





# DTCC Data Repository

*DTCC DATA REPOSITORY (U.S.) LLC  
SEC EXHIBIT HH2  
SUBMISSION DATE: APRIL 2017*

3.3.4	Verification Applicable to Messages Submitted Pursuant to CFTC Regulations and SEC Regulations.....	<a href="#">1847</a>
3.3.4.1	Verification Methodology Applicable to Messages Submitted Pursuant to CFTC Regulations and SEC Regulations .....	<a href="#">1847</a>
3.3.4.2	Pairing Methodology .....	19
4.	UNIQUE IDENTIFIERS .....	<a href="#">2019</a>
4.1	Overview.....	<a href="#">2019</a>
4.2	Unique Swap and Security-based Swap Identifiers/Unique Trade Identifiers .....	<a href="#">2019</a>
4.2.1	Identifiers Applicable to Submissions to the CFTC.....	<a href="#">2019</a>
4.2.2	Identifiers Applicable to Submissions to the Canadian Regulators .....	20
4.2.3	Identifiers Applicable to Submissions to the SEC .....	20
4.2.3.1	Identification Codes .....	<a href="#">2120</a>
4.2.3.2	Reporting UICs to DDR .....	22
4.2.3.3	UIC Report.....	<a href="#">2423</a>
4.3	Legal Entity Identifier (“LEI”) .....	<a href="#">2423</a>
4.4	Unique Product Identifiers (“UPIs”).....	24
5.	PUBLIC REPORTING OF SWAP AND SECURITY-BASED SWAP DATA/DATA ..	<a href="#">2524</a>
5.1	DDR Public Price Dissemination of Data - Description.....	<a href="#">2524</a>
5.1.1	Public Price Dissemination Pursuant to CFTC Regulations .....	<a href="#">2524</a>
5.1.2	Public Dissemination of Security-based Swap Data Pursuant to SEC Regulations	<a href="#">2625</a>
5.1.3	Public Price Dissemination pursuant to Canadian Regulations .....	<a href="#">2625</a>
5.1.4	Identity of Parties Not to be Disclosed.....	<a href="#">2625</a>
5.2	DDR Notification.....	<a href="#">2625</a>
5.3	Block Trade Calculation for CFTC Reporting.....	<a href="#">2625</a>
5.4	Aggregate Data Available to the Public Pursuant to Canadian Regulations .....	<a href="#">2726</a>
6.	ACCESS TO AND USE OF DATA .....	<a href="#">2726</a>
6.1	Public Data.....	<a href="#">2726</a>
6.2	Access by Designated Regulators .....	<a href="#">2726</a>
6.3	DDR Use of Swap and Security-based Swap Data Information.....	<a href="#">2726</a>
6.4	Access by Third Party Service Providers to Data Retained by DDR .....	<a href="#">2827</a>

# DTCC Data Repository

DTCC DATA REPOSITORY (U.S.) LLC  
SEC EXHIBIT HH2  
SUBMISSION DATE: APRIL 2017

6.5	Access to Data by Other Regulators and Entities .....	<a href="#">2827</a>
6.5.1	Notification.....	<a href="#">2827</a>
6.6	Access to DDR Systems and Data Generally .....	<a href="#">2827</a>
6.7	Denial of Access to Data.....	<a href="#">2928</a>
6.8	Privacy Policy and Procedures.....	<a href="#">2928</a>
7.	DDR SYSTEM.....	<a href="#">2928</a>
7.1	System Capacity .....	<a href="#">2928</a>
7.2	DDR System Availability .....	<a href="#">2928</a>
7.3	Emergency Responses .....	<a href="#">3028</a>
8.	BUSINESS CONTINUITY .....	<a href="#">3029</a>
8.1	Business Continuity and Disaster Recovery .....	<a href="#">3029</a>
8.2	Wind-Down Plan .....	<a href="#">3130</a>
9.	DATA INFORMATION SECURITY .....	<a href="#">3130</a>
9.1	Overview.....	<a href="#">3130</a>
9.2	System Safeguards .....	<a href="#">3230</a>
10.	RESOLUTION OF DISPUTES, TERMINATION & DISCIPLINARY PROCEDURES	
	<a href="#">3234</a>	
10.1	Resolution of User Disputes .....	<a href="#">3234</a>
10.1.1	Erroneous Records .....	<a href="#">3334</a>
10.1.2	Disputes Between Users.....	<a href="#">3332</a>
10.2	Denial of User Application .....	<a href="#">3432</a>
10.2.1	Application to DDR Declined.....	<a href="#">3432</a>
10.2.1.1	Hearing .....	<a href="#">3433</a>
10.2.1.2	Notices.....	<a href="#">3634</a>
10.3	Involuntary Termination Procedures .....	<a href="#">3635</a>
10.3.1	User Termination Events by DDR .....	<a href="#">3635</a>
10.3.2	Notice and Effect of Termination.....	<a href="#">3735</a>
10.3.3	Right of Appeal to Involuntary Termination.....	<a href="#">3736</a>
10.4	Other Disciplinary Actions .....	<a href="#">3837</a>
10.4.1	Restriction of Use and Costs .....	<a href="#">3837</a>
10.4.2	Procedures for Disciplinary Proceedings .....	<a href="#">3937</a>

# DTCC Data Repository

*DTCC DATA REPOSITORY (U.S.) LLC  
SEC EXHIBIT HH2  
SUBMISSION DATE: APRIL 2017*

10.5 Audits, Provision of Information and Cooperation.....	<a href="#">4038</a>
11. CONFLICTS OF INTEREST .....	<a href="#">4139</a>
11.1 General Conflict of Interest Resolution Processes.....	<a href="#">4139</a>
11.2 Director Conflicts of Interest .....	<a href="#">4139</a>
11.2.1 Reporting Conflicts of Interest.....	<a href="#">4240</a>
11.2.2 Evaluation of a Director’s Actual, Potential or Apparent Conflict of Interest	<a href="#">4341</a>
11.2.3 Resolution of Potential Conflicts of Interest.....	<a href="#">4341</a>
12. TERMS & TERMINOLOGY .....	<a href="#">4341</a>
Appendix A: Forms of User Agreement.....	<a href="#">4846</a>
Appendix B: Operating Procedures .....	<a href="#">5755</a>
DTCC DATA REPOSITORY (U.S.) LLC OPERATING PROCEDURES.....	<a href="#">5856</a>
SWAP DATA REPOSITORY .....	<a href="#">7168</a>
CANADIAN SWAP DATA REPORTING SERVICE .....	<a href="#">7672</a>
Appendix C: Information Privacy Policy of DTCC Data Repository (U.S.) LLC SDR .....	<a href="#">8076</a>

## 1. USERS' RIGHTS AND OBLIGATIONS<sup>1</sup>

---

### 1.1 User Access to DDR Services

The services offered by DTCC Data Repository (U.S.) LLC (“DDR” or the “Company”) that require registration, designation or recognition as a trade repository, swap data repository (“SDR”) or security-based swap data repository (“SBSDR”) under Applicable Law (the “SDR Services”), including in its capacity as a Securities Information Processor (“SIP”), are available to all Market Participants on a fair, open and equal basis. DDR does not impose membership qualifications on Users of its SDR Services beyond requiring execution of membership documents such as the User Agreement and the ability to comply with the technical specifications of the SDR Services as published by DDR from time to time, except as otherwise required by Applicable Law. Specifically, the SDR Services contemplate that Market Participants required to report swap and security-based swap data to a registered, designated or recognized trade repository, SDR or SBSDR in jurisdictions in which DDR operates, will be able to use the SDR Services to satisfy their reporting obligations. DDR does not expect to reject applications to become a User by Market Participants who seek to utilize its SDR Services to satisfy the Users reporting obligations or those of the Market Participant’s customers in accordance with Applicable Law, but if an application to become a User is denied, or if a User’s access is terminated, the procedures by which a User may appeal such decisions are contained in Rules 10.2 and 10.3 respectively below.

