrect or incomplete, Participants must correct and resubmit such information to the System. For Security-based swaps that are not executed on a Platform, the Reporting Side should include the method used to confirm the trade information (e.g., "electronic confirmation service" or "paper confirmation"). Furthermore, Participants are required to warrant and represent that all trade information reported to the ICE SBSDR Service is complete and accurate. If the Counterparties to a Security-based swap use a paper confirmation to confirm the trade, ICE Trade Vault will require the Reporting Side to upload to the System a copy of the confirmation that was agreed upon by the Counterparties.

Clearing Agencies will access the ICE SBSDR Service to report Security-based swaps that have been accepted for clearing. For this reporting process, Counterparties will submit an over-the-counter Security-based swap ("alpha" Security-based swap) to a Clearing Agency to effectuate clearing. The Clearing Agency normally requires that alpha Security-based swaps be confirmed as a condition for clearing. Once the alpha Security-based swap has been accepted for clearing, this Security-based swap is novated into two new Security-based swaps ("beta" and "gamma" Security-based swaps) in which the Clearing Agency assumes its central Counterparty role. The Clearing Agency will report both the beta and gamma Security-based swaps to a SBSDR to discharge its reporting obligation. As part of the clearing process, the resulting beta and gamma Security-based swaps are confirmed by the Clearing Agencies.

Platforms will access the ICE SBSDR Service as Participants to report the relevant data with respect to Security-based swaps that were executed on or subject to the rules of their markets. As part of the execution process, the Security-based swaps are confirmed by Platforms.

4.2.4.7 Validation of Trade Data

Upon the receipt of a trade information for a Security-based swap, the System will perform validations on such information which includes validation that:

a. The submission file is in a valid format for receipt and processing;

b. All fields meet the required field format (e.g., number, date, date timestamp, free form text, or standard data value);

c. All Required and Conditionally Required fields are contained in the submission;

d. All Conditionally Required fields meet the validation standards; and

e. All Standard Data Value fields are provided with an acceptable value.

If the trade information fails any of the above validations, the System will generate an error message and give such information an "Invalid" status. Please reference Exhibit N.5 for a further description of the validation criteria.

4.2.4.8 Non-Mandatory Reports

In accordance with 907(a)(4), a Participant may report a Security-based swap as non-mandatory if it is the non-Reporting Side and the Reporting Side reported such a Security-based swap to an SBSDR other than ICE Trade Vault. In order to submit trade information to ICE Trade Vault as non-mandatory, Participants must submit a "Y" value in the "Non Mandatory Report" field and indicate the "First Reported SDR" for the Reporting Side submitted the Security-based swap.

4.2.4.9 Life Cycle Events

In accordance with Exchange Act Rule 901(e), Participants must submit all subsequent Life Cycle Events for previously submitted trade information to the System. Participants shall include the "Transaction ID" for the original trade in association with Life Cycle Events.

4.2.4.10 End-User Exception Data

In accordance with Exchange Act Rule 901(d)(7), if Counterparties do not intend to submit a mandatorily clearable Security-based swap to a Clearing Agency, Counterparties shall submit the trade information to the System with the appropriate information detailed in Exhibit N.5 and in accordance with Exchange Act Rule 3C(g). To effectively monitor trades where the end-user exception applies, the ICE SBSDR Service provides Regulators and Participants monitoring tools that denote where this exception has been invoked.

4.3 Security-Based Swap Status

Security-based swap status identifies the current reported state of a trade submitted to the ICE SBSDR Service:

- **CONFIRMED**: A cleared Security-based swap or an uncleared Security-based swap that the ICE SBSDR Service deems to be Confirmed.
- **CONFIRMED – VOLUNTARY**: A Confirmed Security-based swap that was submitted to the System by the non-Reporting Side in relation to a Non-Mandatory Report.
- **UNCONFIRMED**: An uncleared Security-based swap for which ICE Trade Vault has not received a supporting confirmation.
- **UNCONFIRMED – VOLUNTARY**: A Security-based swap that was submitted to the System by the non-Reporting Side in relation to a Non-Mandatory Report for which ICE Trade Vault has not received a supporting confirmation.
- **CANCELLED**: An Unconfirmed Security-based swap that has been rescinded or a Confirmed Security-based swap that has been early terminated, busted, or for which a full buyout or novation has been completed prior to the effective date of such Security-based swap.
- **ERRORED**: A Security-based swap that was erroneously reported to the ICE SBSDR Service and deemed to be submitted to System in error by the Participant.
- **INVALID**: A Security-based swap that failed the validation requirements of the System.

