

## Exhibit V.2

### ICE TRADE VAULT

#### **SECURITY-BASED SDR SERVICE DISCLOSURE DOCUMENT**

ICE Trade Vault, LLC ("ICE Trade Vault") offers a security-based swap data repository service for the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of credit asset class (the "ICE SBSDR Service"). This disclosure document is intended to disclose certain information about the ICE SBSDR Service in order to reasonably enable market participants to identify and evaluate the risks and costs associated with using the ICE SBSDR Service. Unless otherwise defined herein, all capitalized terms shall have the meanings ascribed to them in the ICE Trade Vault SBSDR Guidebook (the "Guidebook").

The information below is not an exhaustive description of the ICE SBSDR Service, and further information is available in the Guidebook and on ICE Trade Vault's website at [www.icetradevault.com](http://www.icetradevault.com). It should also be noted that this disclosure document does not address any of the risks and costs associated with entering into security-based swap transactions. The disclosures contained in this document may become incomplete or inaccurate as a result of changes to the ICE SBSDR Service and Applicable Law over time, and therefore ICE Trade Vault reserves the right to update this document as necessary.

#### **(1) CRITERIA FOR ACCESS TO THE ICE SBSDR SERVICE AND SECURITY-BASED SWAP DATA**

Consistent with Applicable Law, ICE Trade Vault provides access to 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 validly engage in security-based swap transactions and do not require the use of any other Ancillary Service offered by ICE Trade Vault, except for any Ancillary Service(s) that ICE Trade Vault is required to provide.

For security reasons, access to the ICE Trade Vault system is strictly limited to market participants ("Participants") with valid permissions and security access. Participants will only have access to their own data and data that ICE Trade Vault is required to make publically available ("Public Data"). Passwords must meet technical and procedural processes for information security and must be from eight to fourteen characters in length, utilize three different character types, and must be reset at least annually.

##### ***Market Participant Access Criteria***

Access to the ICE SBSDR Service is provided to Participants that have duly executed a Participant Agreement with ICE Trade Vault and have completed and delivered to ICE Trade Vault the applicable ICE Trade Vault Enrollment Form. These documents are available upon request from ICE Trade Vault.

When enrolling with ICE Trade Vault, Participants must designate a master user ("Administrator"). The Administrator will create, permission and maintain all user IDs for its firm. This ensures ICE Trade Vault access is granted by a trusted individual at the Participant's firm who is closest to and has the most knowledge of those in the firm who require access.

##### ***Regulator Access Criteria***

Regulators requiring or requesting access to the ICE SBSDR Service should contact the Chief Compliance Officer (via email: [TradeVaultChiefComplianceOfficer@theice.com](mailto:TradeVaultChiefComplianceOfficer@theice.com)) to request access and the necessary documentation. Upon enrollment with the ICE SBSDR Service, each

Regulator's designated Administrator will manage the Regulator's access to the ICE SBSDR Service.

To the extent required by Applicable Law, Regulators will be given direct electronic access to the ICE SBSDR Service in order to fulfill their legal and statutory responsibilities under Applicable Law. Such access shall include, where applicable, proper tools for the monitoring, screening and analyzing of security-based swap transaction data, including, but not limited to, web-based services and services that provide automated transfer of data to Regulators. The ICE SBSDR Service shall provide Regulators the ability to view individual market participants' data and aggregated data sets.

## **(2) ICE SBSDR SERVICE TECHNOLOGY – CONNECTION AND LINKING CRITERIA**

Participants and Regulators may access the ICE SBSDR Service through a web-based front-end that requires user systems to (a) satisfy the minimum computing system and web browser requirements specified in the ICE Trade Vault Technical Guides, (b) support HTTP 1.1 and 128-bit or stronger SSL data encryption, and (c) support the most recent version of Adobe Flash Player.

## **(3) POLICIES AND PROCEDURES TO SAFEGUARD SECURITY-BASED SWAP DATA AND OPERATIONAL RELIABILITY**

ICE SBSDR Service data is saved to a redundant, local database and a remote disaster recovery database in near real-time. The ICE SBSDR 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 SBSDR Service from the date of submission until five years after expiration of the trade (last day of delivery or settlement as defined for each product). After the initial five-year period, Participants' 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 termination date. Participants will retain unimpaired access to its online and archived trade data.

ICE Trade Vault maintains and will continue to maintain a robust emergency and business-continuity and disaster recovery plan ("Business Continuity Plan") that allows 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. In accordance with the Business Continuity Plan, all production system hardware and software is replicated in near real-time at a geographical- and vendor-diverse disaster recovery site to avoid any loss of data.

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

## **(4) DATA PRIVACY POLICIES AND PROCEDURES**

ICE Trade Vault recognizes its responsibility to ensure data confidentiality and dedicates significant resources to information security to prevent the misappropriation or misuse of Confidential Information and any other SBSDR Information not subject to public dissemination (i.e., the information identified in Exchange Act Rule 902(c)). ICE Trade Vault does not, as a condition of accepting security-based swap data from Participants, require the waiver of any privacy rights by such Participants. ICE Trade Vault maintains a security policy that sets forth technical and procedural processes for information security and contains an extensive list of policies and means of implementation.