In order to be granted access to the DDR Systems, receive trade information, confirm or verify transactions, submit messages or receive reports a Market Participant must be on-boarded as a DDR User. For those Market Participants that on-board, DDR provides a mechanism for parties to access the DDR System in order to confirm and verify transactions, identify any missing information, and provide Unique Identification Code (“UIC”) information as required under ~~these procedures~~ the applicable provisions of this Rulebook. ~~These Market Participants Users~~ are required to keep information current and notify DDR of any changes to information they provided through the on-boarding process, ~~including but not limited to identifiers and any relevant internal mapping of static data.~~

The provisions of the DDR Rules do not govern, and will not preclude DDR from offering, services other than SDR Services (“Other Services”), which may include services ancillary to SDR Services, to Users and other persons, to the extent permitted by Applicable Law. For the

---

<sup>1</sup> Capitalized terms used but not otherwise defined in these rules have the meanings set forth in Rule 12.

avoidance of doubt, Other Services may be offered on terms other than those set forth herein. DDR does not and will not bundle or tie the SDR Services with any Other Services.

## 1.2 User Rules & Applicable Law

To participate in the SDR Services offered by DDR, each User must:

- (a) enter into a User Agreement in one of the forms provided in Appendix A (including, for Canadian Users, the “DDR Canada – Local Counterparty” tab in Annex I to the User Agreement); and
- (b) agree to be bound by the terms of the User Agreement and Operating Procedures (set forth in Appendix B), which incorporate terms of this Rulebook, which is an “Applicable Publication” as defined in the Operating Procedures (collectively the “DDR Rules”).

DDR and its Users are subject to all Applicable Law including Applicable Regulations relevant to the User or the transaction associated with such User. DDR may reject a Transaction Record submitted due the submission failing to meet DDR validations, including but not limited to the submission failing to be in a format that can be ingested by DDR, failing to meet jurisdictional requirements or failing to provide required data elements. A rejected submission is deemed not to have been submitted at all with respect to reporting to the jurisdiction for which it was rejected (it is possible that one Transaction Record is submitted to comply with reporting in more than one jurisdiction and may be acceptable for one jurisdiction, but rejected for the other).

## 1.3 Access User Interface & Recordkeeping

Users will be provided logins and the ability to view or receive reports and to view and provide trade details via (a) computer-to-computer links, (b) secure web interface, or (c) other means of access designated by DDR from time to time, for the purpose of effecting electronic submission of records of eligible transactions.

The interfaces will allow Users to view full trade details associated with any individual swap or security-based swap, as represented by a Unique Swap Identifier (“USI”), Unique Transaction Identifier (“UTI”) or other similar method of identification of each swap or security-based swap transaction submitted to DDR, which they have permission to view. Users must identify any errors on the trade details or missing information and promptly correct such error or provide such missing information.

An entity will be permitted to view the records relating to an individual swap or security-based swap if it is:

# DTCC Data Repository

DTCC DATA REPOSITORY (U.S.) LLC  
SEC EXHIBIT HH2  
SUBMISSION DATE: APRIL 2017

- (a) A counterparty or an authorized agent of a counterparty to the transaction; ~~or~~  
~~(b) A regulator and the transaction is reportable to that regulator; or~~  
~~(e)(b)~~ A third party agent submitter of the transaction (agents who are submitters will not be able to view the current positions, unless authorized by a counterparty to the transaction, but will be able to see the submission report to view the success / failure of messages submitted by them).

DDR will maintain an audit trail of information submitted by Users.

DDR shall retain exclusive control over the System through which the SDR Services are provided.

## 1.3.1 Recordkeeping

DDR shall maintain all information as required by Applicable Law as well as maintain swap and security-based swap data throughout the existence of the swap or security-based swap and for 15 years following termination of the swap or security-based swap or as otherwise required by Applicable Regulations. The records will be readily accessible throughout the life of a swap and security-based swap and for 5 years following its termination and shall be in an electronic format that is non-rewriteable and non-erasable. For the remainder of the retention period, the swap or security-based swap record will be retrievable within 3 business days.

### 1.3.1.1 Authorized Personnel – DDR Books and Records

Questions with regard to the types of books and records maintained by DDR in the normal course of business may be addressed to DDR's ~~Chief Executive~~Senior Officer, ~~Counsel~~counsel, Chief Compliance Officer, and/or Business Manager during normal business hours.

### 1.3.1.2 Transfer of Records

In the event DDR ceases doing business or ceases to be a registered or designated trade repository it shall continue, for a period of not less than five (5) years or upon transfer to the Designated Regulator or its designee or another registered or designated trade repository for that jurisdiction, to preserve, maintain, and make accessible to each Designated Regulator or its designee, the records and data required by Applicable Regulation.

## 1.4 User Fees

All fees imposed by DDR in connection with the reporting of swap or security-based swap data and any other supplemental or ancillary services provided shall be equitable and established in a uniform and non-discriminatory manner. DDR's Fee ~~Schedule~~Schedules will be available to all Market Participants on DDR's website. ~~All fees imposed by DDR, as approved by the DDR Board of Directors ("Board"), will be commensurate to DDR's costs for providing the System, including the SDR Services.~~



## 1.5 Limitation of Liability

Limitations on liability as between the User and DDR are contained in Section 9 of the Operating Procedures, attached hereto as Appendix B.

## 2. MANAGEMENT & CORPORATE STRUCTURE

---

### 2.1 Ownership & Structure

DDR is organized as a limited liability company under the laws of the State of New York. DDR is a wholly owned subsidiary of DTCC Deriv/SERV LLC (“Deriv/SERV”). Deriv/SERV is a wholly owned subsidiary of The Depository Trust & Clearing Corporation (“DTCC”), which is the ultimate parent of DDR.

### 2.2 Management

DDR is governed by a Board. The number of Directors on the Board shall be determined by Deriv/SERV as the sole member of DDR. The Board is composed of individuals selected from the following groups: employees of DDR’s users (either fees paying Users or End Users) with derivatives industry experience, buy-side representatives, independents, and members of senior management or the Board of DTCC. The Board will include appropriate representation by individuals who are independent as specified by Applicable Regulations. The Deriv/SERV Nominations Committee shall periodically review the composition of the Board to assure that the level of representation of Directors from Users, management and non-Users is appropriate for the interests of these constituencies in DDR. DDR welcomes suggestions from Market Participants of proposed or alternative candidates to serve on the DDR Board, which may be submitted through the Notices procedures described in the Operating Procedures Section 3 of the Important Legal Information section.

The Board reserves the right to establish committees as necessary and appropriate to manage its operations and provide strategic guidance. All relevant governance transparency documents and information required under Applicable Law will be readily accessible.

DDR Officers are selected by Deriv/SERV senior management, who must then be ratified by the DDR Board. DDR ~~Senior~~ Officers shall consist of at least a: ~~Chief Executive~~ Senior Officer (“CEO”),<sup>2</sup> Treasurer or Chief Financial Officer and a Chief Compliance Officer.

SEC Regulations require an SBSDR to be registered as a SIP. In its capacity as a SIP, DDR shall cause each U.S. DDR director, officer and employee to be fingerprinted and shall submit or cause such fingerprints to be submitted to the Attorney General of the United States for identification and appropriate processing. Non U.S. directors, officers and employees of DDR shall be requested to comply with these fingerprinting requirements.