4.4 Life Cycle Event Status

In accordance with Exchange Act Rule 907(a)(3), Life Cycle Events shall be reported via the FpML protocol. The Life Cycle Event status identifies an action taken with respect to a trade submitted to the ICE SBSDR Service:

- **EARLY TERMINATED**: With respect to a Confirmed Security-based swap, where both Counterparties have confirmed the termination of such Security-based swap prior to its original termination date.

- **MODIFIED TERMS**: With respect to a Confirmed Security-based swap, where both Counterparties have confirmed the terms of such Security-based swap have been modified, including, but not limited to, a change in cash flows, a change in title and or date of the master agreement, or a corporate action that effects the economic terms of the Security-based swap.
- **NOVATED**: With respect to a Confirmed Security-based swap, where all parties have confirmed that the rights, liabilities, duties and obligations of the stepping-out party have been transferred to the stepping-in party.
- **ASSIGNMENT**: With respect to a Confirmed Security-based swap, where all parties have confirmed that the interest or benefit of the stepping-out party have been transferred to the stepping-in party, but not the obligations.
- **OPTION EXERCISED**: With respect to a Confirmed security-based swap option, where both Counterparties have confirmed the exercise of all or part of the option. This Life Cycle Event is only available for those options where automatic exercise is not applicable.

4.5 No Invalidation or Modification of Valid Security-Based Swap Data

In accordance with Exchange Act Rule 13n-5(b)(5), ICE Trade Vault maintains internal policies and procedures in place to ensure the recording process and operation of the ICE SBSDR Service does not invalidate or modify the terms of trade information. Furthermore, these controls are regularly audited to ensure the prevention of unauthorized and unsolicited changes to SBSDR Information maintained in the System through protections related to the processing of Security-based swaps.

4.6 Correction of Errors in SBSDR Information

In accordance with Exchange Act Rule 905(a), Participants are responsible for the timely resolution of errors contained in trade information that has been submitted to ICE Trade Vault. ICE Trade Vault provides Participants electronic methods to extract SBSDR Information for reconciliation purposes. If the non-Reporting Side discovers an error contained in the trade information submitted to the System on its behalf, that Counterparty shall promptly notify the Reporting Side of such error. If the Reporting Side discovers an error contained in the trade information that it previously submitted to the System, or receives notification from a Counterparty of an error, the Reporting Side shall promptly submit to the System amended trade information that remediates such error.

For Security-based swaps that are neither executed on a Platform nor submitted to a Clearing Agency, Counterparties shall resolve errors discovered in SBSDR Information in accordance with the Counterparties' master trading agreement and Applicable Law. Participants are required to promptly notify ICE Trade Vault of trade information that is submitted in error to the System. For a Security-based swap executed on a Platform that is subsequently submitted to a Clearing Agency, disputes must be resolved in accordance with the Platform's agreement and Applicable Law. The Platform is required to promptly notify ICE Trade Vault of any trade information submitted in error to the System. Disputes involving cleared transactions shall be resolved in accordance with the Clearing Agency's terms and Applicable Law. The Clearing Agency is required to promptly notify ICE Trade Vault of any trade information submitted in error to the System.

In accordance with Exchange Act Rule 905(b), the SBSDR, upon discovery of an error or receipt of notice of an error, will verify the accuracy of the terms of the Security-based swap and, following such verification, promptly correct the erroneous information regarding such Security-based swap contained in its system. ICE Trade Vault will disseminate a corrected transaction report in instances where the initial report included erroneous primary trade information.

4.6.1 Dispute Process

Participants are required to promptly notify ICE Trade Vault of trade Information that is disputed by the Counterparties to the trade. Participants shall utilize the "Dispute" functionality contained in the ICE SBSDR Service to do so. A Participant can dispute SBSDR Information stored in the System by populating a "Y" value in the "Dispute Status" field and populating its Counterparty ID in the "Disputing Party" field. The SBSDR Information associated with the Security-based swap will be deemed "Disputed" until such time that the Counterparty that initiated the dispute process submits a message to the System indicating that the SBSDR Information is no longer in dispute. ICE SBSDR Service will provide Regulators with reports identifying the SBSDR Information that is deemed disputed.

