Swap Data Repository Rulebook

ICE Trade Vault

April 10, 2019[1]

Table of Contents

Key Terms & Definitions

- Ancillary Services: All services offered by ICE Trade Vault other than the ICE SDR Service.
- API: Application Programming Interface.
- Applicable CFTC Regulations: Rules promulgated by the CFTC that are applicable to the ICE SDR Service, including but not limited to rules pertaining to: Swap Data Repositories (17 CFR Part 49); Swap Data Recordkeeping and Reporting Requirements (17 CFR Part 45); Real-Time Public Reporting of Swap Transaction Data (17 CFR Part 43); Confirmation, Portfolio Reconciliation, and Portfolio Compression Requirements for Swap Dealers and Major Swap Participants (17 CFR Part 23); and End-User Exception to Mandatory Clearing of Swaps (17 CFR Part 39).
- Applicable Law: Any and all applicable domestic and foreign governmental laws and regulations (including but not limited to Applicable CFTC Regulations), judicial orders or decisions, and rules, regulations, interpretations and protocols, as amended from time to time.
- CEA: The Commodity Exchange Act, as amended from time to time.
- CFTC: The U.S. Commodity Futures Trading Commission.
- End-Users: Participants that rely on the end-user exception from mandatory clearing requirements under 17 CFR Part 39 of Applicable CFTC Regulations.
- ICE: IntercontinentalExchange, Inc., a publicly traded company.
- ICE eConfirm Service: The electronic platform utilized for (i) the matching and confirming of previously executed trades with other counterparties, and (ii) the matching of trade data with a third party broker responsible for arranging the trade.
- ICE Real-Time Ticker: An architectural component of the ICE SDR Service which will publicly disseminate trade data in real-time as prescribed by 17 CFR Part 43 of Applicable CFTC Regulations.
- ICE SDR Service: The regulated swap data repository ("SDR") service offered by ICE Trade Vault utilized for the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of swaps.
- ICE Trade Vault: ICE Trade Vault, LLC.
- Legal Entity Identifier ("LEI"): As defined in the Applicable CFTC Regulations, the assigned value used for unique identification of a counterparty to any swap.
- Non-Swap Dealer/Major Swap Participant ("Non-SD/MSP"): A Participant that is not classified as a Swap Dealer or a Major Swap Participant.
- Participant: An entity that has validly enrolled in the ICE SDR Service with ICE Trade Vault.
- Regulator: An Appropriate Domestic Regulator or an Appropriate Foreign Regulator, as defined in the Applicable CFTC Regulations, acting within the scope of its jurisdiction.

- SDR Information: As defined in the Applicable CFTC Regulations, any information that the ICE Trade Vault SDR receives from Participants or maintains on their behalf.
- Section 8 Material: As defined in the Applicable CFTC Regulations, the business transactions, trade data or market positions of any person and trade secrets or names of customers.
- Trusted Source: A Swap Execution Facility, a Designated Contract Market or a Derivatives Clearing Organization that has a duly executed user agreement in effect with ICE Trade Vault.
- Unique Product Identifier ("UPI"): As defined in the Applicable CFTC Regulations, the assigned value used for categorization of swaps with respect to the underlying products referenced therein.
- Unique Swap Identifier ("USI"): As defined in the Applicable CFTC Regulations, the value created and assigned to a swap and used to identify that particular swap transaction throughout its existence.

The following terms have the meanings set forth in the CEA and CFTC regulations, as amended from time to time: Appropriate Domestic Regulator; Appropriate Foreign Regulator; Derivatives Clearing Organization ("DCO"); Designated Contract Market ("DCM"); Eligible Contract Participant ("ECP"); Major Swap Participant: ("MSP"); Swap Data Repository ("SDR"); Swap Dealer ("SD"); and Swap Execution Facility ("SEF").

General Provisions

2.1 Governance

ICE Trade Vault, LLC, is organized as a limited liability company in the state of Delaware and is a wholly owned subsidiary of ICE.

ICE Trade Vault is governed by a minimum three-member Board of Directors ("Board of Directors"), of which at least one director shall be a "Public Director" as defined in the Applicable CFTC Regulations. The Board of Directors shall (i) be the governing body of ICE Trade Vault; (ii) designate and authorize specific appointed officers to act on behalf of the Board of Directors; (iii) fix, determine and levy all SDR fees, when necessary; (iv) make and amend the rules of the SDR; (v) have the power to act in emergencies; and (vi) delegate any such power to the appropriate party.

2.1.1 Chief Compliance Officer

The Chief Compliance Officer ("CCO") of ICE Trade Vault is appointed by, and reports directly to, the President of ICE Trade Vault. The Board of Directors approves the compensation of the CCO and meets with the CCO at least annually. The CCO also works directly with the Board of Directors in certain instances, for example, when resolving conflicts of interest. The CCO has supervisory authority over all staff acting at the direction of the CCO and his or her responsibilities include, but are not limited to: (i) preparing and signing a compliance report which shall be provided to the CFTC at least annually in accordance with CFTC regulations §§ 49.22(e) and (f); (ii) overseeing and reviewing ICE Trade Vault's compliance with Section 21 of the CEA and any related rules adopted by the CFTC (including reviewing ICE Trade Vault's compliance with Core Principles 2 ("Governance Arrangements") and 3 ("Conflicts of Interest") applicable to SDRs pursuant to CFTC regulations §§ 49.20(d) and 49.21(c) respectively); (iii) establishing and administering written policies and procedures reasonably designed to prevent violations of the CEA, the core principles applicable to SDRs and Applicable Law; (iv) in consultation with the Board of Directors, resolving any conflicts of interest that may arise including (a) conflicts between business considerations and compliance requirements; (b) conflicts between business considerations and the requirement that ICE Trade Vault provide fair and open access as set forth in CFTC regulation § 49.27; and (c) conflicts between ICE Trade Vault's management and members of the Board of Directors; (v) establishing and implementing procedures for the remediation of noncompliance issues; (vi) taking reasonable steps to ensure compliance with the CEA and Applicable CFTC Regulations relating to agreements, contracts, or transactions, and with CFTC regulations under Section 21 of the CEA, including confidentiality and indemnification agreements entered into with foreign or domestic regulators pursuant to Section 21(d) of the CEA; (vii) establishing procedures for the remediation of noncompliance issues identified by the CCO through a compliance office review, look-back, internal or external audit finding, self-reported error, or validated complaint; (viii) establishing and following appropriate procedures for the handling, management response, remediation, retesting, and closing of noncompliance issues; (ix) establishing and administering a written code of ethics designed to prevent ethical violations and to promote honesty and ethical conduct; and (x) ensuring ICE Trade Vault maintains sufficient information technology systems, staff and other resources to fulfill its duty to monitor, screen and analyze swap data in a manner consistent with CFTC regulations §§ 49.13 and 49.14.

Pursuant to CFTC regulation § 49.22, removal of the CCO requires the approval of the Board of Directors and notice to the CFTC of the CCO's removal within two business days of such removal. ICE Trade Vault shall further notify the CFTC within two business days of the appointment any new CCO, whether interim or permanent.

Any compliance questions and concerns regarding the ICE SDR Service may be submitted to TradeVaultChiefComplianceOfficer@theice.com.

2.2 Overview of Regulatory Requirements

The CEA requires that all swap transaction data, without exception, be reported to an SDR. The fundamental purpose of an SDR is to provide transparency to the swaps market and deliver real-time, public disclosure of transaction data. An SDR is required to register with the CFTC, comply with all core principles applicable to an SDR under Applicable CFTC Regulations and Applicable Law, meet compliance requirements by reporting economic terms of a swap transaction and reporting and recording lifecycle events related to that transaction, manage data reporting obligations, and maintain policies and procedures to ensure data security. An SDR 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) real-time reporting; (iv) monitoring, screening and analyzing data; (v) maintaining data privacy and integrity; and (vi) permitting access to regulators.

2.3 SDR Rules; Conflicts with Applicable Law

The rules of the ICE SDR Service consist of, collectively, this SDR Rulebook and all other documents incorporated by reference herein. Consistent with Applicable CFTC Regulations, ICE Trade Vault may voluntarily request that the CFTC approve any and all ICE SDR Service rules, or ICE Trade Vault may self-certify to the CFTC that present and/or future rules or rule amendments comply with the CEA and Applicable CFTC Regulations.

Any Applicable Law affecting the (i) duties or obligations of ICE Trade Vault or (ii) the performance of any Participant or Trusted Source shall take precedence over the rules of the ICE SDR Service. In the event of a conflict between Applicable Law and the rules of the ICE SDR Service, Applicable Law shall prevail.

2.4 System Availability and Support; Hours of Operation

The ICE SDR Service and ICE Real-Time Ticker Service are available seven days per week, 24 hours a day. ICE Trade Vault reserves the right to take the services offline, only if necessary, 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, if more extensive maintenance or upgrades are necessary. ICE Trade Vault will provide Participants with advanced notice of any scheduled maintenance in accordance with CFTC Regulation § 43.3(f)(3). All data submitted during system down time is stored and processed once the service has resumed.

The ICE Trade Vault help desk is available to receive customer calls in the United States from 8:30 AM ET to 6:30 PM ET, on all local business days, and in London from 9:00 AM GMT to 6:00 PM GMT, Monday through Friday, on all local business days. To reach the help desk, contact: TradeVaultSupport@theice.com or 1.770.738.2102.

2.5 Service, Commitment and Continuity

ICE Trade Vault shall notify all Participants and Trusted Sources using the ICE SDR Service of its intention to cease operation of the ICE SDR Service for any reason at least three months in advance or, if ICE Trade Vault intends to cease operations in less than three months, as soon as practicable.

2.6 Insurance

ICE Trade Vault maintains and will continue to maintain in force business liability coverage in the minimum amount of $10 million for each and every claim and in the annual aggregate, to protect

itself from a claim due to negligence on its part relating to the ICE SDR Service. ICE Trade Vault will provide, upon request by a Participant or Trusted Source, a certificate of insurance evidencing the insurance requirements have been satisfied and will provide Participants and Trusted Sources 30 days' advance notice of any cancellation or material reduction in coverage.

2.7 ICE SDR Service Pricing

In accordance with CFTC Regulation § 49.27(b), any fees or charges imposed by ICE Trade Vault in connection with the ICE SDR Service shall be equitable and established in a uniform and non-discriminatory manner. Fees or charges shall not be used as an artificial barrier to access to the ICE SDR Service. ICE Trade Vault shall not offer preferential pricing arrangements for the ICE SDR Service to any market participant on any basis, including volume discounts or reductions unless such discounts or reductions apply to all market participants uniformly and are not otherwise established in a manner that would effectively limit the application of such discount or reduction to a select number of market participants.

2.8 Emergency Authority

2.8.1 Authority

ICE Trade Vault is authorized to determine, in its sole discretion, whether an emergency exists with respect to or otherwise threatens the ICE SDR 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 CFTC or other regulatory agency of competent jurisdiction.

2.8.2 Circumstances Requiring Invocation of Emergency Authority

Circumstances requiring the invocation of emergency authority include: (i) any occurrence or circumstance which 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 which threatens or may threaten the proper functionality of the ICE SDR Service; (iv) any occurrence or circumstance which may materially affect the performance of the ICE Trade Vault systems; (v) any action taken by any governmental body or any regulator, Trusted Source or Participant which may have a direct impact on the ICE Trade Vault systems; and (vi) any other circumstance which may impact ICE Trade Vault in a materially adverse manner.

2.8.3 Emergency Authority Procedures

If the President, or any individual designated by the President or the Board of Directors, determines that an Emergency 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 ICE SDR Service or the systems and facilities of ICE Trade Vault and take or place into immediate effect a temporary emergency action or rule. Any such rule may remain in effect for up to 30 business days, after which time it must be approved by the Board of Directors to remain in effect. The CCO will be consulted in the event any emergency action may raise potential conflicts of interest. Any such action or rule 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 ICE SDR Service rules;

- extending, limiting or changing the operating hours of the ICE SDR Service;
- temporarily limiting or denying access to the ICE SDR Service, including access to any relevant ICE Trade Vault system or facilities; 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, or any individual designated by the President and approved by the Board of Directors, the physical functions of the ICE SDR Service 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 suspending the ICE SDR Service.