## 2.3 Chief Compliance Officer (“CCO”)

The CCO shall have the authority and resources to develop and enforce policies and procedures necessary to fulfill the duties set forth in the Applicable Regulations of any jurisdiction in which DDR provides SDR Services. The Board is responsible for the appointment and removal of the CCO and approval of CCO compensation, which is at the discretion of the Board and effected by a majority vote. Each Designated Regulator which has jurisdiction over DDR shall be notified within two business days of the appointment or removal of the CCO. The CCO reports to the DDR ~~Chief Executive~~Senior Officer, who is responsible for supervising and recommending the compensation of the CCO. The DDR Board shall meet with the CCO at least annually. The CCO shall have supervisory authority over all staff acting at the direction of the CCO. The duties of the CCO include, but are not limited to, the following:

- (a) oversee and review DDR’s compliance with Applicable Law in jurisdictions where DDR is registered, designated, recognized or otherwise licensed;
- (b) in consultation with the Board or the ~~CEO~~Senior Officer, resolve any conflicts of interests that may arise, including, but not limited to, conflicts between business considerations and compliance requirements, conflicts between business considerations and compliance requirements for fair and open access, and conflicts between the management and members of the Board;
- (c) establish and administer written policies and procedures reasonably designed to prevent violation of Applicable Law;
- (d) take reasonable steps to ensure compliance with Applicable Law relating to agreements, contracts or transactions and confidentiality agreements entered into with foreign or domestic regulators;
- (e) establish procedures for the remediation of non-compliance issues identified by the CCO through a compliance office review, look-back, internal or external audit finding, self-reported error, or validated complaint;
- (f) notify the Board as soon as practicable upon becoming aware of a circumstance indicating that DDR, or an individual acting on its behalf, is in non-compliance with the Applicable Laws of a jurisdiction in which it operates and either; (1) the non-compliance creates a risk to a User; (2) the non-compliance creates a risk of harm to the capital markets in which it operates; (3) the non-compliance is part of a pattern of non-compliance; or (4) the non-compliance may have an impact on

DDR's ability to carry on business as a trade repository in compliance with Applicable Law.

- (g) establish and follow appropriate procedures for the handling, management response, remediation, retesting and closing of noncompliance issues;
- (h) establish and administer a written code of ethics; and
- (i) prepare and sign an annual compliance report in accordance with Applicable Regulations and associated recordkeeping.

### **2.3.1 Annual Compliance and Financial Reports**

The DDR Chief Compliance Officer shall annually prepare and sign a report that contains a description of DDR's compliance with Applicable Regulation. The Chief Compliance Officer shall submit the annual compliance report to the Board for its review prior to the filing of the report. The report, which shall be filed with the Designated Regulators within 60 days of DDR's fiscal year-end, shall include such information as may be required under Applicable Regulations and signed by the CCO. The DDR Chief Compliance Officer shall also file, or cause to be filed, a financial report of DDR in conjunction with the annual compliance report, where required by Applicable Regulation.

### **2.4 Duty to Monitor, Screen and Analyze Swap and Security-based Swap Data**

Consistent with Applicable Regulation, DDR shall establish and maintain sufficient information technology, staff and other resources to fulfill the ability to monitor, screen and analyze all swap and security-based data recorded by DDR in such manner as the Designated Regulators may require. DDR will provide access only to such authorized parties that are specified by the Designated Regulators, according to Applicable Regulations. In addition, DDR will maintain and provide a list of authorized parties in the manner and frequency required by Applicable Regulation. DDR shall provide Designated Regulators with monitoring tools and other access to swap and security-based swap data in a manner that is substantially similar to the capabilities developed for internal use, which will be accessible only by authorized parties.

Consistent with Applicable Regulation, DDR has the capacity and will maintain the capacity to:

- (i) monitor swap and security-based swap data;
- (ii) build reports for analysis of swap and security-based swap data;
- (iii) send completed reports to its Designated Regulators as applicable;
- and (iv) accept monitoring, screening, and analysis requests from its Designated Regulators.

## 3. USER SUBMISSION OF DATA

---

### 3.1 Asset Classes

DDR will provide Market Participants with the ability to submit data for over-the-counter (“OTC”) derivatives for Credits, Equities, Rates, Foreign Exchange (“FX”) and other Commodity asset classes.

### 3.2 Connectivity

With regard to User connectivity, specifications and requirements, please see the DDR Operating Procedures as set forth in Appendix B.

### 3.3 Transactional Data and Submission Processing

#### 3.3.1 General; Message Types

The SDR Services are designed to support required public price dissemination, and regulatory data reporting for regulators including, primary economic terms, primary and secondary data, confirmation data, valuation data, original swap termination data and other continuation data whether reported via discrete transactions or point-in-time position snapshots as well as any other derivatives data required to be reported to a trade repository as specified by any Designated Regulator. The SDR Services will support the submission of data in the manner acceptable (including, where applicable, separate or combined messages) pursuant to Applicable Regulations and as described in the Applicable Publications provided to Users on DDR’s website.

DDR’s policies and procedures are designed to prevent any provision in a valid swap or security-based swap from being invalidated or modified. The DDR System and controls are regularly monitored and audited to ensure compliance with such policies and procedures and to ensure that adequate system-wide protections are in place.

#### 3.3.2 Reporting Parties and Trusted Sources

To enable reporting parties under Applicable Regulations to meet their reporting obligation or make voluntary submissions, DDR ~~will support~~ supports a variety of Market Participants, including but not limited to the following entity types:

- Trade counterparties
- DCOs

































## 5.4 Aggregate Data Available to the Public Pursuant to Canadian Regulations

DDR will provide aggregate data on open positions pursuant to the Canadian Regulations. DDR will also make transaction level reports of aggregated transactions available to the public pursuant to the Canadian Regulations.

## 6. ACCESS TO AND USE OF DATA

---

### 6.1 Public Data

Public Data shall be available in accordance with Applicable Regulations and accessible on DDR's website as further specified in Section V of the Appendices to the Operating Procedures as set forth in Appendix B.

### 6.2 Access by Designated Regulators

Pursuant to Applicable Law, the Designated Regulators, as well as any designee of the Designated Regulators, including another registered entity, shall be provided with direct electronic access to ~~DDR~~ data reported to DDR in satisfaction of such Designated Regulator's regulatory mandate in order to satisfy their legal and regulatory obligations. ~~Access to U.S. DDR data to other domestic or foreign regulators or appropriate third parties shall be governed by Applicable Regulations.~~

### 6.3 DDR Use of Swap and Security-based Swap Data Information

As part of the SDR Services, DDR receives and collects swap and security-based swap data in the ordinary course of its business from various Market Participants and registered entities for the purpose of maintaining a centralized recordkeeping facility for swaps and security-based swaps. The collection and maintenance of this data is designed to enhance the transparency, promote standardization and reduce systemic risk by making this data available to regulators and the public pursuant to Applicable Law. Therefore, access to ~~U.S. swap or security-based swap~~ data maintained by DDR to Market Participants is generally prohibited, except to either counterparty to that particular swap or security-based swap, such counterparty's authorized third party service providers or other parties specifically authorized by the User or counterparty pursuant to Rule 1.3, or 6.4, or to ~~Appropriate Domestic or Foreign Regulators~~ other regulators or entities in accordance with ~~Applicable Regulation and~~ Rule 6.5 below.

~~It is neither the current purpose nor intent of DDR to engage in any commercial use of nonpublic data relating to SDR Services.~~ DDR shall not, as a condition of the reporting of swap and security-based swap transaction data, require a Reporting Party to consent to the use of reported

data for commercial or business purposes. DDR shall not make commercial use of real-time swap data prior to its public dissemination.

## 6.4 Access by Third Party Service Providers to Data Retained by DDR

Third-party access to ~~DDR~~ data maintained by DDR is permissible provided the following conditions have been satisfied in addition to any other provisions of Applicable Regulations:

- (a) DDR and the third-party service provider to DDR shall have strict confidentiality procedures that protect data and information from improper disclosure; and
- (b) DDR and the third-party service provider shall enter a “Confidentiality Agreement” setting forth minimum confidentiality procedures and permissible use of the information maintained by DDR which are equivalent to DDR’s privacy procedures.