4.7 Duty to Apply and Monitor Flags

Consistent with the requirements of Exchange Act Rule 907(a)(3), ICE Trade Vault will apply submitted flags to trade information that is: (i) an error correction required to be disseminated by Exchange Act Rule 905(b)(2); or (ii) a Life Cycle Event, or any adjustment due to a Life Cycle Event, required to be disseminated by Exchange Act Rule 902(a). In addition Participants are required to apply certain flags with respect to primary trade information, and flags will be publicly disseminated if the Security-based swap is eligible for public dissemination. These flags are required as part of the trade information that is submitted to the System and are denoted with "Y/N" Boolean values. These flags address Security-based swap characteristics that may contribute to creating a distorted market view in accordance Exchange Act Rule 907(a)(4). Such flags include:

(1) A flag indicating that the Security-based swap is customized and does not provide all of the material information necessary to identify such customized Security-based swap or does not contain the data elements necessary to calculate the price;

(2) Flag indicating bespoke Security-based swap;

(3) Flag for late transaction report (more than twenty-four hours);

(4) Flag for inter-affiliate transaction;

(5) Flag for Security-based swap resulting from compression/netting;

(6) Flag for "forced trading session" conducted by a Clearing Agency;

(7) Flag for Security-based swap from the default for a clearing member;

(8) Flag for cross-border public dissemination exemption;

(9) Flag for Historical Security-based swap public dissemination exemption;

(10) Flag for Historical Security-based swap Life Cycle Event public dissemination;

(11) Flag for an allocation Security-based swap resulting from a bunched Security-based swap;

(12) Flag for package Security-based swap;

(13) Flag for prime broker Security-based swap;

(14) Flag to indicate a report is an error correction which is required to be publicly disseminated (Rule 907(a)(3)); and

(15) Flag for Security-based swap that is exempt from public dissemination in accordance with Exchange Act Rule 902(c).

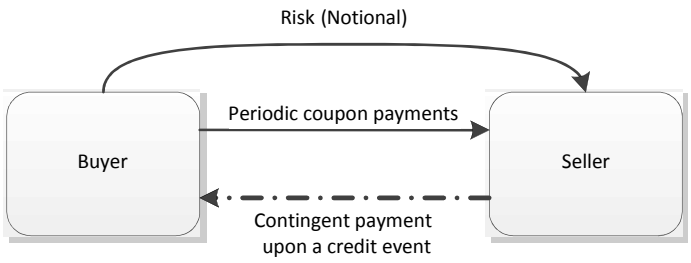
In accordance with Exchange Act Rule 901(c)(7), ICE Trade Vault will apply new flags as directed by the SEC. New flags will be recorded in the Guidebook.

4.8 Positions: Calculations and Reporting

The Position break out component of the ICE SBSDR Service will allow ICE Trade Vault to calculate open Positions for persons with open Security-based swaps for which ICE Trade Vault maintains records. Provisions in this Guidebook for Position break outs will be specified by product and comply with Applicable SEC Regulations.

ICE Trade Vault offers services as a registered SBSDR which require the calculation of Positions for Security-based swaps. As background, Position calculations are performed by market participants, Clearing Agencies and SBSDRs to aggregate and categorize Security-based swap transactions into exposures. Market convention is to define a taxonomy (see Section 6.5 of this Guidebook) for an asset class to facilitate the Position calculations. In general terms, a taxonomy defines the underlying transactions types associated with an asset class. Transactions types are furthered categorized into product definitions; a collection of fields that describe the attributes associated with a particular Security-based swap. Where possible, the taxonomy further defines acceptable data values and alpha/numerical formats that are acceptable for each field. The end result is a classification of financial instruments in a format that accurately represents risk exposures to a particular reference index or entity.

For example, a single-name credit default swap ("CDS") transaction specifies a reference entity, coupon, termination date, seniority, restructuring value, notional amount and notional currency. The buyer pays the seller quarterly payments calculated by multiplying the coupon by the notional amount. The quarterly payments continue until the CDS transaction reaches the termination date or the reference entity experiences a credit event (e.g., bankruptcy). If a credit event occurs, the seller is liable to the buyer for the full notional value minus the current market value of reference bond after factoring in the credit event - the recovery rate. The basic cash flows and risk transfer are outlined in the following diagram.