In the event that any action has been taken pursuant to this Section 2.8, 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 ICE SDR 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.

In accordance with the requirements of CFTC regulation § 49.23(e), ICE Trade Vault will notify the CFTC as soon as practicable of any action taken, or proposed to be taken, pursuant to this rule. 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 and Trusted Sources via email as soon as practicable of any action taken, or proposed to be taken, pursuant to this rule.

2.9 Disciplinary Rules

2.9.1 Jurisdiction

ICE Trade Vault shall have the authority to conduct investigations and prosecute and impose sanctions for any violations of this Rulebook and Applicable Law ("Violations") committed by Participants and Trusted Sources as provided in this Section 2.9.

2.9.2 CCO Powers and Duties

The CCO is responsible for enforcing these disciplinary rules and he or she shall have the authority to inspect the books and records of all Participants or Trusted Sources that are reasonably relevant to any investigation carried out pursuant to this Rule 2.9. The CCO also has the authority to require any Participant or Trusted Source to appear before him or her to answer questions regarding alleged Violations. The CCO may also delegate such authority to ICE Trade Vault employees, including officers, and such other individuals (who possess the requisite independence) as ICE Trade Vault may hire on a contract basis.

The CCO shall conduct investigations of possible Violations, prepare written reports with respect to such investigations, furnish such reports to the Board of Directors and conduct the prosecution of such Violations.

If, in any case, the CCO (or another ICE Trade Vault employee designated for this purpose by ICE Trade Vault) concludes that a Violation may have occurred, he or she may:

- issue a warning letter to the Participant or Trusted Source informing it that there may have been a Violation and that such continued activity may result in disciplinary sanctions; or

- negotiate a written settlement agreement with the Participant or Trusted Source, whereby the Participant or Trusted Source, with or without admitting guilt, may agree to (i) a cease and desist order or a reprimand; (ii) a fine for each Violation plus the monetary value of any benefit received as a result of the Violation; and/or (iii) a suspension or revocation of SDR privileges or a termination of Participant or Trusted Source status.

Any settlement recommended by the CCO shall be subject to the approval of the Board of Directors and shall become final and effective pursuant to Rule 2.9.5.

2.9.3 Board of Directors' Disciplinary Authority

The Board of Directors shall have the power to direct that an investigation of any suspected Violation be conducted by the CCO and shall hear any matter referred to it by the CCO regarding a suspected Violation.

In any case where the Board of Directors concludes that a Violation has occurred, the Board of Directors shall advise the Participant or Trusted Source of that fact pursuant to Rule 2.9.4 and may: (i) refer or return the matter to the CCO with instructions for further investigation; (ii) approve a settlement agreement negotiated pursuant to this rule with such Participant or Trusted Source (which may provide for a penalty other than that recommended by the CCO); and/or (iii) issue charges that include, but are not limited to,

- a cease and desist order or a reprimand;
- a fine for each Violation plus the monetary value of any benefit received as a result of the Violation; and/or
- a suspension or revocation of SDR privileges or a termination of Participant or Trusted Source status.

2.9.4 Notice of Charges; Right to Hearing

Pursuant to instructions from the Board of Directors, the CCO shall serve a Notice of Charges (a "Notice") on the Participant or Trusted Source responsible for a Violation (the "Respondent"). Such Notice shall state: (i) the acts, practices or conduct in which the Respondent is charged; (ii) how such acts, practices or conduct constitute a Violation; (iii) that the Respondent is entitled, upon written request filed with ICE Trade Vault within twenty days of service of the Notice, to a formal hearing on the charges; (iv) that the failure of the Respondent to request a hearing within twenty days of service of the Notice, except for good cause shown, shall be deemed a waiver of its right to a hearing; (v) that the failure of the Respondent to file a written answer to the Notice with the CCO within twenty days of service of the Notice shall be deemed an admission of all of the acts, practices or conduct contained in the Notice; and (vi) that the failure of the Respondent to expressly deny a particular charge contained in the Notice shall be deemed an admission of such acts, practices or conduct.

Any hearing requested by Respondent shall be conducted pursuant to rules and procedures adopted by the Board of Directors, which, in the judgment of the Board of Directors, are sufficient to give such Respondent an opportunity to fully and fairly present to the Board of Directors the Respondent's case. No member of the hearing panel shall hear a matter in which that member, in the determination of the CCO, has a direct financial, personal or other interest in the matter under consideration.

2.9.5 Hearing on Penalty; Failure to Request Hearing Deemed Acceptance of Penalty.

In the event (i) the Respondent fails to file an answer or admits to or fails to deny any charge of a Violation contained in the Notice or (ii) after a hearing conducted pursuant to Rule 2.9.4 the Board

of Directors determines that any charged Violation did in fact occur with respect to a Respondent, the Board of Directors shall find the Respondent guilty of each such Violation and may impose a penalty for each such Violation. The CCO shall promptly notify the Respondent of any such penalty and of the Respondent's right to a hearing on the penalty. Failure to request a hearing on the penalty in a timely manner, absent good cause shown, shall be deemed to be acceptance of the penalty.

2.9.6 Liability for Expenses

In addition to any penalty which may be imposed upon a Respondent pursuant to Rule 2.9.5 a Respondent found to have committed a Violation may, in the discretion of the Board of Directors, be required to pay to ICE Trade Vault an amount equal to any and all out-of-pocket expenses incurred by ICE Trade Vault in connection with the prosecution of such Violations..

2.9.7 Effective Date of Penalties

If a Respondent enters into a settlement agreement, the terms of which have been approved by the Board of Directors, any penalty included as a part of such settlement agreement shall become final and effective on the date that the Board of Directors approves or enters into such settlement agreement.

Any decision (including any penalty) by the Board of Directors shall be the final decision of ICE Trade Vault and shall become effective fifteen days, or such longer time as the Board of Directors may specify, after a copy of the written decision of the Board of Directors has been served on the Respondent; *provided*, *however*, that in any case where the user has consented to the action taken and to the timing of its effectiveness, the Board of Directors may cause the decision involving any disciplinary action (including any penalty) to become effective prior to the end of the fifteen day period.

Any fine imposed by the Board of Directors shall be due and payable on the effective date of the decision imposing such fine (or on such later date as the Board of Directors may specify) and shall bear interest from such effective date until paid at a rate of LIBOR + 2%.

2.10 Conflicts of Interest

2.10.1 Definitions

For purposes of this Rule 2.10 the following definitions shall apply:

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.

2.10.2 Prohibition

No member of the Board of Directors or of any committee thereof which 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.

2.10.3 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, whether such member has one (1) of the relationships listed in Section 2.10.2 of this Rule with a Named Party in Interest.

2.10.4 Procedure and Determination

The CCO shall determine whether any member of the deliberating body is subject to a prohibition under Rule 2.10.2. Such determination shall be based upon a review of the following information: (i) information provided by the member pursuant to Rule 2.10.3, and (ii) any other source of information that is maintained by or reasonably available to ICE Trade Vault.

Access, Connectivity and Use of Data

3.1 Fair and Equal Access Policy

Consistent with Applicable Law, ICE Trade Vault provides access to the ICE SDR Service on a fair, open and equal basis. Access to, and usage of, the ICE SDR Service is available to all market participants that validly engage in swap transactions and does not require the use of any other service offered by ICE Trade Vault.

Access to ICE Trade Vault is strictly limited to users with valid permissions and security access. Participants shall only have access to their own data and data that ICE Trade Vault is required to make publicly available ("Public Data").

3.1.1 Participant and Trusted Source Access

Access to the ICE SDR Service is provided to parties that have a duly executed user agreement in effect with ICE Trade Vault.

When enrolling with ICE Trade Vault, Participants and Trusted Sources must designate a master user ("Administrator"). The Administrator will create, permission and maintain user IDs for their firm with regards to accessing the user interface (UI). Application Program Interface (API) user IDs may be requested from ICE Trade Vault at tradevaultsupport@theice.com. Production user IDs for the APIs will be provided once the Participant has completed the applicable conformance testing plan within an ICE Trade Vault test environment.

3.1.2 Public Access

Public users will have the ability to access the ICE Trade Vault website and view Public Data in accordance with Part 43 of Applicable CFTC Regulations at www.icetradevault.com.

3.1.3 Regulator Access

Any Regulator requiring or requesting access to the ICE SDR 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 CFTC regarding any request received from a Regulator for access to the swap data maintained by ICE Trade Vault.

Following notification to the CFTC of the request for data access for a Regulator and due execution of necessary documentation, ICE Trade Vault shall provide access to the requested swap data consistent with Applicable CFTC Regulations. Each Regulator's designated master user ("Regulator Administrator") will manage the Regulator's user access to the ICE SDR Service. Such access may include, where applicable, proper tools for the monitoring, screening and analyzing of swap transaction data, including, but not limited to, web-based services and services

that provide automated transfer of data to Regulators. The ICE SDR Service shall provide Regulators the ability to view individual Participants' data and aggregated data sets.

Consistent with CFTC regulation § 49.18, a Regulator will be required to execute a written agreement stating that the Regulator shall abide by the confidentiality requirements described in Section 8 of the CEA relating to the swap data that is provided prior to the Regulator's receipt of any requested data or information. In addition each such regulator shall agree to indemnify ICE Trade Vault and the CFTC for any expenses arising from litigation relating to the information provided under Section 8 of the CEA.

3.1.4 Third-Party Reporters

All third-party reporters of ICE Trade Vault will be subject to the following conditions:

(1) The third party service provider must agree to strict confidentiality obligations and procedures that protect data and information from improper disclosure; and

(2) Prior to swap data access, the third-party service provider would be required to execute a confidentiality agreement setting forth minimum confidentiality obligations with respect to the information maintained by ICE Trade Vault that are equivalent to the privacy procedures for swap data repositories outlined in Applicable CFTC Regulations.

3.2 Revocation of Access

Prior to implementing a limitation or revocation of a Participant's or Trusted Source's access to the ICE SDR Service or data maintained by ICE Trade Vault, the CCO shall review the basis for the limitation or revocation for compliance with Applicable Law and the rules of the ICE SDR Service, and provide advance notice to the Participant or Trusted Source of such limitation or revocation. If the CCO determines that a Participant or Trusted Source has been discriminated against unfairly, the CCO shall take such actions as are necessary to restore that Participant's or Trusted Source's access to such service or data.

3.3 Reinstatement of Suspended User; Revocation or Modification of Other Actions; Termination of Status

A Participant or Trusted Source that has been suspended pursuant to Rule 3.2 may seek reinstatement, revocation or modification of such action by submitting an application to the Board of Directors in such form and accompanied by such information as ICE Trade Vault may prescribe. Such application may be rejected or granted in whole or in part by the Board of Directors in its discretion. If a Participant or Trusted Source that has been so suspended does not appeal within twenty (20) days after the commencement of such suspension, or if such Participant or Trusted Source shall have so applied and the Board of Directors shall have rejected the application, the Board of Directors may terminate such Participant's or Trusted Source's status after giving such user notice and an opportunity to be heard at a hearing before the Board of Directors. Any such hearing shall be conducted pursuant to rules and procedures adopted by the Board of Directors which, in the judgment of the Board of Directors, are sufficient to give such user an opportunity to fully and fairly present to the Board of Directors the user's reasons why the application should be granted.

3.4 Connectivity

Participants, Trusted Sources and Regulators may access the ICE SDR Service through a web-based front-end that requires user 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, and (c) support the most recent version of Adobe Flash Player. DCOs may connect to the ICE SDR Service through direct electronic access via an API.

3.5 Commercial and Non-Commercial Use of Data

Pursuant to Applicable CFTC Regulations, ICE Trade Vault and its affiliates are prohibited from using, for commercial or business purposes, swap data accepted and maintained by the ICE SDR Service without the express written consent of the Participant or Trusted Source submitting trade data. ICE Trade Vault employee access to SDR data is strictly limited to those with the direct responsibility for supporting Participants, Trusted Sources and Regulators, and ICE Trade Vault employees are prohibited from using SDR data other than in the performance of their job responsibilities.