## 6.5 Access to ~~U.S.~~ Data by Other Regulators and Entities

~~Any regulator seeking~~Prior to providing the access contemplated by this section, any entity authorized by Applicable Law to receive access to data held by DDR shall ~~be subject to the regulations applicable to the data being requested and shall apply for access by filing~~(a) have entered into an MOU or other arrangement addressing confidentiality (“Confidentiality Agreement”), as required under Applicable Law, (b) file a request for access with DDR ~~and certifying, wherein the entity specifically describes the data sought and certifies, in a manner acceptable to DDR, that the entity is acting within the scope of its jurisdiction in a manner acceptable to DDR. Designated Regulators are not subject to these requirements with respect to data that is submitted to jurisdiction and Confidentiality Agreement, and (c) provide~~ additional information required by DDR for the purpose of compliance with the respective Designated Regulator’s regulations. For access to all other data, such Designated Regulators are subject to Applicable Regulations governing such access to fulfill the request.

### 6.5.1 Notification

DDR shall promptly notify the Designated Regulator, each as appropriate, regarding any request received by a regulator to gain access to ~~swap or security-based swap~~ data maintained by DDR pursuant to the Designated Regulator’s respective Applicable Regulations. Such notification shall be provided to each Designated Regulator in such form as they may require. Once DDR has provided the Designated Regulator with such notification and the requirements set forth in Section 6.5 have been met, DDR shall provide access to the requested swap or security-based swap data.

## 6.6 Access to DDR Systems and Data Generally

Any request for access to DDR Systems or ~~Data~~data, other than as noted above, shall be reviewed by DDR ~~Counsel~~counsel in accordance with DDR’s Rules and Applicable Law.

Requestors and relevant Designated Regulators will be notified in writing of a valid request and with respect to a denial or limitation of such access.

## **6.76.7 Denial of Access to Data**

In the event a request for access to data made pursuant to Section 6.2-6.6 is denied by DDR, the party making the request (the “Subject Party”) shall be notified of the grounds for the denial (the “Data Access Denial Notice”). It shall thereafter be the responsibility of the Subject Party to address the issues identified in the Data Access Denial Notice and resubmit the application in accordance with the applicable provisions of Section 6.

## **6.8 Privacy Policy and Procedures**

Please see “Information Privacy Policy of DTCC Data Repository (U.S.) LLC SDR” in Appendix C.

## **7. DDR SYSTEM**

---

### **7.1 System Capacity**

Consistent with Applicable Law, the DDR System is designed to provide reliable, secure and adequate scalable capacity sufficient to perform the functions of an SDR. DDR conducts routine assessments of the capacity of the DDR System, including measuring peak and average system usage against projected usage, and also considers the anticipated impact of system changes in relation to current and future DDR System capacity.

### **7.2 DDR System Availability**

The DDR System is available 7 days per week, 24 hours per day Monday through Sunday, except from 10:00 pm (ET) Saturday to 6:00 am (ET) Sunday to enable maintenance to be performed on the DDR System (“Closed Hours”). On occasion, as necessary to support time sensitive processes or maintenance occurring outside of Closed Hours, DDR Systems may be unavailable for processing (“Unscheduled Downtime”). Data submitted during DDR System Unscheduled Downtime is stored and processed once the service has resumed. If during Unscheduled Downtime DDR cannot receive and hold in queue transaction information that was required to be reported pursuant to Applicable Regulations, it will immediately upon resumption of processing operations provide an Important Notice pursuant to the Operating Procedures notifying Users that it has resumed normal operations.

## 7.3 Emergency Responses

DDR retains the right to exercise emergency authority in the event of circumstances determined by DDR to require such response or upon request by the Designated Regulators as applicable. Any exercise of DDR's emergency authority shall be adequate to address the nature and scope of any such emergency. The ~~CEO~~Senior Officer of DDR shall have the authority to exercise emergency authority and in his/her absence, any other officer of DDR shall have such authority.

Circumstances requiring the invocation of emergency authority include, but are not limited to, occurrences or circumstances:

- (a) determined by DDR to constitute an emergency;
- (b) which threaten the proper functioning of the DDR System and the SDR Services; or
- (c) which materially and adversely affect the performance of the DDR System and the SDR Services.

Emergencies include but are not limited to natural, man-made and information technology emergencies. DDR shall notify the Designated Regulators, as soon as reasonably practicable, of an invocation of emergency authority or a material system outage is detected by DDR. Such notification shall be provided in accordance with Applicable Regulations and will include the reasons for taking such emergency action, how potential conflicts of interest were minimized and documentation of the decision-making process.

Documentation underlying the emergency shall be made available to the Designated Regulators upon request.

DDR shall avoid conflicts of interest in decision-making with respect to an emergency authority taken. If a potential conflict of interest arises, the CCO shall be notified and consulted for the purpose of resolving the potential conflict. DDR shall issue an Important Notice as to all Users as soon as reasonably practicable in the event such emergency authority is exercised. Any emergency actions taken by DDR may be terminated by the ~~CEO~~Senior Officer and in his/her absence, any other officer of DDR. Such termination of an emergency action will be followed by the issuance of an Important Notice as soon as reasonably practicable.

## 8. BUSINESS CONTINUITY

---

### 8.1 Business Continuity and Disaster Recovery

The DDR System is supported by DTCC and relies on the disaster recovery program maintained by DTCC. DDR follows these key principles for business continuity and disaster recovery,

which enable DDR to provide timely resumption of critical services should there be any disruption to DDR business:

- (a) Achieve recovery of critical services within a four-hour window with faster recovery time in less extreme situations;
- (b) Disperse staff across geographically diverse operating facilities;
- (c) Operate multiple back-up data centers linked by a highly resilient network technology;
- (d) Maintain emergency command and out-of-region operating control;
- (e) Utilize new technology which provides high-volume, high-speed, asynchronous data transfer over distances of 1,000 miles or more;
- (f) Maintain processes that mitigate marketplace, operational and cyber-attack risks;
- (g) Test continuity plan readiness and connectivity on a regular basis, ensuring that Users and third party vendors/service providers can connect to our primary and back-up sites;
- (h) Communicate on an emergency basis with the market, Users and government agency decision-makers; and
- (i) Evaluate, test and utilize best business continuity and resiliency practices.

## **8.2 Wind-Down Plan**

In order to satisfy applicable regulatory requirements, DDR maintains written rules, policies and procedures reasonably designed to facilitate its orderly wind-down. Such rules, policies and procedures are approved by its Board and shared with its regulators. These rules, policies and procedures are contained in the form of a Wind-Down Plan. The plan is designed to address critical operations and services performed as a going concern during a wind-down period and to assess the effectiveness of a full range of options for an orderly wind-down.

## **9. DATA INFORMATION SECURITY**

---

### **9.1 Overview**

DDR will be responsible for monitoring the performance of DTCC in regard to implementation and maintenance of information security within its infrastructure.

## 9.2 System Safeguards

DTCC has established a Technology Risk Management team, whose role is to manage information security risk and ensure the availability, integrity and confidentiality of the organization's information assets.

Various policies have been developed to provide the framework for both physical and information security and are routinely refreshed. The Technology Risk Management team carries out a series of processes to endeavor to ensure DDR is protected in a cost-effective and comprehensive manner. This includes preventative controls such as firewalls, appropriate encryption technology and authentication methods. Vulnerability scanning is used to identify high risks to be mitigated and managed and to measure conformance against the policies and standards.

Standards for protecting Company information are based upon the sensitivity level of that information. Control standards specify technical requirements for protection and end user handling of information while in use, transmission, and storage.

Verification of accuracy of information received or disseminated by the DDR System is completed systemically. Upon receipt, all data is subject to verification of the submitter. The submitter must be recognized by the DDR System and the submitter must be eligible to submit records. For example, a Market Participant may submit records on its own behalf or a SEF may submit records on behalf of Market Participants. The actual records must then meet all data format and content requirements.

## 10. RESOLUTION OF DISPUTES, TERMINATION & DISCIPLINARY PROCEDURES

---

### 10.1 Resolution of User Disputes

Transaction data that has been submitted to DDR must be complete and accurate. In order to satisfy this requirement, DDR employs the verification and dispute processes set forth in this Rulebook. These processes are designed to allow the non-reporting User opportunity to verify the accuracy of the transaction information submitted by the Reporting Party. This also provides those non-reporting Users with minimum technology capabilities a simplified method of verifying the accuracy of transactions submitted on their behalf.