A Position consists of one or multiple single-name CDS transactions that share the same product attributes as defined by the taxonomy. Single-name CDS transactions on the same UPI

are aggregated and netted to calculate an overall Position for a Participant. Positions are measured by notional value for the credit asset class. Net buyers are indicated by a positive notional value and net sellers by a negative notional value. Two Positions (buyer and seller) are created for a single-name CDS transaction that is bilateral or uncleared. In the instance a single-name CDS transaction is cleared, four Positions are created to accurately represent the transaction: 1) client to clearing broker, 2) clearing broker to client, 3) clearing broker to Clearing Agency and 4) clearing house to clearing broker. For example, Dealer B enters into a bilateral single-name CDS contract against Dealer S on reference entity Corp. XYZ for a notional amount of $10 million. The two Positions are created to reflect this transaction and demonstrated in Table A (Alpha Security-based Swap Positions):

Table A (Alpha Security-based Swap Positions)

Trade	Position	Working Company	Counterparty	Product / Reference Entity	Buy Notional	Sell Notional	Net Notional
Alpha	1	Dealer B	Client S	Corp. XYZ	10	0	10
	2	Client S	Dealer B	Corp. XYZ	0	-10	-10

If the counterparties to the previous example agree to clear this transaction, the alpha Security-based swap is terminated and corresponding beta and gamma Security-based swaps are created to allow the Clearing Agency to assume its central Counterparty role. In most instances, one of the counterparties is not a member of the Clearing Agency and must use the services of a clearing broker and the other Counterparty is a Clearing Agency member. Two additional Positions are created between the Clearing Agency and the clearing broker to properly reflect this clearing arrangement as demonstrated in Table B (Beta and Gamma Security-based Swap Positions) - Dealer B is a clearing member of the Clearing Agency while Dealer S requires the services of a clearing broker. The net Positions for Dealer B and Dealer S remain unchanged from the original alpha Security-based swap; however, additional cleared Positions are created to represent the clearing relationships.

Table B (Beta and Gamma Security-based Swap Positions)

Trade	Position	Working Company	Counterparty	Product/ Reference Entity	Buy Notional	Sell Notional	Net Notional
Beta	3	Dealer B	Clearing Agency	Corp. XYZ	10	0	10
	4	Clearing Agency	Dealer B	Corp. XYZ	0	-10	-10
Gamma	5	Clearing Agency	Client S	Corp. XYZ	10	0	10
	6	Dealer S	Clearing Broker	Corp. XYZ	0	-10	-10

The Positions can also be demonstrated by removing the Counterparty level of granularity. Table C (Aggregated Positions) provides a rolled-up view of the Positions or net exposures.

Table C (Aggregated Positions)

Working Company	Product/ Reference Entity	Buy Notional	Sell Notional	Net Notional
Dealer B	Corp. XYZ	10	0	10
Clearing Agency	Corp. XYZ	10	-10	0
Dealer S	Corp. XYZ	0	-10	-10

4.9 Time-Stamp Requirements

In accordance with Exchange Act Rule 901(f) ICE SBSDR Service shall, time-stamp in real-time all Security-based swap transaction and pricing data with the date and time, to the nearest second, when such SBSDR Information is submitted to the System.

4.10 Missing UIC Information

In accordance with Exchange Act Rule 906(a), the Reporting Side is required to report its UIC information to the SBSDR. The Reporting Side may report the non-Reporting Side's UIC information, but is not required to do so. If the Reporting Side does not report the non-Reporting Side's UIC information, the Reporting Side must inform the non-Reporting Side that its trade information was reported to ICE Trade Vault without required UIC information. If the non-Reporting Side is not a Participant, the non-Reporting Side should contact ICE Trade Vault (ICETradeVaultSupport@theice.com) to register for access to the SBSDR Service and its trade information.

ICE Trade Vault shall identify in its records any Security-based swap reported to it for which ICE Trade Vault does not have required UIC information. In addition, once a day, ICE Trade Vault shall send a report to each Participant that is a Counterparty to a Security-based swap(s) that lacks required UIC information. A Participant that receives such a report shall provide the missing information with respect to its side of each Security-based swap referenced in the report to ICE Trade Vault within 24 hours.

5 Public Dissemination

In accordance with Exchange Act Rule 902(a), ICE Trade Vault shall publicly disseminate SBSDR Information, which shall include:

- Dissemination of data transaction report of a Security-based swap, which shall contain all of the primary transaction information;
- Dissemination of Life Cycle Event or adjustment due to Life Cycle Event; and
- Ability for the public, Participants and Regulators to download historical data.