ICE Trade Vault may disclose, for non-commercial purposes, certain swap data on an aggregated basis as long as the disclosed data cannot reasonably be attributed to individual transactions or Participants.

ICE Trade Vault offers its web-based front-end to enable Participants and Trusted Sources to report SDR data.).

Acceptance of Data and Reporting Procedures

4.1 Asset Classes

The ICE SDR Service accepts data in respect of all swap trades in the credit, commodities, interest rate and foreign exchange asset classes at this time.

4.2 Trade Data and Data Processing

4.2.1 General

Participants and Trusted Sources reporting trade data to the ICE SDR Service will be required to comply with Parts 43 and 45 of Applicable CFTC Regulations and any other applicable reporting requirements promulgated from time to time by the CFTC.

4.2.2 Reporting Entities and Trusted Sources

Part 45 of the Applicable CFTC Regulations will require each swap trade to designate a reporting entity for creation and continuation data as determined by the hierarchy defined in Part 45. Creation data includes both primary economic terms ("PET") data as well as confirmation data, both of which are described, together with continuation data, in further detail in Rule 4.2.3.

Accordingly, each Participant and Trusted Source utilizing the ICE SDR Service will be assigned a designation in order to apply the applicable reporting hierarchy for trade data and determine the reporting entity for creation and continuation data for each trade. When possible, ICE Trade Vault derives the reporting entity value based on the CFTC reporting entity hierarchy in §§ 45.3, 45.4 and 45.8 of the CFTC Regulations. For bilateral/non-cleared trades, when both the buyer and seller have the same designation, the parties must come to an agreement as to which party will be the reporting entity and either set up a default designation or manually enter a reporting party on the trade submission.

4.2.3 Required Submissions

4.2.3.1 Primary Economic Terms Data

Participants and Trusted Sources must report all primary economic terms of a swap, which include all of the terms of the swap verified or matched by the counterparties at or shortly after the execution of the swap, to the ICE SDR Service as soon as technologically practicable. For swaps

executed on a SEF or DCM, the primary economic terms of a swap are those terms specified in the contract listed on the platform. For non-standardized or bespoke swaps executed bilaterally, the primary economic terms of a swap are those essential economic terms, which may vary, and which counterparties verify following the execution of every swap.

ICE Trade Vault seeks to accept a primary economic term submission that may be amended by submissions to accommodate any updates or corrections. However, a primary economic term submission is required to conform to the relevant ICE Trade Vault UPI (until such time as the CFTC taxonomy for UPI is approved.) In the event that a party submits data with differing primary economic terms, ICE Trade Vault will consider this an update. ICE Trade Vault recognizes that reporting entities may need to update primary economic term submissions. However, disciplinary actions will be considered for excessive message updates not made in good faith by reporting entities.

4.2.3.2 Confirmation Data

Participants and DCOs must report all confirmation data for a swap to the ICE SDR Service as soon as technologically practicable. Confirmation data is the set of all terms matched and agreed upon by the counterparties in confirming the swap.

4.2.3.3 Continuation Data

Participants and DCOs must report all continuation data for swaps previously reported to the ICE SDR Service as soon as technologically practicable and as prescribed by Applicable CFTC Regulations. Continuation data is the set of data generated in connection with lifecycle events that occur prior to a swap's termination date and the data elements necessary to determine the current market value of a swap (i.e., valuation data). The term "lifecycle events" includes, but is not limited to trade cancellations (busted trades), modifications, novations and early terminations.

4.2.3.4 End-User Exception Data

Applicable CFTC Regulations require Participants relying on the end-user exception from mandatory clearing requirements under Part 39 of Applicable CFTC Regulations in respect of certain trades to report additional details about these trades to an SDR. To effectively monitor trades where the end-user exception has been invoked, the ICE SDR Service provides Regulators and Participants monitoring tools that show where the Part 39 requirements have been met or remain to be fulfilled.

4.2.4 Special Provisions for Block Trades

Applicable CFTC Regulations specify how to determine the appropriate minimum sizes for block trades and large notional swap transactions. SDRs are obligated to calculate appropriate block size minimums; formulae are prescribed in the Applicable CFTC Regulations for these calculations. ICE Trade Vault posts appropriate minimum block sizes to its website and shall annually recalculate and republish all block size minimums.

ICE Trade Vault shall handle block trades according to Applicable CFTC Regulations for real-time reporting and dissemination.

4.2.4.1 Exotic Trades

ICE Trade Vault supports an exotic trade schema for the submission of primary economic terms for exotic trades. For the commodities, interest rates and FX asset classes, Participants submit trade data to the ICE SDR Service and must indicate that the trade is "bespoke". . For the credit asset class, Participants may manually submit exotic trade details.

ICE Trade Vault's UPI taxonomy supports the reporting of bespoke products. This is not viewed the same as the reporting of an ad-hoc spread, where UPIs exist for the underlying individual legs of a transaction that does not have a UPI when reported as a spread. ICE Trade Vault does not accept ad-hoc spreads for primary economic term submissions or real-time reporting. In the case of ad-hoc spreads, the reporting counterparty to a swap transaction will be required to report the swap as separate legs to the corresponding ICE Trade Vault UPIs.

ICE Trade Vault supports the reporting of trades with variable economic terms, or shaped trade terms, where price, quantity, or other terms of the trade vary within a specified time period. As such, shaped trades are not considered exotic trades and should be reported with all variable economic terms defined within the trade submission and not as an exotic trade where the full trade terms are not captured.

Trade Status

Trade status identifies the current reported state of a trade submitted to the ICE SDR Service:

- **CONFIRMED**: A trade for which the Confirmation Data has been legally confirmed and automatically submitted to the ICE SDR Service by a DCO (in the case of cleared trades) or the ICE eConfirm Service (in the case of non-cleared trades).
- **CONFIRMED – VOLUNTARY**: A Confirmed trade that was submitted to the ICE SDR Service by a party that is not the reporting entity as part of a voluntary, supplemental report pursuant to CFTC regulation § 45.12.
- **pCONFIRMED**: An uncleared trade for which the Confirmation Data was submitted to the ICE SDR Service by the reporting entity rather than via the ICE eConfirm Service.
- **pCONFIRMED –VOLUNTARY**: A pConfirmed trade for which the Confirmation Data was submitted to the ICE SDR Service by a party that is not the reporting entity as part of a voluntary, supplemental report pursuant to CFTC regulation § 45.12.
- **UNCONFIRMED – PET ONLY**: A trade for which ICE Trade Vault has only received PET Data.
- **UNCONFIRMED – CONTINUATION ONLY**: A trade for which ICE Trade Vault has only received Continuation Data.
- **UNCONFIRMED – PET & CONTINUATION**: A trade for which ICE Trade Vault has received only PET Data and Continuation Data.
- **UNCONFIRMED – VOLUNTARY**: A trade that was submitted to the ICE SDR Service by a party that is not the reporting entity as part of a voluntary, supplemental report pursuant to CFTC regulation § 45.12 and for which ICE Trade Vault has only received either PET Data or Continuation Data.
- **CANCELLED**: An Unconfirmed trade that has been rescinded or a Confirmed trade that has been Busted or for which a full buyout or novation has been completed prior to its effective date. In addition, a cleared swap that has been converted into a related futures position.
- **ERRORED**: A swap that was erroneously reported to the ICE SDR Service and deemed to be submitted to System in error by the User.
- **INVALID**: A swap that failed the validation requirements of the System.

4.3 Lifecycle Event Status

Lifecycle Event status identifies an action taken with respect to a trade submitted to the ICE SDR Service:

- **BUSTED**: With respect to a Confirmed trade, where both counterparties have confirmed the rescission of such trade or completed a full buyout of such trade prior to its effective date. With respect to a pConfirmed trade, where one party to the trade has reported that both parties have rescinded such trade or completed a full buyout prior to the trade's effective date.
- **EARLY TERMINATED**: With respect to a Confirmed trade, where both counterparties have confirmed the termination of such trade prior to its original termination date. With respect to a pConfirmed trade, where one party to the trade has reported that both parties have terminated such trade prior to its original termination date.
- **MODIFIED TERMS**: With respect to a Confirmed trade, where both counterparties have confirmed the terms of such trade have been modified. With respect to a pConfirmed trade, where one party to the trade has reported that both parties have modified the terms of such trade.
- **NOVATED**: With respect to a Confirmed trade, 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. With respect to a pConfirmed trade, where one party to the trade has reported that all parties have confirmed that the rights, liabilities, duties and obligations of the stepping-out party have been transferred to the stepping-in party.
- **CLEARED NOVATION**: An original swap which has been accepted by the DCO for clearing as as such has been terminated.
- **DCO GIVEN-UP**: With respect to a non-cleared Confirmed trade, where both counterparties have confirmed that they have given up such trade for clearing. With respect to a non-cleared pConfirmed trade, where one party to the trade has reported that both parties have given up such trade for clearing.
- **OPTION EXERCISED**: With respect to a Confirmed option trade, where both counterparties have confirmed the exercise of all or part of the option. With respect to a pConfirmed option trade, where one party to the trade has reported that both parties have confirmed an exercise of all or part of the option. This Lifecycle Event is only available for those option and swaption trades where automatic exercise is not applicable.
- **EXCHANGE FOR RELATED POSITION ("EFRP")**: With respect to a Cleared trade, where the DCO has terminated the swap and exchanged the trade for a related futures position.
- **REQUEST TO CORRECT ERRORS (DISPUTED)**: Where one party to a Confirmed trade has reported a request to correct an error or omission in the matched trade terms of such trade.
- **REQUEST TO BUST**: Where one party to a Confirmed trade has reported a request to rescind such trade or complete a full buyout of such trade prior to its effective date.
- **REQUEST TO EARLY TERMINATE**: Where one party to a Confirmed trade has reported a request to terminate such trade prior to its original termination date.

- **REQUEST TO MODIFY TERMS**: Where one party to a Confirmed trade has reported a request to modify the terms of such trade.
- **REQUEST TO NOVATE**: Where one party to a Confirmed trade has reported a request to novate such trade.
- **REQUEST TO DCO GIVE-UP**: Where one party to a non-cleared Confirmed trade has reported a request to give-up such trade for clearing.
- **REQUEST TO OPTION EXERCISE**: Where one party to a Confirmed option trade has reported a request to exercise such option.

4.4 Verification of Accuracy for Data from Trusted Sources

The ICE SDR Service reasonably relies on the accuracy of trade data submitted from Trusted Sources where (i) the Trusted Source has validly enrolled with the ICE SDR Service, and (ii) the data submitted by the Trusted Source evidences that both counterparties agreed to the data. All Trusted Sources connecting to ICE Trade Vault must complete a conformance test to validate submission integrity prior to ICE Trade Vault's acceptance of actual swap data and must immediately inform ICE Trade Vault of any system or technical issues that may affect the accuracy of swap data transmissions. Notwithstanding this Rule 4.6, a Participant shall have a 48-hour period in accordance with CFTC regulation § 49.11(b) within which it may correct data reported to the ICE SDR Service from a Trusted Source, after which the Participant will be deemed to have acknowledged the accuracy of the swap data.

4.5 Verification of Single-Sided Trade Data

When a trade is not electronically matched, ICE Trade Vault must rely on the reporting entity to confirm the accuracy of the trade. Participants shall upload their side of the trade electronically to the ICE SDR Service, and certify that the swap creation and continuation data submitted is accurate and that the trade was confirmed via an alternative method by submitting a confirmation certification message. Submitting a confirmation certification message for the trade will cause the trade status to change to "pConfirmed." Following a lifecycle event or other circumstance requiring the submission of swap continuation data with respect to an existing trade, Participants shall certify that the swap continuation data submitted is accurate.