The procedures and dispute resolution processes with regard to User submissions or maintenance of erroneous information, which are subject to Applicable Regulations and, in particular, the 48-hour correction period, are as follows.



## 10.1.1 Erroneous Records

Upon submission, the DDR System will perform validation checks to ensure that each submitted record is in the proper format and will also perform validation and consistency checks. If the record fails these validation or consistency checks, the record will be rejected and such rejection status will be communicated to the User(s) to correct and re-submit.

In the event that both counterparties to a trade agree that data submitted to DDR contains erroneous information (e.g., through a mutual mistake of fact), such Users may each submit a cancel record, effectively cancelling the incorrect Transaction Record. If a Transaction Record has been submitted by only one counterparty and it is determined by the submitting User that it is erroneous, the submitting User may submit a cancel record. A User may only cancel its own submitted record; it cannot cancel a record where it is not the submitting party of the record. In circumstances where the User disputing the information is not the submitter, the User must submit a dispute record as described in 10.1.2. Where the original record was submitted by a Trusted Source, only such Trusted Source may cancel the original record (but without prejudice to the rights of such counterparties to provide relevant continuation data to the extent they are otherwise permitted or required to provide such data). DDR shall maintain a record of all corrected errors pursuant to Applicable Regulations and such records shall be available upon request to the applicable Designated Regulator.

## 10.1.2 Disputes Between Users

The SDR Services will ~~make available~~ provide trade detail reports that will enable Users to view all Transaction Records, including records submitted by the User and records submitted for a trade allegedly identifying the User as a counterparty to the trade. These reports will allow Users to reconcile the Transaction Records in the SDR Services to their own risk systems.

The Users shall be responsible for resolving any disputes between themselves uncovered during the reconciliation process and, as appropriate, submitting correct information pursuant to Rule 3.3.4 above. The disputed status will remain until the Reporting Party updates the transaction.

All reports and Transaction Records provided to Designated Regulators will include the status of these Transaction Records, including dispute and verification status, thus making such disputes visible to the relevant Designated Regulator and incentivizing the parties to the transaction to resolve the dispute. Where DDR has received conflicting or inconsistent records from more than one submitter in respect of a particular transaction (such as from a SEF and a Reporting Party), DDR will maintain all such records (unless cancelled or modified in accordance with the terms hereof) and will make such records available to Designated Regulators in accordance with the terms hereof and Applicable Law.

## 10.2 Denial of User Application

This Rule 10.2 outlines the process required for DDR to decline the request (an “Application”) of an applicant (an “Applicant”) to become a User of ~~the~~all or any SDR Services. Applicants may be denied access to the DDR System if required pursuant to Applicable Law (e.g., sanctions administered and enforced by the U.S. Department of Treasuries Office of Foreign Assets Control (“OFAC”) or the Canadian Government’s Office of the Superintendent of Financial Institutions (“OSFI”). Applicants to DDR shall be entitled to notice and an opportunity for a hearing in the event that DDR declines an Application. An Applicant may be declined if required by Applicable Law. DDR shall promptly notify all Designated Regulators should an Applicant be denied access to SDR Services, or limited in respect of access to services offered, directly or indirectly. If the denial of an Application is reversed, such Application will be accepted and the Applicant granted access following completion of on boarding requirements.

### 10.2.1 Application to DDR Declined

In conjunction with the denial of an Application, DDR shall furnish the Applicant with a written statement setting forth the grounds for the determination (the “~~Denial Notice~~”). ~~The Denial Notice shall inform the Applicant of its right to request a~~DDR Denial Notice). In case of a denial related to DDR as a SIP, DDR shall furnish the SEC with notice of the denial in such form and containing such information as prescribed by the SEC (the “SIP Denial Notice”), which notice shall be subject to review by the SEC on its own motion, or upon application by the denied Applicant pursuant to Section 11A of the Securities Exchange Act of 1934. If the SEC does not dismiss the proceeding to review the SIP Denial Notice or if the SEC by order sets aside the SIP Denial Notice and requires DDR to permit the Applicant access to all or any SDR Services offered by DDR as a SIP, then DDR shall comply with such order, or shall take such further action as may be afforded DDR under Applicable Law.

The DDR Denial Notice shall inform the Applicant of its right to request a DDR hearing with respect to the determination pursuant to Rule 10.2.1.1.

#### 10.2.1.1 Hearing

(a) To request a hearing on a denial of an Application, an Applicant shall file such a request (the “Hearing Request”) with the Secretary of DDR within 5 business days of receipt of the Denial Notice. The Hearing Request must set forth: (i) the action to be taken by DDR as set forth in the Denial Notice; and (ii) the name of the representative of the Applicant who may be contacted with respect to a hearing.



denial; (ii) the expiration of the applicable time period provided for the filing of a Hearing Notice and/or Applicant Statement; or (iii) when the Decision Notice is delivered to the Applicant. Notwithstanding the foregoing, the Board may in its discretion modify any sanctions imposed or reverse any decision of the Panel that is adverse to an Applicant. The reversal or modification by the Board of a Panel decision or reversal or modification by the Panel of any action by DDR shall not provide such Applicant with any rights against DDR or its officers or Directors for determination made prior to such reversal or modification.

## **10.2.1.2 Notices**

(a) A Denial Notice and Decision Notice shall be sufficiently served if in writing and delivered by courier or U.S. mail to the office address or emailed to the email address provided by such Applicant. Any notice, if mailed by U.S. mail, shall be deemed to have been given when received by the Applicant and any notice emailed will be deemed to have been given upon transmission.

(b) A Hearing Request and Applicant Statement shall be sufficiently served on DDR if in writing and delivered by courier or U.S. mail or emailed to the following address:

DTCC Data Repository (U.S.) LLC  
55 Water Street  
New York, New York 10041  
Attention: Counsel  
ddrnotices@dtcc.com

Any notice in writing to DDR shall be deemed to have been given when received by DDR.

## **10.3 Involuntary Termination Procedures**

### **10.3.1 User Termination Events by DDR**

DDR may summarily terminate a User's account and access to the SDR Services when the Board determines: (a) that the User has materially breached its User Agreement, the DDR Operating Procedures or the rules contained in this Rulebook, which threaten or may cause immediate harm to the normal operation of the System, or any Applicable Law including those relating to the regulations administered and enforced by OFAC or OSFI; or (b) User's account or User's IT system is causing material harm to the normal operation of the System. In addition, DDR can recommend termination to the Board, for example, for failure to pay fees when due. DDR's rights under this Rule 10.3 will be in addition to and separate from its rights under Rule 10.4.

In addition, the following actions must take place before DDR staff initiates any actions which may result in a User's termination of access to the DDR System and, specifically, the SDR Services: (a) DDR senior management, as well as DDR's Counsel and CCO, must be involved in any decision to involuntarily terminate a User; and (b) the Chairman of the Board of DDR must be notified in advance of any involuntary termination.

Upon the summary termination of a User's access pursuant to this Rule 10.3, DDR shall, as soon as possible, notify the impacted User of the termination in writing or via email. Such notice shall state, to the extent practicable, in general terms how pending transaction submissions and other pending matters will be affected and what steps are to be taken in connection therewith.

Additionally, DDR staff will take required action to cancel the digital certificates of individuals with access to the terminating User's data.

### **10.3.2 Notice and Effect of Termination**

(a) Upon the summary termination of a User's access pursuant to this Rule 10.3, DDR shall, as soon as possible, notify all Users of the termination. Such notice shall state to the extent practicable in general terms how pending transaction submissions and other pending matters will be affected and what steps are to be taken in connection therewith. Such termination shall be effective notwithstanding any appeal thereof pursuant to Rule 10.3.3 unless and until such termination is modified or rescinded pursuant to Rule 10.3.3.

(b) Pending Submissions: Notwithstanding any other provision of the DDR Rules, DDR shall have no obligation to accept any submission of a terminated User that was affected after the time at which User was terminated from access to the System.