In accordance with Exchange Act Rule 907(a)(3), ICE Trade Vault will generate a "Trade Report ID" for each public dissemination report. For previously reported disseminated reports, the previous "Trade Report ID" will be indicated on such a report.

5.1 No Advance Disclosure

In accordance with Exchange Act Rule 902(d), no Participant shall disclose any trade information required to be submitted to ICE Trade Vault prior to public dissemination of such information by ICE Trade Vault.

5.2 Errors and Omissions

Participants are required to promptly verify trade information submitted in respect of their transactions and promptly report any discrepancies in accordance with Section 4.6 of this Guidebook. Any errors or omissions in trade information that was publicly disseminated shall be corrected or canceled and immediately publicly disseminated; corrections will reference the previously disseminated report or information. The Reporting Side must verify corrected data with the non-Reporting Side.

5.3 Compliance with Public Dissemination Requirements

In accordance with Applicable SEC Regulations and required time delays, the System shall publicly disseminate Security-based swap transaction and pricing data immediately upon receipt. Public dissemination shall include flags and Life Cycle Events with reference to its previously disseminated transaction.

In accordance with Exchange Act Rule 902(c), ICE Trade Vault will not disseminate the following attributes contained in the SBSDR Information:

(1) The identity of any Counterparty;

(2) With respect to a Security-based swap that is submitted to a Clearing Agency, any information disclosing the business transactions and market positions;

(3) Any information reported pursuant to §242.901(i);

(4) Any Non-Mandatory Report;

(5) Any information that is required to be reported pursuant to §§242.901 and 242.908(a)(1) but is not required to be publicly disseminated pursuant to §242.908(a)(2);

(6) Any information regarding a clearing transaction that arises from the acceptance of a Security-based swap for clearing by a Clearing Agency or that results from netting other clearing transactions; or

(7) Any information regarding the allocation of a Security-based swap.

In accordance with 903(b) and when a transaction is publicly disseminated with a product code, the information necessary to interpret that code shall be made widely available.

6 Unique Identification Codes (UICs)

In accordance with Exchange Act Rule 903(a) and (b) and Exchange Act Rule 907(a)(5), ICE Trade Vault's methodology for assigning UICs is as follows:

1. Any SEC endorsed standard will be used, or in its absence;
2. Any CPMI-IOSCO endorsed standard will be used, or in its absence;
3. Any industry endorsed standard will be used, or in its absence;
4. ICE Trade Vault will generate and ID for the applicable UIC.

In accordance with 903(b), once a UIC is created in the SBSDR, a Participant may submit trade information with that UIC code. All trade information must be submitted consistent with the codes created in the SBSDR and as reflected in Exhibit N.5 (available at www.icetradevault.com); failure to do so will generate an error message and cause the information to be flagged with an "Invalid" status.

6.1 Transaction ID Methodology

In accordance with Exchange Act Rule 901(g), ICE Trade Vault's endorsed Transaction ID methodology is as follows:

(1) If a transaction is executed on a Platform, that Platform shall generate the Transaction ID.

(2) If a transaction is cleared, the Clearing Agency shall generate the Transaction IDs for the resulting cleared Security-based swaps.[3]

(3) If the transaction is executed off-Platform and is not cleared, the parties must mutually agree which side of the trade will be the Transaction ID generator.[4] When the Transaction ID generator is the Reporting Side, that party can request that ICE Trade Vault generate the Transaction ID on its behalf.

(4) For Historical Security-based swaps that have been reported in another jurisdiction, the Transaction ID assigned in that jurisdiction shall be used for reporting.

(5) For Historical Security-based swaps that have not been reported in another jurisdiction, the above methodology will be used.

(6) A multijurisdictional transaction should never have multiple Transaction IDs.

6.2 Counterparty IDs, Execution Agent IDs and Broker IDs

The SEC has recognized the Global LEI System administered by the Regulatory Oversight Committee ("ROC") as a standards-setting system with respect to the assignment of Counterparty IDs, and ICE Trade Vault shall accept LEIs for Counterparty IDs. All Participants,

[3] As described in 4.2.4.6 above, when a Security-based swap is submitted for clearing, it is novated into two new Security-based swaps ("beta" and "gamma" Security-based swaps) in which the Clearing Agency assumes its central counterparty role. The Clearing Agency will generate a Transaction ID for both the beta and gamma Security-based swaps.