4.6 *No Invalidation or Modification of Valid Swap Data*

In accordance with CFTC regulation § 49.10(c), ICE Trade Vault has policies and procedures in place to ensure that the production environment in which the recording process of the ICE SDR Service operates does not invalidate or modify the terms of a valid swap. These controls are regularly audited and prevent any unauthorized, unsolicited changes to swap data submitted to ICE Trade Vault through system-wide protections related to the processing of data associated with the ICE SDR Service and ICE Trade Vault platform.

4.7 Correction of Errors in Trade Records; Dispute Resolution Process

Participants are responsible for the timely resolution of trade record errors and disputes. ICE Trade Vault provides Participants electronic methods to extract data for trade data reconciliation.

For discrepancies with trade data for cleared trades, Participants must report any errors to the relevant DCO, and trade records at ICE Trade Vault will only be adjusted when the DCO submits corrected trade data to the ICE SDR Service.

For discrepancies with trade data for bilateral/non-cleared trades, disputes must be resolved in accordance with the parties' agreement and Applicable Law, and Participants are required to

notify ICE Trade Vault promptly of disputed trade data by utilizing the "dispute" functionality of the ICE SDR Service. When a Participant "disputes" a trade within the ICE SDR Service, the status of the trade will be recorded as "Disputed", and notice of the dispute will be sent promptly to the other party to the trade. The trade record may then be amended or canceled upon mutual agreement of the parties. The status of the trade will remain "Disputed" until either party to the trade provides evidence satisfactory to ICE Trade Vault that the dispute has been resolved. All data provided to regulators will include the status of each trade reported to the ICE SDR Service, including a "Disputed" status.

4.8 Duty to Monitor, Screen and Analyze Swap Data

Consistent with the requirements of CFTC regulation §§ 49.13 and 49.14, ICE Trade Vault has the capacity to monitor, screen and analyze all swap data recorded as part of the ICE SDR Service in accordance with Applicable CFTC Regulations. In this regard the ICE SDR Service performs both (i) standard swap surveillance and (ii) specific tasks based on ad hoc requests of Regulators in a manner consistent with Applicable Law.

4.9 Position Limits: Calculations and Reporting

The position break out ("PBR") component of the ICE SDR Service will convert trade data into standard size positions or durations (e.g., convert a calendar transaction into 12 monthly trade records) for reporting and position limit assessment purposes. Rules for position break outs will be specified by product and comply with Applicable CFTC Regulations.

Real-Time Reporting

ICE Trade Vault provides real-time reporting and public dissemination of swap transaction data through the ICE Real-Time Ticker. The architecture of the ICE Real-Time Ticker is based on the requirements of Applicable CFTC Regulations. The ICE Real-Time Ticker provides the following functionality:

- Dissemination of initial swap transaction data;
- Dissemination of changes, corrections, and cancellations;
- Dissemination of transaction changes that materially impact economic terms;
- Dissemination of block or large notional value swaps with time delays that are applicable for each product;
- Ability to request and replay messages for a given day; and
- Ability for the public, Participants and Regulators to download historical data.

5.1 No Advance Disclosure

No swap transaction or pricing data will be disclosed to any market participant prior to public dissemination on the ICE Real-Time Ticker.

5.2 Errors and Omissions

Participants are required to promptly verify data submitted in respect of their trades and report any discrepancies in accordance with Section 4 of this Rulebook. Any errors or omissions in swap transaction and pricing data that were publicly disseminated in real-time will be corrected or canceled and publicly disseminated as soon as technologically practicable.

5.3 Compliance with Real-Time Dissemination Requirements

ICE Trade Vault shall publicly disseminate swap transaction and pricing data, in compliance with Applicable CFTC Regulations, as soon as technologically practicable upon receipt of such data, unless the data is subject to a time delay in accordance with Applicable CFTC Regulations.

5.4 Untimely Data

Pursuant to CFTC regulation § 49.15(c), ICE Trade Vault shall notify the CFTC of any swap transaction for which the real-time swap data is not received by the ICE SDR Service in accordance with the Real-Time Public Reporting requirements of Applicable CFTC Regulations.

5.5 Additional Time-Stamp Requirements

With respect to block trades and large notional swaps, ICE Trade Vault will, in accordance with Applicable CFTC Regulations, time-stamp in real-time all swap transaction and pricing data with the date and time, to the nearest second, when such swap data is received from a Participant or Trusted Source, and when such swap data is publicly disseminated.

Unique Identifiers

6.1 Unique Swap Identifiers (USIs)

Applicable CFTC Regulations state that USIs shall be assigned to a trade at the venue of execution.

For trades executed on a SEF or DCM (on-platform), responsibility for assigning USIs is placed on the SEF/DCM. The counterparties to these trades must provide the relevant USIs with their trade data submissions in order to allow ICE Trade Vault to tie out the primary economic terms received from SEFs with the more detailed confirmation terms that the parties submit to the ICE SDR Service.

For trades cleared on a DCO, responsibility for assigning USIs is placed on the DCO. The DCO has the responsibility to inform the counterparties of the trade of the USIs.

For trades that are not cleared or executed on a SEF or DCM (off-platform), the ICE SDR Service generates and assigns USIs when the reporting entity of PET data is a non-SD/MSP. When the PET data reporting entity is a SD or MSP, the reporting entity must generate the USI or elect the optional service for ICE Trade Vault to generate the USI on their behalf using their USI namespace. For Historical Swaps, ICE Trade Vault will generate the USI. ICE Trade Vault shall verify the uniqueness of such USIs in compliance with Applicable CFTC Regulations. In addition to creating and disseminating USIs for off-platform trades, ICE Trade Vault will track USIs for processing lifecycle events.

6.2 Legal Entity Identifiers (LEIs)

ICE Trade Vault has the ability to map entities to their assigned LEIs. This allows Participants to submit the entity name as stored in their system and map to the correct LEI.

6.3 Unique Product Identifiers (UPIs)

Applicable CFTC Regulations require UPIs to be created and processed in a centralized registry. ICE Trade Vault shall issue UPIs, maintain reference data representation of each commodity product, including schema definitions, and disseminate the representation to Participants. If the industry creates and adopts a UPI taxonomy and registry, ICE Trade Vault will comply with published standards at that time.

6.3.1 Creating New UPIs

Entities requesting new products must provide the new product specifications to ICE Trade Vault in order to receive a new UPI code and product schema.

Data Retention; Business Continuity

7.1 Data Retention, Access and Recordkeeping

ICE SDR Service data is saved to a redundant, local database and a remote disaster recovery database in near real-time. The ICE SDR Service database is backed-up to tape daily with tapes moved offsite weekly.

Participants' individual trade data records remain available to Participants and Regulators at no charge for online access through the ICE SDR Service from the date of submission until five years after the end date of the trade (last day of delivery or settlement as defined for each product). During this time period, ICE SDR Service data will be available to the Commission via real-time electronic access. After the initial five-year period, Participants' matched trade data will be stored off-line and remain available to Participants and Regulators, upon a three-day advance request to ICE Trade Vault, until ten years from the last date of delivery or pricing of a trade. Participant will retain unimpaired access to its online and archived matched trade data even in the event of Participant's discontinued use of the ICE SDR Service.

Nothing in this rule 7.1 will 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 data from ICE Trade Vault to be delivered other than via the web-based front-end or the API or in a non-standard format, Participant will 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.

ICE Trade Vault may retain copies of communications between officers, employees or agents of ICE Trade Vault, on one hand, and Participants and Trusted Sources (including related parties), 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 CFTC Regulations.

Further, in accordance with CFTC regulation § 49.22(g), ICE Trade Vault will maintain (i) a copy of the written policies and procedures, including the code of ethics and conflicts of interest policies adopted in furtherance of compliance with the CEA and Applicable CFTC Regulations; (ii) copies of all materials, including written reports provided to the Board of Directors or senior officers in connection with the review of the annual compliance report CFTC regulation § 49.22(f)(1) and the Board of Directors minutes or similar written record of such review, that record the submission of the annual compliance report to the Board of Directors or senior officer; and (iii) any records relevant ICE Trade Vault's annual compliance report, including, but not limited to, work papers and other documents that form the basis of the report, and memoranda, correspondence, other documents, and records that are: (A) created, sent or received in connection with the annual compliance report and (B) contain conclusions, opinions, analyses, or financial data related to the annual compliance report.

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.

The CFTC will be notified 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 operation, reliability, security or capacity in a material way.

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 Section 8 Material and any other SDR Information not subject to real-time reporting requirements pursuant CFTC regulation § 43. ICE Trade Vault does not, as a condition of accepting 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' sensitive data, including Section 8 Material and other SDR Information not subject to real-time reporting. ICE Trade Vault annually completes an audit for adherence to the data security policies. 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.

[1] This Swap Data Repository Rulebook was first adopted on June 6, 2012.

ICE Trade Vault Rulebook

Security-Based Swap Data Reporting Annex

Version: 1.0

February ■, 2021

Security-Based Swap Data Reporting (SBSDR) Annex

This SBSDR Annex will only apply to Users that have entered into the ICE Trade Vault Security-Based SDR User Agreement. This SBSDR Annex DOES NOT apply to and does not form part of the Rulebook applicable to any other entity.

ICE Trade Vault has submitted an application to register as a security-based swap data repository ("SBSDR") with the U.S. Securities and Exchange Commission (the "SEC"). Once ICE Trade Vault has been registered as an SBSDR, data with respect to Security-Based Swaps (as defined herein) can be reported to ICE Trade Vault for purposes of compliance with the reporting requirements established by the SEC.

The terms of this SBSDR Annex amend, supplement and form part of the Rulebook solely with respect to an entity that has entered into the ICE Trade Vault Security-Based SDR User Agreement, and solely with respect to such User's reporting of data with respect to Security-Based Swaps. Notwithstanding anything to the contrary in the Rulebook, in the event of any inconsistency between the terms of the Rulebook and the terms of this SBSDR Annex, this SBSDR Annex shall prevail with respect to Security-Based Swap data and the rights and obligations of the parties in respect thereof.

Unless otherwise specified in this SBSDR Annex, all capitalized terms used herein shall have the meanings defined in the Rulebook. All references in the Rulebook to a rule or regulation referenced below in column "A", shall refer to the corresponding SEC rule listed below in column "B".

A	B
Applicable CFTC Regulation **Rulebook Section Reference**	**Applicable SEC Regulations**
2.1.1 Chief Compliance Officer Compliance Report - CFTC regulations §§ 49.22(e) and (f)	Exchange Act Rules 13n-11(d), (e), and (g)
2.1.1. Chief Compliance Officer Governance Arrangements - Section 21 of the CEA and CFTC regulation §49.20(d), Core Principle 2	Exchange Act Rule 13n-4(c)(2)
2.1.1. Chief Compliance Officer Conflicts of Interest - CFTC regulation §49.21(c), Core Principle 3	Exchange Act Rule 13n-4(c)(3)
2.1.1. Chief Compliance Officer Data analysis requirements - CFTC regulations §§ 49.13 and 49.14	Exchange Act Rules 13n-4(b)(7) and 13n-5[1]

[1] *See* Appendix I for No-Action Relief from Exchange Act Rule13n-5(b)(1)(iii) stating that an SBSDR's failure to establish policies and procedures designed to satisfy itself of data completeness will not provide a basis for an enforcement action by the SEC.

A	B
Applicable CFTC Regulation Rulebook Section Reference	**Applicable SEC Regulations**
2.4. System Availability and Support; Hours of Operation CFTC regulation §43.3(f)(3)	Exchange Act Rule 904(b)
8 Data Confidentiality; Sensitive Information and Security CFTC regulation § 43	Exchange Act Rule 902(c)[2]

The following amends, supplements and forms part of the Rulebook as specified above.

1. **Key Terms and Definitions in the Rulebook shall be amended and supplemented as follows:**

Key Terms & Definitions

Administrator: An individual designated by a User, the SEC or Regulator as its administrator with respect to use of the System and passwords.

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.

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), Regulation SBSR – Reporting and Dissemination of Security-Based Swap Information (Exchange Act Rules 900 through 909), in each case, subject to the No-Action Relief.