### **10.3.3 Right of Appeal to Involuntary Termination**

A User whose access to the SDR Services has been terminated pursuant to Rule 10.3 shall be entitled, upon request, to a written statement of the grounds for its termination and shall have the right to appeal its termination of access in accordance with the procedure described below.

(a) A terminated User may appeal its termination of access by filing a written notice of appeal within 5 business days after the date of termination of access.

(b) Appeals shall be considered and decided by the Appeal Panel (a panel comprised of a Chairman and two individuals appointed by the Chairman of the Board to consider appeals under Rule 10.3 and the DDR Rules). ~~Appeal~~Appeals shall be heard as promptly as possible, and in no event more than 5 business days after the filing of the notice of

appeal. The appellant shall be notified of the time, place and date of the hearing not less than 3 business days in advance of such date. At the hearing, the appellant shall be afforded an opportunity to be heard and to present evidence in its own behalf, and may, if it so desires, be represented by counsel. As promptly as possible after the hearing, the Appeal Panel shall, by the vote of a majority of its members, affirm or reverse the termination of access or modify the terms thereof. The appellant shall be notified in writing of the Appeal Panel's decision; and if the decision shall have been to affirm or modify the termination, the appellant shall be given a written statement of the grounds therefor.

- (c) Any decision by the Appeal Panel to affirm or modify a termination shall be reviewable by the Board on its own motion or on written demand by the appellant filed with DDR within 3 business days after receipt of notice of the Appeal Panel's decision. The Board may, but is not required to, afford the appellant a further opportunity to be heard or to present evidence. The appellant shall be notified in writing of the decision of the Board, and if the decision shall have been to affirm or modify the termination, the appellant shall be given a written statement of the grounds therefor.
- (d) The filing of an appeal pursuant to this Rule shall not impair the validity or stay the effect of the termination appealed from. The reversal or modification of a termination shall not invalidate any acts of DDR taken pursuant to such termination prior to such reversal or modification, and the rights of any person which may arise out of any such acts shall not be affected by such reversal or modification.
- (e) A record shall be kept of any hearing held pursuant hereto. The cost of the transcript may, in the discretion of the body holding the hearing, be charged in whole or in part to the terminated User in the event that the termination ~~toof~~ access is finally affirmed.

## **10.4 ~~Sanctions from~~ Other Disciplinary ~~Proceedings~~ Actions**

### **10.4.1 ~~Imposition~~ Restriction of ~~Sanctions~~ Use and Costs**

(a) DDR, at the request of any DDR officer and agreed to by DDR's ~~CEO~~ Senior Officer and CCO, ~~and subject may temporarily deny access to the procedures below, may~~ enure, suspend, expel or limit the activities, functions or operations of, and/or otherwise impose ~~a fine~~ restrictions on, ~~the use of the DDR System on~~ a User, ~~or take such other actions as DDR deems reasonably necessary to protect its systems and other Users,~~ for: (i) a violation of the DDR Rules (including failure to pay fees when due); (ii) any neglect or refusal by such User to comply with any applicable order or direction of DDR; or (iii) any error, delay or other conduct that materially and adversely affects the operations of DDR: ~~(each a "Subject Event")~~. Limits to

the activities, functions or operation of Users may include, but are not limited to, access to the DDR System or ability to submit data via a non-approved source (e.g., temporarily suspending the submission queue, where inbound messaging is at issue, while still allowing the User to maintain access to the web interface and allowing for submissions via other network services such as a spreadsheet upload). Notwithstanding the foregoing, in the event of a Subject Event and in addition to any other action taken by DDR, DDR may assess such User with all costs incurred by DDR in connection with such Subject Event and apply any deterrent charges that DDR deems necessary.

(b) DDR shall provide prompt notice to the applicable Designated Regulators of any action taken in accordance with this Rule or any terminations pursuant to Rule 10.3.

## 10.4.2 Procedures for Disciplinary Proceedings

(a) Before any ~~sanction~~disciplinary action in accordance with Rule 10.4.1 is ~~imposed~~taken, DDR shall furnish the subject User ~~against whom the sanction is sought to be imposed~~ (“Respondent”) with a concise written statement of the charges against the Respondent. However, no prior written statement shall be required to be provided if the action is being taken by DDR in response to protecting the security of data, the DDR System or other Users. In such circumstances, a written statement shall promptly follow the DDR action. The Respondent shall have 10 business days after the service of such statement to file with DDR a written answer thereto. The answer shall admit or deny each allegation contained in the statement of charges and may also contain any defense which the Respondent wishes to submit. Allegations contained in the statement of charges which are not denied in the answer shall be deemed to have been admitted, and any defense not raised in the answer shall be deemed to have been waived. If an answer is not provided to DDR within the time permitted, as determined by the CCO, in consultation with DDR’s Counsel, the allegations shall be deemed to have been admitted, and the Respondent will be notified in writing of any ~~sanction~~disciplinary action that shall be ~~imposed~~taken. If an answer is timely filed, DDR shall (unless the Respondent and DDR shall have stipulated to the imposition of an agreed ~~sanction~~disciplinary action) schedule a hearing before a panel comprised of a Chairman and 2 (two) individuals appointed by the Chairman of the Board to conduct disciplinary proceedings under this Rule (“Disciplinary Panel”). At the hearing, the Respondent shall be afforded the opportunity to be heard and to present evidence on its behalf and may be represented by counsel. A record of the hearing shall be prepared and the cost of the transcript may, in the discretion of the Disciplinary Panel, be charged in whole or in part to the Respondent in the event any ~~sanction is imposed on~~disciplinary action is taken against the Respondent. As soon as practicable after the conclusion of the hearing, the Disciplinary Panel shall furnish the Respondent and the Board with a written statement of its decision. If the decision is to ~~impose a take~~ disciplinary ~~sanction~~action, the written statement shall set forth the

# DTCC Data Repository

*DTCC DATA REPOSITORY (U.S.) LLC  
SEC EXHIBIT HH2  
SUBMISSION DATE: APRIL 2017*

~~sanction~~disciplinary action being ~~imposed~~taken and the facts surrounding the violation of these Rules.

(b) In the event that the Disciplinary Panel censures, fines, suspends, expels or limits the activities, functions or operations of any Respondent, any affected User may apply for review to the Board, by written motion filed with DDR within 5 business days after issuance of the Disciplinary Panel's written statement of its decision.

(c) The granting of any such motion shall be within the discretion of the Board. In addition, the Board may determine to review any such action by a Disciplinary Panel on its own motion. Based upon such review, the Board may affirm, reverse or modify, in whole or in part, the decision of the Disciplinary Panel. The Respondent shall be notified in writing of the decision of the Board which shall be final. Once a decision of the Disciplinary Panel is final, the CCO will facilitate and coordinate the administration of any such ~~sanctions imposed~~disciplinary action taken as a result of such disciplinary proceedings.

(d) Any time limit set forth in this Rule may be extended by the body having jurisdiction over the matter in respect of which the time limit is imposed.

(e) The summary termination of access by a User pursuant to Rule 10.3 shall not be deemed to be a "~~sanction~~disciplinary action" within the meaning of this Rule, and the provisions of this Rule shall be inapplicable to any such summary termination.

## **10.5 Audits, Provision of Information and Cooperation**

Subject to Applicable Law, each User will comply with all reasonable requests by DDR for information, documentation or data concerning such User and related to such User's use of the System as DDR may deem necessary. DDR will have the right to audit or inspect a User (and its facilities) with respect to its use of the System, upon reasonable notice, and Users shall cooperate with such audits or inspections and with other inquiries by DDR concerning their use of the System.

The CCO or his/her delegate shall have authority to investigate any potential rule violation, shall be responsible for enforcing sanctions related to violations and for following the procedures outlined in Rule 10.4.