[4] Parties may wish to consult ISDA's publication entitled "Unique Trade Identifier (UTI): Generation, Communication and Matching" and related materials, available at http://www2.isda.org/functional-areas/technology-infrastructure/data-and-reporting/identifiers/uti-usi/, for more information.

Execution Agents, and Brokers are required to register for an LEI for themselves. If a Counterparty is a non-Reporting Side and does not have an LEI, the Reporting Side must obtain an LEI for the non-Reporting Side as well and provide the LEI to ICE Trade Vault before reporting. If a Counterparty does not have an LEI at time of reporting, the Reporting Side must complete a document describing why they are reporting without an LEI. Please reference Exhibit U.4, ICE Trade Vault Non-Legal Entity Identifier Counterparty Setup Notification Request. If an invalid Counterparty ID, Execution Agent ID or Broker ID is entered, the System will send an error message to the Reporting Side and give such information an "Invalid" status.

6.3 Ultimate Parent/Affiliate Information

In accordance with Exchange Act Rules 906(b) and 907(a)(6), Participants, except for those that are Platforms or Clearing Agencies, shall provide information (e.g., Parent IDs and Counterparty IDs) to identify their ultimate Parent(s) and Affiliates. Participants shall promptly notify ICE Trade Vault of any changes to such information. Please refer to "U.5 - ICE Trade Vault - Ultimate Parent Affiliate Form" for further details.

6.4 Branch ID and Trading Desk ID

In order to receive a Branch ID or Trading Desk ID from the ICE SBSDR Service, Participants must submit the branch and desk information to ICE Trade Vault before reporting a Security-based swap. These IDs will be unique to ICE Trade Vault and will not apply across other SBSDRs. If in future an internationally recognized standards setting system emerges for assigning these UICs that meets the SEC's criteria, Participants will be required to obtain these IDs accordingly and supply them to ICE Trade Vault.

6.5 Unique Product ID

In accordance with Exchange Act Rule 907(a)(1) and 901(c)(1), the ICE SBSDR Service requires assignment of Product IDs to groups of Security-based swaps with the same material economic terms, other than those relating to price and size, to facilitate more efficient and accurate transaction reporting by allowing reporting of a single Product ID rather than the separate data categories. The ICE SBSDR Service shall issue Product IDs and maintain reference data representation for Security-based swaps via the System. This information shall include schema definitions and will be made publicly available on a non-fee basis at www.icetradevault.com. If the industry creates and adopts a Product ID taxonomy and registry, the ICE SBSDR Service shall comply with published standards at such time.

The ICE SBSDR Service will create Products based on an industry accepted UPI taxonomy or, where not available, its own product taxonomy. Participants may submit Product IDs or the underlying taxonomy fields. For example, for the Credit Asset Class (Single-Names), these fields include:

- **Classification**: References the high-level type of product.
- **Reference Entity Name:** The published index name or the underlying single obligor name protection is being bought or sold on.
- **Reference Entity Ticker:** This is a defined term in the 2003 ISDA Credit Derivatives Definitions.
- **Seniority:** Indicates the level of debt referenced in the CDS contract. The specific ISIN is not referenced.

- **Restructuring:** The Restructuring style indicated in the CDS contract defines what kind of debt restructuring triggers a credit event.
- **Scheduled Termination Month:** The termination month is one of the quarterly roll periods; June, December, March or September. The day of the month is predetermined as the 20th of each month.
- **Scheduled Termination Year**: The scheduled maturity year.
- **Coupon:** The standard coupon.
- **Notional Currency**: The standard ISO currency code.
- **Contract Type:** Designates the type of derivative (e.g., Security-based swap, option).

6.5.1 Creating New Product IDs

Participants shall notify the ICE SBSDR Service of any new Security-based swap products they intend to report to ICE Trade Vault by submitting the relevant product information to: ICETradeVaultSupport@theice.com. A complete list of available product information will be made available via link on the public dissemination section of the ICE Trade Vault website (www.icetradevault.com).

If a Product ID is not yet established, the trade information submission will fail the validations performed by the System. If a submission fails based on lack of product information, the Participant submitting the product information will receive an error message, and the ICE SBSDR Service will evaluate the taxonomy submitted and create a Product ID if applicable. The Reporting Side will subsequently be able to update and re-submit a valid Product ID.