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.

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.

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.

[2] *See* Appendix I for No-Action Relief from Exchange Act Rule 902 stating that public dissemination of Security-Based Swap transaction data in accordance with the CFTC rules will not provide a basis for an enforcement action by the SEC.

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.

Counterparty: A person that is a direct counterparty or indirect counterparty of a Security-Based Swap.

Counterparty ID: The Unique Identification Code ("UIC") assigned to a Counterparty to a Security-Based Swap.

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.

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

Execution Agent: Any person other than a broker or trader that facilitates the execution of a Security-Based Swap on behalf of a direct Counterparty.

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

GLEIF: Global Legal Entity Identifier Foundation.

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

ICE SBSDR Service: The SBSDR service offered by ICE Trade Vault.

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), and (i), each subject to the No-Action Relief, 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.[3]

No-Action Relief: The time-limited relief from (i) Security-Based Swap data reporting requirements and (ii) requirements of an SBSDR so long as it registered as a swap data repository with the CFTC, each contained in Cross-Border Application of Certain Security-Based Swap Requirements (Part X.C and Part X.D). The No-Action Relief is summarized in Appendix I to this SBSDR Annex.

[3] *See* Appendix I for No-Action Relief from Exchange Act Rule 901(e) stating that Users' omission to report Life Cycle Events that are not subject to reporting under the CFTC rules will not provide a basis for an enforcement action by the SEC.

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. The term Non-Mandatory Report does not include information that is subject to the No-Action Relief.

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.

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

Personally Identifiable Information: Any information: (i) that a User provides to ICE Trade Vault to obtain ICE SBSDR Service; (ii) about a User resulting from any transaction involving a service between ICE Trade Vault and the User; or (iii) ICE Trade Vault obtains about a User or a Counterparty on whose behalf the User reports a Security-Based Swap to ICE Trade Vault, in connection with providing the ICE SBSDR Service to that market participant.

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

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.

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.

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.

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

Reporting Side: The party to a Security-Based Swap identified in Exchange Act Rule 901(a)(2)[4] as required to report the information specified in the Applicable SEC Regulations to a registered SBSDR, which includes a direct Counterparty to a Security-Based Swap and, with respect to clearing transactions, the Clearing Agency.

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, subject to the No-Action Relief.

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

SBSEF: A Security-Based Swap execution facility.

[4] *See* Appendix I for No-Action Relief from Exchange Act Rule 901(a) stating that following the CFTC rules for the reporting hierarchy will not provide a basis for an enforcement action by the SEC, subject to the exception specified in Appendix I.

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

Security-Based Swap: A Security-Based Swap as defined from time to time by the SEC and the Commodity Futures Trading Commission.[5]

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 Users from time to time.

Third Party Reporter: A person that has been authorized by a Counterparty or a Platform to report SBSDR Information to ICE Trade Vault on behalf of such Counterparty or Platform.

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.

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, subject to the No-Action Relief.

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

User: An entity that has validly enrolled to use the ICE SBSDR Service.[6] A User may be:

(1) A Counterparty to a Security-Based Swap that reports trade information related to a Security-Based Swap 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 trade information related to a Security-Based Swap to ICE Trade Vault to satisfy an obligation under Exchange Act Rule 901(a);

(3) A Clearing Agency that reports trade information related to 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);

(4) An Execution Agent that reports trade information to a Security-Based Swap to ICE Trade Vault to satisfy an obligation under Exchange Act Rule 901(a) on behalf of one or more Counterparties, including externally managed investment vehicles;

(5) A registered broker-dealer (including a registered Security-Based Swap execution facility) that reports trade information related a Security-Based Swap to ICE Trade Vault to satisfy an obligation under Exchange Act Rule 901(a); or

(6) A Third Party Reporter that reports trade information on behalf of a Reporting Side, a non-Reporting Side, or a Platform.

User Agreement: The ICE Trade Vault Security-Based SDR User Agreement.

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

Verified: ICE Trade Vault considers the trade information it receives in respect of a Security-Based Swap to be "Verified" if (i) the Security-Based Swap has been: submitted by a Clearing

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

[6] *See* footnote 4.

Agency User, submitted by a Platform User, or submitted by an electronic confirmation service or affirmation platform User, (ii) the Security-Based Swap is an inter-affiliate swap or (iii) the non-Reporting Side User has submitted a verification message with respect to the Security-Based Swap.

The terms "CEA", "Designated Contract Market", "DCM", "Eligible Contract Participant", "ECP", "ICE eConfirm Service", "ICE Real-Time Ticker", "ICE Real-Time Ticker Service", "Non-Swap Dealer/Major Swap Participant", "Non-SD/MSP" are not applicable to the ICE SBSDR Service and shall be deemed deleted for the purposes of the Rulebook as amended by this SBSDR Annex.

Each reference in the Rulebook to the term listed in column "A" below shall be deleted and replaced by the term in column "B":

A	B
Rulebook reference	**SBSDR Annex Reference**
Applicable CFTC Regulations	Applicable SEC Regulations
CFTC	SEC; *provided that,* when used in this SBSDR Annex, CFTC shall have the meaning given to it in the Rulebook without reference to this SBSDR Annex.
Derivatives Clearing Organization or DCO	Clearing Agency/CA
ICE SDR Service/ ICE Trade Vault Service	ICE SBSDR Service
Swap Execution Facility	SBS SEF
SDR Information	SBSDR Information
SDR Rulebook/Rulebook	SBSDR Rulebook
Section 8 Material	Confidential Information
trade/swap trade/ swap transaction	Security-Based Swap trade/ Security-Based Swap transaction

2. **Rule 2.1 shall be amended by deleting the first reference below and replacing it with the second reference below:**

"of which at least one director shall be a "Public Director" as defined in the Applicable CFTC Regulations"

"who are a fair representation of market participants"

3. **Rule 2.1.1 shall be amended by:**

a. deleting the first reference below and replacing it with the second reference below:

"conflicts between business considerations and the requirement that ICE Trade Vault provide fair and open access as set forth in 49.27;"

"conflicts between business considerations and the requirement for ICE Trade Vault to avoid unreasonable or anticompetitive actions as set forth in Exchange Act Rule 13n-4(c)(1) and (c)(3);"

b. deleting the reference below:

"taking reasonable steps to ensure compliance with the CEA and Applicable CFTC Regulations relating to agreements, contracts, or transactions, and with CFTC regulations under Section 21 of the CEA, including confidentiality and indemnification agreements entered into with foreign or domestic regulators pursuant to Section 21(d) of the CEA; (vii)"

c. deleting the first sentence below and replacing it with the second sentence below:

"Pursuant to CFTC regulation § 49.22, removal of the CCO requires the approval of the Board of Directors and notice to the CFTC of the CCO's removal within two business days of such removal. ICE Trade Vault shall further notify the CFTC within two business days of the appointment any new CCO, whether interim or permanent."

"Pursuant to Exchange Act Rule 13n-11(a), the compensation, appointment, and removal of the CCO shall require the approval of a majority of the Board of Directors."

4. **Rule 2.2 shall be deleted in its entirety and restated as follows:**

2.2 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 the SEC and 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.[7]"

5. **Rule 2.3 shall be deleted in its entirety and replaced with [RESERVED].**

6. **Rule 2.4 shall be amended by deleting the first reference below and replacing it with the second reference below:**

"All data submitted during system down time is stored and processed once the service has resumed."

[7] *See* Appendix I for an explanation of how these rules are affected by the No-Action Relief.

"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.[8] 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 Users that it has resumed normal operations. Any User 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."

7. **Rule 2.5 shall be amended by adding the following at the end of the Rule:**

   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.

8. **Rule 2.7 shall be deleted in its entirety and restated as follows:**

   2.7 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 shall be fair and reasonable and not unreasonably discriminatory. ICE Trade Vault dues, fees, other charges, discounts, or rebates shall be applied consistently across all similarly situated Users. 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.

9. **Rule 2.8.1 shall be amended by deleting the first reference below and replacing it with the second reference below:**

   "the ICE SDR Service"

   "the System or the ICE SBSDR Service"

10. **Rule 2.8.2 shall be amended by deleting the first reference below and replacing it with the second reference below:**

    "(iii) any occurrence or circumstance which threatens or may threaten the proper functionality of the ICE SDR Service; (iv) any occurrence or circumstance which may materially affect the performance of the ICE Trade Vault systems; (v) any action taken by any governmental body or any regulator, Trusted Source or Participant which may have a direct impact on the ICE Trade Vault systems; and (vi) any other circumstance which may impact ICE Trade Vault in a materially adverse manner."

    "(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, the SEC 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."

[8] *See* footnote 2.

11. **Rule 2.8.3 shall be amended by:**

a. in the first paragraph, deleting the first reference below and replacing it with the second reference below:

"the ICE SDR Service or the systems and facilities of ICE Trade Vault"

"the System or the ICE SBSDR Service"

b. in the third bullet point, deleting the first reference below and replacing it with the second reference below:

"temporarily limiting or denying access to the ICE SDR Service, including access to any relevant ICE Trade Vault system or facilities;"

"temporarily limiting or denying access to the System or the ICE SBSDR Service;"

c. in the third paragraph, deleting the first reference below and replacing it with the second reference below:

"including suspending the ICE SDR Service"

"including preventing access to the System or suspending the ICE SBSDR Service"

d. in the fourth paragraph, deleting the first reference below and replacing it with the second reference below:

"to permit the ICE SDR Service"

"to permit the System and the ICE SBSDR Service"

e. deleting the first paragraph below and replacing it with the second paragraph below:

"In accordance with the requirements of CFTC regulation § 49.23(e), ICE Trade Vault will notify the CFTC as soon as practicable of any action taken, or proposed to be taken, pursuant to this rule. 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 and Trusted Sources via email as soon as practicable of any action taken, or proposed to be taken, pursuant to this rule."

"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 Rule 2.8.3. 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 Users via email as soon as practicable of any action taken (time permitting), or proposed to be taken, pursuant to this Rule 2.8.3."

12. **Rule 2.9 shall be deleted in its entirety and replaced with [RESERVED].**

13. **Rule 3 and each subsection thereto shall be deleted in its entirety and restated as follows:**

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 under SEC rules, access to, and use of, the ICE SBSDR Service does not require the use of any ancillary service offered by ICE Trade Vault.

Users shall only have access to (i) data they reported; (ii) data that pertains to a Security-Based Swap to which they are a Counterparty; (iii) data that pertains to a Security-Based Swap for which the User is an Execution Agent, Platform, registered broker-dealer or a Third Party Reporter; and (iv) data that ICE Trade Vault is required to disseminate publicly.

3.1.1 User Access

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

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

3.1.2 Denial of User Enrollment

ICE Trade Vault may decline the request of an applicant to become a User of the ICE SBSDR Service if such denial is required in order to comply with Applicable Law (e.g., to comply with sanctions administered and enforced by the Office of Foreign Assets Control of the U.S. Department of the Treasury ("OFAC")). ICE Trade Vault shall notify the SEC of any such denial.

If an applicant is denied by ICE Trade Vault for any other reason, the denial shall be treated as an "Access Determination" (as defined below), and the applicant will be entitled to notice and an opportunity to contest such determination in accordance with Rule 3.4 of this Rulebook. If the denial of an application is reversed, the applicant will be granted access to the ICE SBSDR Service promptly following completion of onboarding requirements.

3.1.3 Regulator Access

Prior to providing the access contemplated by this Rule, any entity authorized by Applicable Law to receive access to data held by ICE Trade Vault shall (i) have entered into a Memorandum of Understanding or other arrangement between such Regulator and the SEC that is in full force and effect (an "MoU") addressing confidentiality and access to data ("Confidentiality Agreement"), as required under Applicable Law; (ii) file a request for access with ICE Trade Vault by contacting the CCO (via email: TradeVaultChiefComplianceOfficer@theice.com) wherein the entity specifically describes the data sought within the scope of its jurisdiction and Confidentiality Agreement and with such specificity that is acceptable to ICE Trade Vault; and (iii) provide any additional information reasonably required by ICE Trade Vault to fulfill the request. ICE Trade Vault shall then promptly notify the SEC regarding any initial request received from a Regulator for access to the Security-Based Swap data maintained by ICE Trade Vault in accordance with Exchange Act Rule 13n-4.

