Trade Repository Rulebook

ICE Trade Vault Europe

21 December 2020

Version History

Version	Date	Description of change
1.0	19 December 2017	Clarification as to how user IDs and passwords are issued.
2.0	25 May 2018	Update to Section 8 - Data Confidentiality; Sensitive Information and Security
3.0	21 December 2020	Update to Key Terms & Definitions to include references to: ICE EMIR Data File Service, Transition Period, and Withdrawal Agreement Update to Section 2.4 - System Availability and Support; Hours of Operation Update to Section 3.1.4 to include provisions relating to the transfer of data in relation to Brexit
4.0	31 July 2023	Update to reflect the deactivation of the ICE EMIR Data File Service.

Table of Contents

ICE Trade Vault Europe Trade Repository Rulebook

1. Key Terms & Definitions

- API: application programming interface.
- Applicable EMIR ITS: Regulatory implementing technical standards promulgated by the European Commission pursuant to Commission Implementing Regulations that are applicable to the ICE TR Service, including but not limited to technical standards pertaining to:

  Commission Implementing Regulation (EU) No 2017/105 of 19 October 2016 amending Implementing Regulation (EU) No 1247/2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No. 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories; and

  Commission Implementing Regulation (EU) No 1248/2012 of 19 December 2012 laying down implementing technical standards with regard to the format of applications for registration of trade repositories according to Regulation (EU) No. 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories.
- Applicable EMIR RTS: Regulatory technical standards promulgated by the European Commission pursuant to Commission Delegated Regulations that are applicable to the ICE TR Service, including but not limited to technical standards pertaining to:

  Commission Delegated Regulation (EU) No 150/2013 of 19 December 2012 supplementing Regulation (EU) No. 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories with regard to regulatory technical standards specifying the details of the application for registration as a trade repository;

  Commission Delegated Regulation (EU) No 151/2013 of 19 December 2012 supplementing Regulation (EU) No. 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories with regard to regulatory technical standards specifying the data to be published and made available by trade repositories and operational standards for aggregating, comparing and accessing the data; and

  Commission Delegated Regulation (EU) No 2017/104 of 19 October 2016 amending Delegated Regulation (EU) No 148/2013 supplementing Regulation (EU) No. 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories with regard to regulatory technical standards on the minimum details of the data to be reported to trade repositories.
- Applicable Law: Any and all applicable national, federal, supranational, state, regional, provincial, local or other governmental statute, law, ordinance, regulation (including but not limited to EMIR), rule, directive, technical standard (including, but not limited to Applicable EMIR ITS and Applicable EMIR RTS), code, guidance, order, published practice or concession, judgment or decision as amended from

time to time.

- Appointed Reporting Entity: A third party to which a Participant or Trusted Source has delegated the reporting of certain details of derivative contracts pursuant to Applicable Law.
- Article 9 Information: The information set forth in Article 9 of EMIR as supplemented by Applicable EMIR ITS and Applicable EMIR RTS.
- EMIR: The European Market Infrastructure Regulation cited as Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on derivatives, central counterparties and trade repositories.
- EMIR Q&A: The document published by ESMA titled, "Questions and Answers" on the Implementation of EMIR, as amended from time to time.
- ESMA: The European Securities and Markets Authority.
- GLEIF: The Global Legal Entity Identifier Foundation.
- ICE: Intercontinental Exchange, Inc., a publicly traded company.
- ICE eConfirm Service: The electronic platform utilised by Participants and Trusted Sources to report TR data to the ICE TR Service.
- .
- ICE Public Data Aggregation Service: An architectural component of the ICE TR Service which aggregates and publicly displays certain derivative contract data that is reported to the ICE TR Service as prescribed in Commission Delegated Regulation (EU) No 151/2013 of 19 December 2012.
- ICE TR Service: The regulated trade repository service offered by ICE Trade Vault Europe utilised for the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of derivative contracts.
- ICE Trade Vault Europe: ICE Trade Vault Europe Limited.
- Internal Policies and Procedures: The internal policies and procedures in place from time to time of ICE Trade Vault Europe, including but not limited to those relating to compliance, risk, conflicts of interest, controls, internal and external audits, ethics, and internal and external reporting, reasonably designed to prevent violations of Applicable Law by ICE Trade Vault Europe or by its managers and employees.
- Legal Entity Identifier ("LEI"): As defined in the Applicable Law, the assigned code used for unique identification of a counterparty to any derivative contract.
- Participant: An entity that has validly enrolled in the ICE TR Service with ICE Trade Vault Europe through a duly executed Participant Agreement in effect with ICE Trade Vault Europe.
- Regulator: Each entity listed in Article 81(3) of EMIR.
- Rulebook: The ICE Trade Vault Europe Trade Repository Rulebook, as amended from time to time.
- Transition Period: Under the terms of the Withdrawal Agreement, the UK has entered into a transition period, or implementation period, where EU law continues to apply in the UK in the