## 11.CONFLICTS OF INTEREST

---

### 11.1 General Conflict of Interest Resolution Processes

DDR utilizes a conflict of interest resolution process that is reasonably designed to identify and mitigate potential and existing conflicts of interest in DDR's decision-making process on an ongoing basis, as required by Applicable Law.

All conflicts of interest, including all potential conflicts of interest, involving the officers, employees, consultants and temporary employees of DDR ("DDR Staff") are escalated to the DDR Chief Compliance Officer except in cases where the DDR Chief Compliance Officer has a conflict of interest, in which case the matter shall be directed to the attention of DDR's Chief ExecutiveSenior Officer and the Chairman of the DDR Audit Committee. The DDR Chief Compliance Officer, in consultation with the DDR Audit Committee, will resolve all conflicts of interest. Any conflict of interest not resolved by the DDR Audit Committee shall be escalated to the DDR Board for resolution.

When resolving conflicts of interest, the DDR Chief Compliance Officer, DDR's Senior Officer, the DDR Audit Committee and the DDR Board ("Responsible Parties") consider all relevant facts and circumstances. The Responsible Parties, as applicable, will determine whether to require the DDR Staff member to recuse himself or herself from any decisions involving the matter in which he or she has a conflict of interest or take any other action that is deemed appropriate.

### 11.1.12 Director Conflicts of Interest

A Director conflict of interest is present whenever the interests of the Company compete with the interests of a Director, the Director's employer, or any other party with which a Director is associated, or otherwise whenever a Director's corporate or personal interests could be reasonably viewed as affecting his or her objectivity or independence in fulfilling the Director's duties to the Company.

While it is not possible to anticipate all possible conflict situations, conflicts of interest typically arise whenever a Director, an immediate family member or other personal associate of a Director or a firm with which a Director is associated as a Director, officer, employee or beneficial owner of 1% or more of the firm's equity interests, has (directly or indirectly) a business interest in a party with whom the Company is doing business in some capacity other than as a User or in a transaction or other activity that competes (directly or indirectly) with a transaction or activity which the Company is pursuing or conducting.

Situations involving potential conflicts of interest may also include instances in which a Director, an immediate family member or other personal associate of a Director, or a firm with

which a Director is associated as a Director, officer, employee or beneficial owner, has (directly or indirectly):

- (a) a compensation arrangement (other than with respect to fees payable to a Director in his or her capacity as an employee or Director) or other interest in a transaction with the Company;
- (b) a compensation arrangement or other interest in or affiliation (subject to *de minimis* exceptions) with any entity or individual that: (a) sells goods or services to, or purchases goods or services from, the Company; or (b) the Company has, or is negotiating, or contemplating negotiating, any other transaction or arrangement;
- (c) used his or her position, or confidential information or the assets of the Company to his or her (or an associated party's) personal advantage or for an improper or illegal purpose;
- (d) solicited or accepted any gift, entertainment, or other favor where such gift might create the appearance of influence on the Director (other than gifts of nominal value, which are clearly tokens of respect and friendship unrelated to any particular transaction or arrangement);
- (e) acquired any property or other rights in which the Company has, or the Director knows or has reason to believe at the time of acquisition that the Company is likely to have, an interest;
- (f) taken advantage of an opportunity related to the activities of the Company that is available to the Company or to the Director, unless the Board has made an informed decision that the Company will not pursue that opportunity;
- (g) a business interest that is affected by any transaction, arrangement, or decision involving the Company; or
- (h) any other circumstances that may, in fact or in appearance, make it difficult for the Director to exercise independence, objective judgment or otherwise perform effectively.

## **11.2.1 Reporting Conflicts of Interest**

Conflict identification and analysis can be difficult and, therefore, Directors are at all times expected to act on the side of caution and immediately bring to the attention of the Chief Compliance Officer and either the Chairman of the Board or the Counsel any matters that may involve conflicts of interest or be reasonably perceived by others to raise questions about potential conflicts even if the person does not believe that an actual conflict exists. Disclosures should be made in advance, before any action is taken on the matter.

In addition, each Director shall complete an annual Questionnaire Concerning Conflicts of Interest, disclosing any actual, potential, or apparent conflicts. They shall also promptly disclose any relevant change in circumstances. The Questionnaires shall be reviewed by the Company's Counsel and the Chief Compliance Officer.

## **11.32.2 Evaluation of a Director’s Actual, Potential or Apparent Conflict of Interest**

The Chief Compliance Officer, in consultation with the Chairman of the Board or the Counsel, as appropriate, shall evaluate Director conflict disclosures and make other necessary inquiries to determine the extent and nature of any actual or potential conflict of interest, consulting with the Chairman of the Board or the Counsel as appropriate. If appropriate, the Chief Compliance Officer shall consider alternatives to the proposed transaction or arrangement and consult with the Board when needed. A director's conflict of interest may, in appropriate circumstances, require the director's recusal from discussion or voting.

## **11.42.3 Resolution of Potential Conflicts of Interest**

The Company may enter into a transaction or other arrangement in which there is an actual or potential conflict of interest only if at a duly held Board meeting a majority of those Directors (if a quorum is present at such time) who have no interest in the transaction or arrangement approve the transaction or arrangement after determining, in good faith and after reasonable inquiry, that:

- (a) entering into the transaction or arrangement is in the best interests of the Company, while considering the Company’s purpose and resources, and the possibility of creating an appearance of impropriety that might impair the confidence in, or the reputation of, the Company (even if there is no actual conflict or wrongdoing);
- (b) the transaction or arrangement in its entirety, and each of its terms, are fair and reasonable to the Company, after consideration of available alternatives;
- (c) the transaction or arrangement furthers the Company’s purpose; and
- (d) the transaction or arrangement is not prohibited by law or regulation.

## **12. TERMS & TERMINOLOGY**

---

**Applicable Law** – Any and all applicable laws and regulations, judicial orders and decisions, and rules, regulations, interpretations and protocols, as amended from time to time in a jurisdiction in which DDR is registered, designated, recognized or otherwise licensed as a trade repository

**Applicable Publications** – those documents designated by DDR as “Applicable Publications” pursuant to the Operating Procedures. Such documents include message specifications and upload templates.

**Applicable Regulations** – Regulations promulgated by Designated Regulators









## APPENDIX A: FORMS OF USER AGREEMENT

---

1. Repository User Agreement
2. Repository User Agreement for View-Only Access
3. Repository Supplement to the User Agreement





















## APPENDIX B: OPERATING PROCEDURES

---

1. DTCC Data Repository (U.S.) LLC Operating Procedures
2. Swap Data Repository Appendix to the DTCC Data Repository (U.S.) LLC Operating Procedures
3. Canadian Repository Appendix to the DTCC Data Repository (U.S.) LLC Operating Procedures

## DTCC DATA REPOSITORY (U.S.) LLC OPERATING PROCEDURES

### 1. Introduction

DTCC Data Repository (U.S.) LLC (the “Company” or “DDR”), a New York limited liability company, has entered into User Agreements with various institutions that are potential users (each, a “User”) of one or more services (each, a “Service”) to be provided by the Company. The automated systems or other mechanisms through which the Company provides the Services are referred to herein as the “System.”

As used in these Operating Procedures, the term “User” shall also include a Third Party Submitter as defined in the Appendices to these Operating Procedures, except as provided therein or as the context may otherwise require.