Following notification to the SEC of such initial request for data access from a Regulator and due execution of necessary onboarding documentation, ICE Trade Vault shall provide such Regulator access to requested Security-Based Swap data (absent objection by the SEC).

Each Regulator's designated Administrator will manage the Regulator's access to the ICE SBSDR Service. Such access may include, where permitted by Applicable Law and any relevant MoU or other arrangement, tools for the monitoring, screening and analyzing of Security-Based Swap trade information, including, but not limited to, services that provide automated transfer of data to Regulators. The ICE SBSDR Service shall provide Regulators the ability to view data sets consistent with Applicable Law and any relevant MoU.

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 SEC. Nothing in this Rulebook shall be construed as restricting in any way the SEC's access to the ICE SBSDR Service and the SBSDR Information submitted to ICE Trade Vault.

3.2 Violations of Rulebook/Applicable Law

3.2.1 Jurisdiction

ICE Trade Vault shall have the authority to conduct inquiries into, and impose access restrictions in response to, any violation of this Rulebook and/or Applicable Law ("Violations") committed by Users as provided in this Rule 3.2. In addition ICE Trade Vault reserves the right to notify the SEC of any Violations.

3.2.2 CCO Powers and Duties

The CCO is responsible for enforcing this Rule 3.2 and shall have the authority to inspect the books and records of all Users that are reasonably relevant to any inquiry carried out pursuant to this Rule 3.2. The CCO shall also have the authority to require any User to appear before him or her to answer questions regarding possible Violations. The CCO may also delegate such authority to ICE Trade Vault employees, including officers, and such other individuals (who possess the requisite independence from ICE Trade Vault and the relevant User) as ICE Trade Vault may hire on a contractual basis.

The CCO shall conduct inquiries of possible Violations, prepare written reports with respect to such inquiries, furnish such reports to the Board of Directors and conduct the examinations with respect to such Violations.

If, in any case, the CCO (or another ICE Trade Vault employee designated for this purpose by ICE Trade Vault) concludes that a Violation may have occurred, he or she may:

- issue a warning letter to the User informing it that there may have been a Violation and that such continued activity may result in access restrictions and notice to the SEC; and/or
- negotiate a written settlement agreement with the User, whereby the User, with or without admitting responsibility, may agree to (i) comply with a cease and desist order; and/or (ii) a limitation of access to the ICE SBSDR Services and the System.

Any settlement recommended by the CCO shall be subject to the approval of the Board of Directors and shall become final and effective pursuant to Rule 3.2.3.

3.2.3 Board of Directors' Disciplinary Authority

The Board of Directors shall have the power to direct that an inquiry of any possible Violation be conducted by the CCO and shall hear any matter referred to it by the CCO regarding a possible Violation.

In any case where the Board of Directors concludes that a Violation has occurred, the Board of Directors may: (i) refer or return the matter to the CCO with instructions for further investigation; (ii) approve a settlement agreement negotiated pursuant to Rule 3.2.2 with such User (which may provide for consequences other than those recommended by the CCO); and/or (iii) take, or instruct the CCO to take, any further action it deems necessary including, but not limited to, issuing:

- a cease and desist order or a written warning; and/or
- a limitation of access to the ICE SBSDR Services and the System.

3.3 Revocation of Access

ICE Trade Vault may revoke a User's access to the System, the ICE SBSDR Service or SBSDR Information in accordance with this Rule 3.3 following a determination that (i) the User has violated any provision of the User Agreement (including by failing to pay any fees when due), this Rulebook, Applicable Law or any ICE Trade Vault policies and procedures related to the ICE SBSDR Service or (ii) such action is necessary or appropriate in light of ICE Trade Vault's regulatory responsibilities or for the protection of the integrity of the System (each, an "Access Determination"). Access Determinations shall be made by the CCO based on the information gathered during the inquiry, if any, conducted in accordance with Rule 3.2.2 and reviewed by the President and General Counsel of ICE Trade Vault within 5 business days of such determination prior to implementing any revocation of access. Notwithstanding the foregoing, the CCO's Access Determination may be implemented immediately without prior review by the President or General Counsel ("Immediate Revocation") where the CCO determines such revocation is necessary for the protection of the integrity of the System or to fulfill ICE Trade Vault's regulatory responsibilities.

If (i) an Immediate Revocation occurs or (ii) the President and General Counsel conclude that an Access Determination is appropriate and in compliance with Applicable Law, the CCO shall, within 1 business day, provide notice by email to the User to which the Access Determination applies, including in such notice the specific reasons for the determination. If the President and General Counsel conclude that limitation or revocation of access pursuant to an Access Determination made by the CCO would constitute unreasonable discrimination, the President and General Counsel shall take such actions as are necessary to maintain or restore access to the System, the ICE SBSDR Service or SBSDR Information, as applicable.

3.4 Review and Dispute of Revocation of Access

Following notice of an Access Determination to a User that does not involve an Immediate Revocation, revocation of such User's access shall occur only after User has been given an opportunity to contest the determination before the Board of Directors within 10 business days of such notice. In the event of an Immediate Revocation, a User shall be entitled to notice and opportunity to contest within 10 business days of such revocation.

- In order to contest an Access Determination, the User must notify ICE Trade Vault within 1 business day of notice of such determination. A meeting to address the determination shall occur as promptly as possible within the timeframes specified in this Rule 3.4 and may be held by telephone, in person or via such other means as are acceptable to ICE Trade Vault. ICE Trade Vault and User will each be responsible for their own expenses in participating in the meeting.

- The User shall be notified of the time, place and date of the meeting not less than 2 business days in advance of such date.
- At the meeting, the User will have an opportunity to present evidence before the Board of Directors. The User is not required to, but may be if it wishes, represented by counsel at User's sole expense except as provided below.
- Within 5 business days after the meeting, a majority of the Board of Directors will either affirm or reverse the Access Determination. The User shall be notified in writing of the Board of Directors' decision. If the Board of Directors decides to affirm the Access Determination, the notification shall include the grounds for such decision. The decision of the Board of Directors shall become final and effective once notified to the User.

A record shall be kept of any meeting held in accordance with this Rule 3.4. The cost of the transcript may be charged in whole or in part to the User in the event that the Access Determination is affirmed.

3.5 Final Access Determinations

If the Board of Directors affirms an Access Determination, ICE Trade Vault shall promptly file notice thereof with the SEC in such form and with such information as the SEC may prescribe. ICE Trade Vault will also notify the SEC of all final Access Determinations by ICE Trade Vault in its annual amendment to its Form SDR.

Pursuant to Exchange Act Section 11A, any notice to the SEC of an Access Determination shall be subject to review by the SEC on its own motion, or upon application to the SEC by the User whose access has been limited or revoked (the "Suspended User"), within thirty days after notice of the Access Determination has been filed with the SEC and received by the Suspended User.

3.6 Implementation of a Revocation of Access

Upon an Access Determination becoming effective (whether due to an Immediate Revocation or because the User has not requested a meeting within one business day of receipt of its notice of Access Determination or the Board of Directors affirmed an Access Determination), ICE Trade Vault will notify the User (the "Terminated User") of the effective date of revocation of access. The notice provided to the Terminated User will also specify how any pending submissions will be handled. ICE Trade Vault will take all necessary steps to terminate the Terminated User's license to access and use the System in accordance with the Access Determination, including by cancelling such User's ID and password(s).

Upon the termination of a Terminated User's access, ICE Trade Vault will, as soon as possible, notify all other Users of the revocation of access. ICE Trade Vault's notice to other Users will provide, to the extent relevant, information on how pending transaction submissions and other pending matters will be impacted by the Access Determination and what steps are to be taken by all affected parties.

ICE Trade Vault shall not accept any submission from a Terminated User that was effected after the time at which the Access Determination became effective. If a Terminated User has satisfied all outstanding obligations to ICE Trade Vault, ICE Trade Vault will consider allowing a Terminated User to submit data via a Third Party Reporter on a case-by-case basis.

3.7 Connectivity

Users and the SEC may access the System through a web-based front-end that requires systems to (i) satisfy ICE Trade Vault minimum computing system and web browser requirements; (ii) support HTTP 1.1 and 128-bit or stronger SSL data encryption; (iii) the most recent version of Internet Explorer or Chrome; and (iv) support the most recent version of Adobe Flash Player. Regulators may access the System through services that provide automated transfer of data. The SEC may connect to the ICE SBSDR Service through Direct Electronic Access.

3.8 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, Users, the SEC 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 Users.

14. **Rule 4 and each subsection thereto shall be deleted in its entirety and replaced with the following:**

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

Users reporting trade information to the ICE SBSDR Service will be required to comply with reporting obligations under Applicable SEC Regulations, subject to the No-Action Relief, 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),[9] ICE Trade Vault requires all Users to report complete and accurate trade information and to review and resolve all error messages generated by the System with respect to the data they have submitted.

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

[9] *See* footnote 1.

Side, as determined by the hierarchy specified in Exchange Act Rule 901(a),[10] 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)),[11] secondary trade information (set forth in Exchange Act Rule 901(d)),[12] and Life Cycle Events (set forth in Exchange Act Rule 901(e)),[13] and each within the timeframe specified in the Applicable SEC Regulations. Primary trade information, secondary trade information, and Life Cycle Events are described in this Rulebook in further detail.

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), as clarified by the No-Action Relief, each User that is a Security-Based Swap dealer, security-based major swap participant, or Clearing Agency 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 User shall review and update its policies and procedures at least once annually in accordance with Exchange Act Rule 906(c).[14]

Each Reporting Side must maintain, or cause its trading counterparty to maintain, the required Unique Identification Codes,[15] (including but not limited to any internal mapping of static data) and to ensure they remain current and accurate. Upon the written request of ICE Trade Vault, a Reporting Side must promptly provide such identifier information, including any internal mapping, in the manner and form requested by ICE Trade Vault.

4.2.3 Non-Reporting Side

Users that are non-Reporting Sides may verify or dispute the accuracy of trade information that has been submitted by a Reporting Side to ICE Trade Vault where the non-Reporting

[10] *See* footnote 4.

[11] *See* Appendix I for relief from Exchange Act Rule 901(c)(2)-(7) providing that Users' omission to report primary trade information that is not subject to reporting under CFTC rules will not provide a basis for an enforcement action by the SEC. Note that primary trade information required under Exchange Act Rule 901(c)(1) must still be reported.

[12] *See* Appendix I for No-Action Relief from Exchange Act Rule 901(d), providing that Users' omission to report secondary trade information that is not subject to reporting under the CFTC rules will not provide a basis for an enforcement action by the SEC.

[13] *See* footnote 3.

[14] *See* Appendix I for the SEC's expectation of registered Security-Based Swap dealers or registered broker dealers that arrange, negotiate or execute Security-Based Swap Transactions on behalf of a foreign affiliate.

[15] *See* Appendix I for No-Action Relief from Exchange Act Rule 903(b) requiring an SBSDR to publish information needed to interpret codes on a non-fee basis.

Side is identified as the Counterparty by sending a verification message indicating that it verifies or disputes such trade information. Users' obligations with respect to missing UIC information are addressed in Rule 4.10 below.

If the non-Reporting Side is not a User, the non-Reporting Side should contact ICE Trade Vault (TradeVaultSupport@theice.com) to register for access to the SBSDR Service to verify its trade information. ICE Trade Vault will attempt to notify such a non-Reporting Side where such party's LEI is provided by the Reporting Side using the email address for the non-Reporting Side that was reported by the Reporting Side. Such email notice to the non-Reporting Side will indicate that ICE Trade Vault has received trade information to which the non-Reporting Side is indicated as a party to the trade and that it must register for access to the SBSDR Service to verify the accuracy of the information submitted and provide any missing UIC information, if applicable. If the Reporting Side provided the non-Reporting Side's LEI but elected not to provide an email address for the non-Reporting Side, ICE Trade Vault will attempt to so notify the non-Reporting Side using available email contact information contained in the static data maintained by ICE Trade Vault with respect to market participants, to the extent Trade Vault is permitted by Applicable Law to utilize such data (without contravening, for example, local privacy laws or contractual obligations of ICE Trade Vault). ICE Trade Vault will not verify the validity of any email address and will not confirm whether any of its email notices were duly received or take further action if an email notice is rejected.