same way as prior to 31 January 2020.

- TR Information: As defined in the Applicable Law, any information that ICE Trade Vault Europe receives from Participants or maintains on their behalf, as part of the ICE TR Service.
- Trusted Source: A CCP or other Appointed Reporting Entity that has a duly executed Trusted Source Agreement in effect with ICE Trade Vault Europe.
- Unique Product Identifier ("UPI"): As defined in the Applicable Law, the assigned distinctive code used for categorisation of derivative contracts with respect to the underlying products referenced therein.
- Unique Trade Identifier ("UTI"): As defined in the Applicable Law, the distinctive code created and assigned to a derivative contract.
- Withdrawal Agreement: The Withdrawal Agreement concluded between the EU and UK establishes the terms of the UK's orderly withdrawal from the EU, which took effect at 11pm on 31 January 2020.

The following terms have the meanings set forth in EMIR, Applicable EMIR ITS or Applicable EMIR RTS, as amended from time to time: "concluded", "close links", "derivative contract", "Financial Counterparty", "Non-Financial Counterparty", "counterparty", "trading venue", "central counterparty" ("CCP"), "Trade Repository" ("TR"), and "OTC derivative contracts".

2. General Provisions

2.1 Governance

ICE Trade Vault Europe Limited is organised as a limited company registered in England and Wales and is a wholly owned subsidiary of ICE.

The Board of Directors shall (i) be the governing body of ICE Trade Vault Europe; (ii) designate and authorise specific appointed officers to act on behalf of the Board of Directors; (iii) fix, determine and levy all TR fees, when necessary; (iv) make and amend the rules of the TR; (v) have the power to act in emergencies; and (vi) delegate any such power to the appropriate party.

The Board of Directors of ICE Trade Vault Europe shall operate in accordance with the Internal Policies and Procedures, Applicable Law, the articles of association of ICE Trade Vault Europe, and any specific terms of reference that may govern the Board of Directors from time to time.

In addition to the Board of Directors, ICE Trade Vault Europe has senior managers in charge of various reporting lines within ICE Trade Vault Europe. Senior management from time to time includes the Executive Director and the Chief Compliance Officer ("CCO").

All staff report into one or more reporting lines headed by a senior manager. Senior managers also meet with the Board of Directors at least once annually to report and discuss matters and ensure ongoing effective monitoring and supervision of the ICE TR Service by the Board of Directors.

The level of compensation of the Board of Directors and senior managers will be set in accordance with the Internal Policies and Procedures.

2.1.1 Chief Compliance Officer

The CCO of ICE Trade Vault Europe is appointed by the Executive Director of ICE Trade Vault Europe. The Board of Directors approves the compensation of the CCO, the level of which will be set in accordance with the Internal Policies and Procedures. The CCO will also meet with the Board of Directors at least annually to report and discuss compliance matters and ensure ongoing effective monitoring and supervising of compliance issues. Removal of the CCO requires the approval of the Board of Directors