ICE Trade Vault uses a multi-tiered firewall deployment 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 network zone behind

external firewalls. A second set of internal firewalls further isolate ICE Trade Vault database systems, while 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. In addition, the security policy imposes an accountable and standard set of best practices to protect the confidentiality of Participants' SBSDR Information, including Confidential Information and other SBSDR Information not subject to public dissemination. ICE Trade Vault completes an audit for adherence to the data security policies on at least an annual basis. The audit tests the following applicable controls, among others, to ICE Trade Vault systems: (i) logical access controls; (ii) logical access to databases; (iii) physical and environmental controls; (iv) backup procedures; and (v) change management.

## **(5) COMMERCIAL AND NON-COMMERCIAL USE OF DATA**

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

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

## **(6) DATA ACCURACY AND DISPUTE RESOLUTION**

The ICE SBSDR Service reasonably relies on the accuracy of trade data submitted by Participants. All Participants must complete a conformance test to validate data submission integrity prior to ICE Trade Vault's acceptance of actual security-based swap data and must immediately inform ICE Trade Vault of any system or technical issues that may affect the accuracy of security-based swap data transmissions.

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. If the non-Reporting Side for a security-based swap transaction discovers an error in the information reported with respect to such security-based swap, that entity shall promptly notify the Reporting-Side of the error. If the Reporting Side for a security-based swap transaction discovers an error in the information reported with respect to a security-based swap, or receives notification from a Counterparty of an error, such person shall promptly submit to the ICE SBSDR Service an amended report pertaining to the original transaction report in a manner consistent with ICE SBSDR Service policies and procedures. ICE Trade Vault will disseminate a corrected transaction report in instances where the initial report included erroneous primary trade information.

For transactions executed off Platform that are not cleared, trade data 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 SBSDR Service. When a Participant "disputes" a trade within the ICE SBSDR 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 SBSDR Service, including a "Disputed" status.

## **(7) ICE TRADE VAULT SERVICES**

The ICE SBSDR Service is a security-based swap data repository service offered by ICE Trade Vault for the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of credit derivatives trades. ICE Trade Vault offers certain Ancillary Services (i.e., services offered by ICE Trade Vault that are not core SBSDR functions) that ICE Trade Vault is required to provide pursuant to Exchange Act Rule 13n-5. These Ancillary Services include the (i) confirmation of the accuracy of the data submitted to ICE Trade Vault; and (ii) resolution of trade record errors and disputes.

## **(8) PRICING**

For the most current pricing of ICE SBSDR Service, please visit the website at [www.icetradevault.com](http://www.icetradevault.com).

## **(9) ICE TRADE VAULT GOVERNANCE ARRANGEMENTS**

ICE Trade Vault is organized as a limited liability company in the state of Delaware and is a wholly owned subsidiary of Intercontinental Exchange Holdings, Inc., which is wholly-owned by Intercontinental Exchange, Inc. ("ICE"), a publicly traded company. ICE Trade Vault is managed by a Board of Directors that is responsible for overseeing the operations of ICE Trade Vault.

The Board of Directors plays an active and important role in the oversight of all risks relating to ICE Trade Vault. The powers and authority of the Board of Directors include the ability to: (i) designate and authorize specific appointed officers to act on behalf of the Board of Directors; (ii) fix, determine and levy all fees, when necessary; (iii) prepare and amend the Guideook; (iv) act in emergencies; and (v) delegate any such power to the appropriate party. The Board of Directors oversees ICE Trade Vault's security-based swap data repository functions as well as other regulated services that ICE Trade Vault provides, such as the swap data repository registered with the CFTC.

The Board of Directors consists of at least three Directors, all of which are appointed by ICE, the ultimate parent company to ICE Trade Vault. ICE considers several factors in determining the composition of the Board of Directors, including whether directors, both individually and collectively, possess the required integrity, experience, judgment, commitment, skills and expertise to exercise their obligations of oversight and guidance over a security-based swap data repository and a swap data repository regulated by the CFTC. Additionally, in accordance with Exchange Act Rule 13n-4(c)(2), ICE Trade Vault provides participants with the opportunity to participate in the process for nominating the ICE Trade Vault Independent Director and with the right to petition for alternative candidates, as described above. Members of the Board of Directors must have the following attributes:

- a) sufficiently good reputation;
- b) requisite skills and expertise to fulfill their responsibilities in the management and governance of a security-based swap data repository;
- c) a clear understanding of such responsibilities; and
- d) the ability to exercise sound judgment regarding security-based swap data repository affairs.

At least one Director will at all times be "independent" in accordance with applicable provision(s) of the New York Stock Exchange Listed Company Manual. Two officers of ICE Trade Vault's parent, ICE, currently serve as the Non-Independent Directors.

## ***CCO Governance, Authority and Responsibility***

The CCO of ICE Trade Vault is appointed by the Board of Directors 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 with a financial report that conforms to the requirements of Exchange Act Rule 13n-11(f), which shall be provided to the SEC annually in accordance with Exchange Act Rule 13n-11(d);
- (ii) reviewing the compliance of ICE Trace Vault with respect to the requirements and core principles described in Section 13(n) of the Exchange Act and the Applicable SEC Regulations; and
- (iii) establishing and administering written policies and procedures reasonably designed to prevent violations of the Exchange Act, the core principles applicable to SBSDRs and Applicable Law.