4.2.4 Other Reporting Entities

A Platform on which a Security-Based Swap was executed and submitted for clearing to a Clearing Agency shall report to an SBSDR certain information as required under Applicable SEC Regulations and 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.

In accordance with Exchange Act Rule 906(c), each User that is a Platform, or a registered broker-dealer (including a registered SBSEF) 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 User shall review and update its policies and procedures at least once annually in accordance with Exchange Act Rule 906(c).

4.2.5 Required Submissions

4.2.5.1 Submission Methods

In accordance with Exchange Act Rule 901(h), Users 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 Extensible Markup Language ("XML") format. Only Users may submit trade information to the System.

4.2.5.2 Primary Trade Information

In accordance with Exchange Act Rule 901(c),[16] Users must report all primary trade information, and this information must be submitted to the System consistent with "Exhibit

[16] *See* footnote11.

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. ICE Trade Vault reserves the right to modify the field list, validations, and XML tags as it deems necessary in order to facilitate the accurate reporting of data. 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 submitter is required to properly amend and resubmit non-conforming trade information. A Security-Based Swap that fails the validation requirements of the System resulting in an Invalid status will not be viewed as a reported trade.

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, or if twenty-four hours would fall on a day that is not a business day, by the same time on the next business day. Furthermore, ICE Trade Vault shall make systematically available standard data values as denoted in Exhibit N.5 to the SEC and Users.

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 Product ID field does not include the following information (e.g., an exotic product), 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. The value submitted for the execution time should use the ISO-8601 Standard.

ii. 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; and

(6) Whether Counterparties intend that the Security-Based Swap to be submitted for clearing.[17]

4.2.5.3 Secondary Trade Information

In accordance with Exchange Act Rule 901(d),[18] Users 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 Users 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 N5 and includes, as applicable and to the extent not previously submitted as primary trade information:[19]

(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;

---

[17] Note that prongs (2) to (6) are subject to No-Action Relief from Exchange Act Rule 901(c)(2)-(7), see Appendix I.

[18] *See* footnote 12.

[19] Note that all secondary trade information required pursuant to Exchange Act Rule 901(d) is subject to the No-Action Relief, and the omission of any data not required under the CFTC rules will not provide a basis for an enforcement action by the SEC.

(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, Users should submit the pre-allocated Security-Based Swap with the "Allocation Status" field set to "Pre." Once the Security-Based Swap is allocated, the pre-allocation Security-Based Swap should be canceled upon the submission of the new post-allocation Security-Based Swaps which have the field "Allocation Status" set to "Post." The submission of the new post-allocation Security-Based Swap will require the submission of the following fields: "Counterparty 1 or 2 Agent" information and the "Previous Transaction ID".

4.2.5.4 Historical Security-Based Swap Reporting

In accordance with Exchange Act Rule 901(i), Users must report all of the information required by Exchange Act Rule 901(c) and 901(d), each subject to the No-Action Relief, that is available for the Historical Security-Based Swaps they are reporting and must indicate whether the swap is open at the time of the report. Users shall submit a value of "Y" for the "Flag for Historical Security-Based Swap public dissemination exemption" field. Furthermore, as applicable, Users 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. The System will accept Historical Security-Based Swaps via API submissions in the Extensible Markup Language ("XML") format. Only Users may submit trade information to the System. Where a field is not applicable for a historical submission, a "Not Applicable" indicator should be submitted.

4.2.5.5 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". A Security-Based Swap will be considered exotic when the information reported pursuant to Exchange Act Rule 901(c)(1)(i)-(iv) does not provide all of the material information necessary to identify the Security-Based Swap or does not contain the data elements necessary to calculate the price. Users shall report 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 with respect to exotic Security-Based Swaps. Users should submit exotics under the exotic product identifier, and, where a field is not applicable for an exotic submission, a "Not Applicable" indicator should be submitted. To ensure that users of public reports of "exotic swaps" do not get a distorted view of the market, Users shall submit a

value of "Y" for the 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.

4.2.5.6 Package Security-Based Swap Reporting

ICE Trade Vault supports the reporting of package Security-Based Swaps. For Security-Based Swaps that were executed as ad-hoc spread or package transactions, Users should submit trade information in accordance with the appropriate product identifiers with a Transaction ID per leg of the package transaction with each indicating it is part of a package trade with a Package ID included on each to link the Security-Based Swaps. To ensure that users of public reports of "package swaps" do not get a distorted view of the market, Users shall submit a value of "Y" for the flag indicating that the Security-Based Swap is part of a package.

4.2.5.7 Verification of Trade Data

Users must verify that all trade information that they submit to the ICE SBSDR Service is complete and accurate. If any trade information is found to be incorrect or incomplete, Users reporting on behalf of Reporting Sides must correct and resubmit such information to the System. Users other than the Reporting Side reporting on behalf of non-Reporting Side may upload a verification message to indicate the trade has been verified.

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. 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 and verified by the Clearing Agencies. The Clearing Agency must submit the Cleared Novation Termination or Rejection message for the alpha Security-Based Swap to the SBSDR where the alpha was reported. The Cleared Novation message to terminate an alpha must be submitted by a Clearing Agency User and include the alpha Transaction ID, alpha SBSDR, alpha's buyer and seller IDs, beta and gamma Transaction IDs, action type, Life Cycle Event, and clearing acceptance timestamps. Upon receiving a cleared novation termination message, ICE Trade Vault will validate that it currently has the related alpha trade to be terminated; if it does not have the alpha trade, the Cleared Novation message will fail. If the Cleared Novation message fails on the first attempt to report, the Clearing Agency should attempt to report it again at the end of the following business day. If the Cleared Novation message still fails, the Clearing Agency should contact the counterparties to confirm the accuracy of the alpha trade's Transaction ID and the SBSDR to which it was to be reported.

Platform Users will access the ICE SBSDR Service 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 and verified by Platforms.

4.2.5.8 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:

(1) The submission file is in a valid format for receipt and processing;

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

(3) All Required and Conditionally Required fields are contained in the submission;

(4) All fields meet the validation requirements; and

(5) 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. Trade information that receives an Invalid status is not considered to have been reported in accordance with the SBSDR reporting obligations. Please reference Exhibit N.5 for a further description of the validation criteria.

4.2.5.9 Non-Mandatory Reports

ICE Trade Vault has chosen not to accept Non-Mandatory Reports.

4.2.5.10 Life Cycle Events

In accordance with Exchange Act Rule 901(e),[20] and 901(j), Users must report Life Cycle Events for previously submitted trade information to the System within 24 hours of the occurrence of a Life Cycle Event, or if 24 hours falls on a day that is not a business day, by the same time on the next business day. Users shall include the "Previous Transaction ID" for the original trade in association with Life Cycle Events. Users will submit the full updated or new trade terms which resulted from the Life Cycle Event and include the "Life Cycle Event Status" to indicate the event which occurred. The System will accept Life Cycle Events via API submissions in the Extensible Markup Language ("XML") format. Only Users may submit trade information to the System.

4.2.5.11 End-User Exception Data

In accordance with Exchange Act Rule 901(d)(7),[21] if Counterparties do not intend to submit a mandatorily clearable Security-Based Swap to a Clearing Agency, the User reporting the trade 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 the SEC, Regulators and Users 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:

[20] *See* footnote 3.

[21] *See* footnote 12.

- **VERIFIED**: Reported trade details are considered verified when:
  - the Security-Based Swap trade details have been submitted by a Clearing Agency User, submitted by a Platform User, or submitted by an electronic confirmation service or affirmation platform User;
  - the Security-Based Swap is an inter-affiliate swap; or
  - the non-Reporting Side User has submitted a verification message with respect to the Security-Based Swap.
- **UNVERIFIED**: A Security-Based Swap that is not "Verified."
- **CANCELLED**: A Security-Based Swap that has been rescinded, compressed, early terminated or busted or that has been terminated by a Life Cycle Event.
- **ERROR**: A Security-Based Swap that was erroneously reported to the ICE SBSDR Service and deemed to be submitted to System in error by the User.
- **DISPUTED**: A Security-Based Swap in respect of which the non-Reporting Side has submitted a dispute message.
- **REJECTED**: A Security-Based Swap that has been rejected by a Clearing Agency or prime broker.
- **INVALID**: A Security-Based Swap that failed the validation requirements of the System.

4.4 Life Cycle Event Status

Life Cycle Events shall be reported via XML API, the message shall contain all relevant trade terms plus the applicable Life Cycle Event. The Life Cycle Event status identifies an action taken with respect to a trade submitted to the ICE SBSDR Service:

- **EARLY TERMINATE**: The Security-Based Swap has been terminated prior to its original termination date.
- **MODIFY TRADE**: The Security-Based Swap has been modified to reflect a change in terms, including, but not limited to, a change in cash flows, a change in title or date of the master agreement, or a corporate action that affects the economic terms of the Security-Based Swap.
- **NOVATED**: The rights, liabilities, duties and obligations of the stepping-out party have been transferred to the stepping-in party.
- **CLEARED NOVATION:** An "alpha" or original Security-Based Swap has been terminated by acceptance to clearing.
- **ASSIGNMENT**: All parties to a Security-Based Swap have confirmed that the interest or benefit of the stepping-out party has been transferred to the stepping-in party, but not the obligations.
- **OPTION EXERCISE**: A new trade has resulted from the exercise of all or part of the Security-Based Swaption into a swap has occurred.

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), Users are responsible for the timely resolution of errors contained in trade information that they submit to ICE Trade Vault. ICE Trade Vault provides Users electronic methods to extract SBSDR Information for reconciliation purposes. 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. 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.

Both Platforms and Clearing Agencies are similarly 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.

4.7 Dispute Process for Reported Data

Disputes involving clearing transactions shall be resolved in accordance with the Clearing Agency's rules and Applicable Law. For an alpha Security-Based Swap executed on a Platform and reported by a Platform User, disputes must be resolved in accordance with the Platform's rules and Applicable Law. For Security-Based Swaps that are reported by a User that is neither a Platform nor a Clearing Agency, Counterparties shall resolve disputes with respect to SBSDR Information in accordance with the Counterparties' master trading agreement and Applicable Law.

If a User elects to verify a trade and a dispute results, Users are required to promptly notify ICE Trade Vault of trade Information that is disputed. Users shall utilize the "Dispute" functionality contained in the ICE SBSDR Service to do so. A User can identify disputed SBSDR Information stored in the System by submitting a dispute message via a delimited file upload and populating a "Y" value in the "Dispute Status" field and the Counterparty ID of the party that initiated the dispute 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 by submitting a dispute message via a delimited file upload and populating a "N" value in the "Dispute Status". ICE SBSDR Service will provide the SEC and Regulators with reports identifying the SBSDR Information that is deemed disputed.

4.8 Positions: Calculations and Reporting

The methodology for the calculation of Positions for Security-Based Swaps is outlined in the SBSDR Participants User Guide. Please refer to "Exhibit N.2 - SBSDR Participants User

Guide", available on the ICE Trade Vault website (www.icetradevault.com) for further details.

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.

15. **Rule 5 and each subsection thereto shall be deleted in their entirety and restated as follows:**

Public Dissemination

In accordance with Exchange Act Rule 902(a),[22] 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, Users, the SEC and Regulators to download historical data.

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. Reports will be available at www.ICETradeVault.com and will be widely accessible as contemplated under Exchange Act Rule 900(tt). For more information, please consult ICE Trade Vault's Public Dissemination Guide.