### 2. User Information; Non-Repudiation

- a. The Company will maintain for the benefit of Users a database that (A) assigns to each User a unique alpha-numeric identifier and (B) groups Users into families (each, a “Family”) as directed by the Users (through User Agreements or in such other manner as designated by the Company from time to time) that desire to be so grouped. (The Company may use for this purpose a uniform counterparty identifier, such as a Legal Entity Identifier or Global Markets Entity Identifier, or similar identifier provided or required by a regulator or provided by a third party acceptable to the Company.) Users may access the System through (i) computer-to-computer links (“Computer-to-Computer Links”), (ii) a secure Web front end (the “Web Front End”), or (iii) other means of access designated by the Company from time to time, in each case supported by or on behalf of the Company for the purpose, among possible others, of effecting electronic submission of records of eligible transactions, all in the manner and subject to the security arrangements established by the Company from time to time, as set forth in the Company’s Applicable Publications (described below). The security arrangements established by the Company will include (a) means of determining whether particular records were submitted to the System through Computer-to-Computer Links established with a particular User or its Family or (b) access to the Web Front End by means of digital certificate(s) and password(s), or other secure identifiers, assigned to that User or its Family. Records submitted to the System (as described below) indicating a particular User as the submitting party (through an identifier referred to above) shall be conclusively presumed to have been duly authorized by the User whenever such records are so determined to have been submitted through Computer-to-Computer Links established with that User or its Family, or through access of the Web Front End by means of the digital certificate(s) and password(s), or other secure identifiers, assigned to that User or its Family. If a



























## Swap Data Repository Appendix to the DTCC Data Repository (U.S.) LLC Operating Procedures

### SWAP DATA REPOSITORY

#### I. INTRODUCTION

The DTCC Data Repository (U.S.) LLC data repository for swaps and security-based swaps (the “Swap Data Repository”, “SDR” or “Company”) is implemented and maintained by the Company as a “swap data repository” as defined in and for purposes of the Commodity Exchange Act, as amended (the “CEA”), and the regulations thereunder, and a “security-based swap data repository” as defined in and for purposes of the Securities Exchange Act of 1934, as amended (the “Exchange Act”). The Swap Data Repository may also provide services in similar capacities under the laws of other jurisdictions, and may also provide such services with respect to transactions that are not swaps or security-based swaps for purposes of the CEA or the Exchange Act.

Without limiting the foregoing, the SDR will, following its registration as a “swap data repository” under the CEA and/or “security-based swap data repository” under the Exchange Act, as applicable, (i) perform all of the required functions of a swap data repository under part 49 of the regulations of the Commodity Futures Trading Commission (the “CFTC”); (ii) perform all of the required functions of a security-based swap data repository under Securities and Exchange Commission (“SEC”) Rules 13n-1 through 13n-11; (iii) accept, from or on behalf of Users, transaction and life-cycle data for swaps as specified in parts 43 and 45 of the CFTC regulations, as and when required to be reported to a swap data repository thereunder; (iv) accept, from or on behalf of Users, transaction and life-cycle data for security-based swaps as specified in SEC Regulation SBSR, as and when required to be reported to a security-based swap data repository thereunder; (v) verify and maintain swap and security-based swap data as required by such regulations; (vi) publicly disseminate in real-time and perform recordkeeping of swap data as and when required under part 43 and part 49 of the CFTC regulations, either directly or through one or more third parties; (vii) publicly disseminate security-based swap data as and when required under SEC Regulation SBSR, either directly or through one or more third parties; (viii) provide access to swap and security-based swap data to appropriate regulators as described herein and (ix) generate reports with respect to transaction data maintained in the Swap Data Repository, in each case as specified in further detail in the Operating Procedures and Applicable Publications.

The Swap Data Repository will be deemed a Service for purposes of the Operating Procedures; provided that in the event of any conflict between this Appendix and any other provision of the Operating Procedures (or the appendices thereto) in connection with the operation of the Swap Data Repository, this Appendix shall govern.











Canadian Repository Appendix to the  
DTCC Data Repository (U.S.) LLC Operating Procedures

## CANADIAN SWAP DATA REPORTING SERVICE

### I. INTRODUCTION

The DTCC Data Repository (U.S.) LLC (“DDR” or “Company”) has been designated ~~under section 21.2.2 of the Securities Act (Ontario) and section 31.6 of the Securities Act (Manitoba) and~~ or recognized under sections 12 and 14 of the Derivatives Act (Quebec), and such other trade repository statutes or legislation in, as applicable, by the Canadian ~~provinces~~ Regulators, as that term is defined below, as may from time to time designate or recognize DDR, as a trade repository for records submitted by or on behalf of Users from time to time (“Records”) with respect to one or more categories or types of derivatives transactions (“Derivatives Transactions”) or the status thereof or events with respect thereto, in each case as may be specified by the Company, and as a source for generation of reports (“Reports”) relating to such transactions to Users and applicable regulatory or supervisory authorities as specified herein. The Company may also provide services in similar capacities under the laws of other jurisdictions.

Without limiting the foregoing, the Company will (i) perform all of the required functions of a trade repository under the applicable regulations (“Canadian TR Regulations”) of the ~~Ontario Securities Commission (the “OSC”), the Manitoba Securities Commission (“MSC”) and Autorité des marchés financiers (“AMF”) and such other Canadian regulators as have designated or recognized DDR as a trade repository~~ Alberta Securities Commission, Autorité des marchés financiers, British Columbia Securities Commission, Manitoba Securities Commission, Financial and Consumer Services Commission New Brunswick, Office of the Superintendent of Securities Newfoundland and Labrador, Northwest Territories Securities Office, Nova Scotia Securities Commission, Office of the Superintendent of Securities Nunavut, Ontario Securities Commission, Office of the Superintendent of Securities Prince Edward Island, Financial and Consumer Affairs Authority of Saskatchewan, and Office of the Superintendent of Securities Yukon Territories (together, the “Canadian Regulators”); (ii) accept, from or on behalf of Users, transaction and life-cycle data for swaps, as and when required to be reported to a trade repository under the Canadian TR Regulations; (iii) verify and maintain swap data as required by such regulations; (iv) publicly disseminate and perform recordkeeping of swap data as and when required under the Canadian TR Regulations, either directly or through one or more third parties; (v) provide access to swap data to appropriate regulators as described herein and (vi) generate reports with respect to transaction data maintained in the Company, in each case as specified in further detail in the Operating Procedures and Applicable Publications.

The Canadian Swap Data Reporting Service will be deemed a Service for purposes of the Operating Procedures; provided that in the event of any conflict between this Appendix and any other provision of the Operating Procedures (or the appendices thereto) in connection with the Derivatives Transactions (and related Records) included or to be included in DDR for the purposes of reporting such transactions to Canadian Regulators, this Appendix shall govern.







## **APPENDIX C: INFORMATION PRIVACY POLICY OF DTCC DATA REPOSITORY (U.S.) LLC SDR**

---

1. Information Privacy Policy of DTCC Data Repository (U.S.) LLC SDR







- **Law Enforcement, Regulatory, and Judicial Requests:** disclosures of DDR Confidential Information to law enforcement agencies or regulatory agencies that are permitted or required by law (e.g., responding to a subpoena, order or request of any court, governmental, regulatory or other relevant authority, agency or organization);
- **Third-Party Service Providers:** disclosures to affiliated and non-affiliated third parties that perform support services for DDR. Pursuant to Applicable Law, including CFTC Regulation 49.17(e), DDR clearly sets forth the use of DDR Confidential Information and the minimum confidentiality procedures that the third-party service provider must maintain as part of the service agreement or similar agreement or as part of a separate confidentiality or nondisclosure agreement; and
- **Authorized Disclosure:** disclosures with the express consent of the applicable reporting entity or person.

## Information Safeguarding

DDR has established an information security program setting forth reasonable administrative, technical and physical safeguards to: (i) ensure the security and confidentiality of DDR Confidential Information; (ii) protect against anticipated threats or hazards to the security of DDR Confidential Information; (iii) protect against unauthorized access to or use or disclosure of DDR Confidential Information, as well as unauthorized alteration and/or destruction; and (iv) protect against any misappropriation or misuse of DDR Confidential Information. DDR has also established certain measures designed to facilitate the periodic testing of their information security controls, systems and procedures.

## Changes to this Privacy Policy

DDR may change this Privacy Policy from time to time, as necessary or appropriate, based on factors which may include (i) results of testing and monitoring, (ii) changes to the business and operation of DDR or the SDR Services, and (iii) changes to regulations and laws.

## Contact Information

Please contact the Privacy Office of the DDR for further information regarding this Privacy Policy at [privacyoffice@dtcc.com](mailto:privacyoffice@dtcc.com).