7 Data Retention; Business Continuity

7.1 Data Retention, Access and Recordkeeping

Trade information submitted to ICE Trade Vault is saved in a non-rewriteable, non-erasable format, to a redundant, local database and a remote disaster recovery database in near real-time. The database of trade information submitted to ICE Trade Vault is backed-up to tape daily with tapes moved offsite weekly.

Participants' individual trade information records remain available to Participants and Regulators at no charge for online access from the date of submission until five years after expiration of the transaction. During this time period, trade information submitted to ICE Trade Vault will be available to Regulators via Direct Electronic Access.

Nothing in this Section 7.1 shall require a Participant to pay fees associated with ICE Trade Vault's standard regulatory reporting and access obligations. However, if a Participant or its Regulator requests or requires archived trade information from ICE Trade Vault to be delivered other than via the web-based front-end or the API or in a non-standard format, such Participant may be required, in accordance with the ICE Trade Vault schedule of fees and charges, to reimburse ICE Trade Vault for its reasonable expenses in producing data in response to such request or requirement as such expenses are incurred. Similarly, ICE Trade Vault may require a Participant to pay all reasonable expenses associated with producing records relating to its transactions pursuant to a court order or other legal process, as those expenses are incurred by ICE Trade Vault, whether such production is required at the instance of such Participant or at the instance of another party with authority to compel ICE Trade Vault to produce such records.

ICE Trade Vault may retain copies of communications between officers, employees or agents of ICE Trade Vault, on the one hand, and Participants, on the other hand, in such manner and for such periods of time as ICE Trade Vault may deem necessary and appropriate to comply with Applicable SEC Regulations.

Further, in accordance with Exchange Act Rule 13n-7(b), ICE Trade Vault shall maintain, for a period of not less than five years, the first two years in a place that is immediately available to representatives of the SEC, at least one copy of the written policies and procedures, including the code of ethics and conflicts of interest policies adopted in furtherance of compliance with the Exchange Act and Applicable SEC Regulations and correspondence, memoranda, papers, books, notices, accounts, and such other records as ICE Trade Vault may have created or received in the course of conducting the ICE SBSDR Service.

7.2 Business Continuity and Disaster Recovery

ICE Trade Vault has implemented systems and procedures that allow for timely resumption of key business processes and operations following unplanned interruptions, unavailability of staff, inaccessibility of facilities, and disruption or disastrous loss to one or more of ICE Trade Vault's facilities or services. All production system hardware and software is replicated in near real-time at a geographically and vendor-diverse disaster recovery site to avoid any loss of data.

ICE Trade Vault shall notify the SEC as soon as it is reasonably practicable of ICE Trade Vault's invocation of its emergency authority, any material business disruption, or any threat that actually or potentially jeopardizes automated system capacity, integrity, resiliency, availability or security.

8 Data Confidentiality; Sensitive Information and Security

ICE Trade Vault recognizes its responsibility to ensure data confidentiality and dedicates significant resources to information security to prevent the misappropriation or misuse of Confidential Information and any other SBSDR Information not subject to public dissemination (i.e., the information identified in Exchange Act Rule 902(c)). ICE Trade Vault does not, as a condition of accepting Security-based swap data from Participants, require the waiver of any privacy rights by such Participants.

ICE Trade Vault uses a multi-tiered firewall scheme to provide network segmentation and access control to its services. Firewalls are deployed in redundant pairs and employ stateful-inspection technology. ICE Trade Vault application servers are housed in a demilitarized zone behind external firewalls. A second set of internal firewalls further isolate ICE Trade Vault database systems, an intrusion system provides added security to detect any threats, and network sensors analyze all internet and private line traffic for malicious patterns.

Tactical controls are regularly examined and tested by multiple tiers of internal and external test groups, auditors and independently contracted third-party security testing firms. The controls impose an accountable and standard set of best practices to protect the confidentiality of Participants' trade information, including Confidential Information and other SBSDR Information not subject to public dissemination. ICE Trade Vault completes an audit for adherence to the data security policies on at least an annual basis. The audit tests the following applicable controls, among others, to ICE Trade Vault systems: (i) logical access controls; (ii) logical access to databases; (iii) physical and environmental controls; (iv) backup procedures; and (v) change management.