While ICE Trade Vault may publicly disseminate SBSDR Information in accordance with the CFTC rules based on the No-Action Relief from Exchange Act Rule 902, the No-Action Relief is subject to the following exceptions:

- if the notional amount of Security-Based Swap based of a single credit instrument or a narrow based index is $5 million or greater, ICE Trade Vault will disseminate a capped size of $5MM + rather than the actual notional amount to be disseminated under CFTC rules;
- if the Security-Based Swap transaction is an interdealer transaction between non-U.S. dealers for which at least one party uses the "arranged, negotiated, or executed" ("ANE") exception from the *de minimis* thresholds, ICE Trade Vault will disseminate SBSDR Information immediately in accordance with SEC requirements; and
- if the Security-Based Swap transaction is between an entity relying on the ANE exception and a registered Security-Based Swap dealer, ICE Trade Vault will disseminate SBSDR Information immediately in accordance with SEC requirements.

5.1 No Advance Disclosure

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

[22] *See* footnote 2.

5.2 Errors and Omissions

Users are required to promptly verify trade information submitted in respect of their transactions and promptly report any discrepancies in accordance with Rule 4.6 of this Rulebook. 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.

16. **Rule 6 and each subsection thereto shall be deleted in their entirety and restated as follows:**

Unique Identification Codes (UICs)

In accordance with Exchange Act Rule 903(a) and (b), 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 an ID or an ID will be provided by Users for the applicable UIC.

In accordance with Rule 903(b),[23] once a UIC is created in the SBSDR, a User 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.

Users reporting on behalf of a Reporting Side must report Reporting Side UIC information as well as the Counterparty ID and Execution Agent ID[24] of the non-Reporting Side and, where applicable, the Clearing Agency ID and Platform ID. Users reporting on behalf of a Platform must report the Counterparty ID or the Execution Agent ID of each Counterparty, as applicable, and the Platform ID. When there is no applicable UIC code for a field, a "Not Applicable" value must be submitted in order for the field to be considered reported. Users reporting on behalf of a Reporting Side may submit the non-Reporting Side UIC information, but they are not required to do so. Users reporting on behalf of Reporting Sides and Users reporting on behalf of a Platform can submit all UIC information in the standard Trade Vault SECXML submission message. If the Reporting Side User does not supply the non-Reporting Side's UIC information and the non-Reporting Side is an SEC Participant, then the non-Reporting Side or its Execution Agent or Third Party Reporter (if any) must submit

[23] *See* footnote 15.

[24] Note that the omission of the Execution Agent ID as a result of the No-Action Relief from Exchange Act Rule 901(d) will not provide a basis for an enforcement action by the SEC. *See* Appendix I.

this information to ICE Trade Vault. UICs for the non-Reporting side can be provided using a UIC csv upload containing a minimal number of fields including:[25]

a) Submitter ID

b) Submitter ID Source

c) Transaction ID

d) Counterparty 1/Counterparty 2 Branch ID

e) Counterparty 1/Counterparty 2 Broker ID

f) Counterparty 1/Counterparty 2 Desk ID

g) Counterparty 1/Counterparty 2 Trader ID

6.1 Transaction ID Methodology

If a CPMI-IOSCO Transaction ID methodology is in place, it shall be used. Otherwise, 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.[26]

(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.[27] 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.

(7) A Transaction ID shall not be more than 54 characters, all letters should be upper cased.

---

[25] Note that prongs (d) to (g) are subject to No-Action Relief from Exchange Act Rule 901(d), see Appendix I.

[26] As described in 4.2.5.7 above, when a Security-Based Swap is submitted for clearing, it is novated into two new Security-Based Swap**s ("beta" and "gamma" Security-Based Swap**s) 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.

[27] 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.

6.2 Counterparty 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 IDs to different types of entities, and ICE Trade Vault shall accept LEIs as Counterparty IDs. All Users are required to register for an LEI for themselves. If a Counterparty does not have an LEI at time of reporting, or is not eligible to obtain an LEI, the User reporting the trade must complete a document describing why the Counterparty is reporting without an LEI a minimum of two business days prior to reporting. Please reference Exhibit U.4, ICE Trade Vault Non-Legal Entity Identifier Counterparty Setup Notification Request. Users are expected to inform ICE Trade Vault of the identity of the Counterparties that intend to trade before executing and reporting such Security-Based Swaps. For entities with an LEI, ICE Trade Vault will verify the entity name and LEI in GLEIF and then make the entity eligible for submission for Users using an LEI. For entities which submit the ICE Trade Vault Non-Legal Entity Identifier Counterparty Setup Notification, ICE Trade Vault will create an Internal ID. Users may then report Security-Based Swaps using that ID for such entity. If an invalid Counterparty ID is entered, the System will send an error message to the Reporting Side indicating such information and the submission will receive **an "Invalid" status**.

6.3 Unique Product ID

In accordance with 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. 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 a SEC or CPMI-IOSCO accepted UPI taxonomy or, where not available, its own product taxonomy. Exotic and basket products will be created upon request when there is need to execute a trade that does not conform to the current product structure. Users may submit Product IDs or the underlying taxonomy fields. 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 Date:** The maturity, termination, or end date of the transaction.
- **Coupon:** The standard coupon.

- **Notional Currency**: The standard ISO currency code.
- **Contract Type:** Designates the type of derivative (e.g., Security-Based Swap, option, swaption).

6.4 Creating New Product IDs

Users shall notify the ICE SBSDR Service of any new Security-Based Swap products they intend to report a minimum of 2 business days prior to executing and reporting Security-Based Swaps for that product to ICE Trade Vault by submitting the relevant product information to: TradeVaultSupport@theice.com. The request should include the data for the prescribed taxonomy fields. Once the request is received, ICE Trade Vault will review the request and create applicable products. 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 and the Security-Based Swap will be placed in an "Invalid" status. If a submission fails based on lack of product information, the User 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.

17. **Rule 7.1 shall be deleted in its entirety and restated as follows:**

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.

Counterparties' individual trade information records remain available to Users in accordance with Rule 3.1.1, the SEC 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 the SEC and Regulators via Direct Electronic Access.

Nothing in this Rule 7.1 shall require a User to pay fees associated with ICE Trade Vault's standard regulatory reporting and access obligations. However, if a User 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 User 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 User 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 User or at the instance of another party with authority to compel ICE Trade Vault to produce such records. For the avoidance of doubt, ICE Trave Vault shall never charge the SEC for access to the SBSDR Information via an API or for any request of SBSDR Information made by the SEC.

ICE Trade Vault may retain copies of communications between officers, employees or agents of ICE Trade Vault, on the one hand, and Users, 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.

APPENDIX I

The Applicable SEC Regulations are subject to the following Security-Based Swap data reporting relief provisions and relief for SBSDRs, which conform a number of Applicable SEC Regulations to the corresponding Applicable CFTC Regulations. This No-Action Relief will be in effect through to the earlier of October 6, 2025 or a date which may be set by the SEC by giving the industry twelve months' prior notice.

The No-Action Relief states that the following situations will not provide a basis for an enforcement action by the SEC:

Security-Based Swap reporting relief provision	**Exchange Act rules affected**	**Current CFTC rules referenced[1]**
If parties determine their duty to report a Security-Based Swap (or to participate in the selection of the Reporting Side) based on the CFTC rules rather than on the rules established by the SEC, except that a non-U.S. person in a Security-Based Swap transaction where either side is relying on the *arranged, negotiated or executed,* "ANE" exception for *de minimis* counting, must comply with the SEC requirement as to the person obligated to report the Security-Based Swap transaction -the broker-dealer or Security-Based Swap dealer providing the ANE services.	Exchange Act Rule 901(a) Reporting obligation hierarchy Exchange Act Rule 901(a)(2)(ii)(E) SEC reporting rule for transactions affected by the ANE provision	CFTC Regulation 45.8
If the reporting party omits to report certain data elements and those data elements are not required to be reported under the CFTC rules as of date of transaction, except for the requirement for the reporting party to identify Security-Based Swaps and underlying securities.	Exchange Act Rule 901(c)(2)-(7) Primary trade information Exchange Act Rule 901(d) Secondary trade information	CFTC Regulation 45.3
If ICE Trade Vault does not establish policies and procedures with respect to the reporting of data elements required under 901(c)(2)-(7) or 901(d).	Exchange Act Rules 907(a)(1) SBSDR establishing policies and procedures re: same	
If the reporting party omits to report certain life cycle events and those data elements are not required to be reported under the CFTC rules in force at time of the life cycle event.	Exchange Act Rule 901(e) Reporting of Life Cycle Events	CFTC Regulation 45.4

[1] The SEC anticipates that the CFTC rules may be further amended from time to time during the term of the No-Action Relief; the SEC relief will apply to the CFTC rules as they are amended.

Security-Based Swap reporting relief provision	Exchange Act rules affected	Current CFTC rules referenced[1]
If ICE Trade Vault does not establish policies and procedures with respect to the reporting of primary trade information and secondary trade information.	Exchange Act Rule 907(a)(3) SBSDR establishing policies and procedures re: same	
If ICE Trade Vault disseminates Security-Based Swap transaction data consistently with the CFTC public dissemination rules; *provided that:* a. if the notional amount of Security-Based Swap based of a single credit instrument or a narrow based index is $5 million or greater, ICE Trade vault must disseminate a capped size of $5MM + rather than the actual notional amount to be disseminated under CFTC rules; b. if the Security-Based Swap transaction is an interdealer transaction between non-U.S. dealers for which at least one party uses the ANE exception from *de minimis* counting, SEC requirements to disseminate information immediately will prevail; and c. if the Security-Based Swap transaction is between an entity relying on the ANE exception and a registered Security-Based Swap dealer (U.S. or non-U.S.), SEC requirements to disseminate information immediately will prevail.	Exchange Act Rule 902 Public dissemination	CFTC Regulation Part 43
If ICE Trade Vault permits the reporting or dissemination of Security-Based Swap transaction information that includes codes in place of certain data elements, even if the information needed to interpret those codes is not widely available on a non-fee basis.	Exchange Act Rule 903(b) Interpretation of codes	
If ICE Trade Vault does not send reports of missing UIC to its Users.	Exchange Act Rule 906(a) Reports of missing UIC	
If ICE Trade Vault does not collect ultimate parent and affiliate information from its Users.	Exchange Act Rule 906(b) Ultimate parent and affiliate information	

Security-Based Swap reporting relief provision	Exchange Act rules affected	Current CFTC rules referenced[1]
If ICE Trade Vault does not establish policies and procedures requiring Users to supply information on their ultimate parents and affiliates.	Exchange Act Rule 907(a)(6) Policies and procedures re: parents and affiliates	
If ICE Trade Vault does not establish policies and procedures with respect to condition flags in reporting Security-Based Swap transactions if ICE Trade Vault complies with similar CFTC rules for condition flags or other trade indicators.	Exchange Act Rule 907(a)(4) Condition Flags	
If ICE Trade Vault does not establish policies and procedures for assigning UIC's.	Exchange Act Rule 907(a)(5) Policies and procedures re: assigning UIC	
If ICE Trade Vault does not confirm with both counterparties the accuracy of the data it receives with respect to a Security-Based Swap.	Exchange Act §13(n)(5)(B) and Exchange Act Rule 13n-4(b)(3)	
If ICE Trade Vault does not establish policies and procedures designed to satisfy itself that transaction data submitted to it is complete and accurate, clearly identifies the source for each trade side and clearly identifies the pairing method, if any.	Exchange Act Rule 13n-5(b)(1)(iii)	
If ICE Trade Vault does not adhere to Exchange Act securities information processor requirements.	Exchange Act §11A(b)	
In footnote 770 of the No-Action Relief the SEC explains that it expects Security-Based Swap dealers or registered broker-dealers to establish policies and procedures including mechanisms to identify the foreign affiliates for which an ANE transaction was performed, to ensure the reporting of such transaction and that inter-dealer ANE transactions are publicly disseminated.	Exchange Act Rule 906(c) Policies and procedures to be established by registered Security-Based Swap dealers and registered broker-dealers	