The CCO also works directly with the Board of Directors in certain instances, for example, when identifying, managing and resolving compliance issues. 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 an annual compliance report and carrying out an ongoing compliance officer review; (ii) overseeing, monitoring and reviewing ICE Trade Vault Europe's (and its employees' and managers') compliance with Applicable Law; (iii) establishing, administering, monitoring compliance with, and updating the Internal Policies and Procedures; (iv) in consultation with the Product Manager and no less than once each calendar quarter, reviewing, updating and approving any revision to the User Guides; (v) reviewing requests from relevant authorities for and granting access to TR Information in accordance with Article 81(3) EMIR and verifying and updating the access granted to such relevant authorities no less than once each calendar quarter (in consultation with ESMA to the extent necessary to resolve any ambiguity regarding such access); (vi) establishing, administering, monitoring, and updating programmes for staff and managers to receive appropriate training on the Internal Policies and Procedures and the ICE TR Service; (vii) in consultation with the Board of Directors, identifying, managing and resolving any conflicts of interest that may arise including, but not limited to: (a) conflicts between business considerations and compliance requirements; (b) conflicts between business considerations and the requirement that ICE Trade Vault Europe provide fair and open access; (c) conflicts concerning ICE Trade Vault Europe's management, employees and members of the Board of Directors or any close links of such persons; and (d) conflicts between ICE Trade Vault Europe and other entities in its corporate group; (viii) establishing and implementing procedures for the remediation of noncompliance issues; (ix) taking reasonable steps to ensure compliance with Applicable Law relating to agreements, contracts, or transactions; (x) 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; (xi) establishing and following appropriate procedures for the handling, management response, remediation, retesting, and closing of noncompliance issues, including in relation to breaches of Internal Policies and Procedures; (xii) establishing and administering a written code of ethics designed to prevent ethical violations and to promote honesty and ethical conduct; and (xiii) ensuring ICE Trade Vault Europe maintains sufficient information technology systems, staff and other resources to fulfill its duty to monitor, screen and analyze derivative contract data in a manner consistent with Applicable Law.

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

2.2 Overview of Regulatory Requirements

EMIR requires that all Article 9 Information concerning any derivative contract concluded (or any modification or termination) is reported to a TR. A TR is required to register with ESMA, comply with all Applicable EMIR ITS, Applicable EMIR RTS and other Applicable Law, meet compliance requirements by publishing and updating certain aggregate position, transaction and value data, manage data reporting obligations, and maintain policies and procedures to ensure data security and compliance with Applicable Law. A TR also interacts

directly with a range of market participants and is required to engage in the following core duties: (i) collection of data; (ii) recordkeeping; (iii) calculation, aggregation and publication of data accessible by the public (via the ICE Public Data Aggregation Service); (iv) maintaining and ensuring confidentiality, integrity and protection of data; and (v) permitting appropriate access to data by Regulators.

2.3 TR Rules; Conflicts with Applicable Law

The rules of the ICE TR Service consist of, collectively, this TR Rulebook and all other documents incorporated by reference herein.

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

2.4 System Availability and Support; Hours of Operation

ICE Trade Vault Europe reserves the right to take the services offline, only if necessary, between the hours of 11:00 PM London time and 6:00 AM London time on any weekday and from 11:00 PM London time on Friday through 3:00 AM London time on Monday, if more extensive maintenance or upgrades are necessary. ICE Trade Vault Europe will provide Participants with advanced notice of any scheduled maintenance. All data submitted during systemdown time is stored and processed once the service has resumed.

The ICE Trade Vault Europe help desk is available to receive customer calls in London from 8:00 AM London time to 6:00 PM London time, Monday through Friday, on all local business days, and in Atlanta, Georgia from 8:00 AM ET to 6:00 PM ET, on all local business days.

To reach the help desk, contact: TradeVaultSupport@theice.com or +44 (0)20 7488 5100 in London or 1.770.738.2102 in Atlanta.

2.5 Service, Commitment and Continuity

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

2.6 ICE TR Service Pricing

Any fees or charges imposed by ICE Trade Vault Europe in connection with the ICE TR 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 TR Service. ICE Trade Vault Europe shall not offer preferential pricing arrangements for the ICE TR Service to any market participant on any basis. Details of fees and charges imposed by ICE Trade Vault Europe in connection with the ICE TR Service can be found at www.icetradevault.com.

2.7 Emergency Authority

2.7.1 Authority

As part of its Internal Policies and Procedures, ICE Trade Vault Europe maintains a business continuity policy and disaster recovery plan to ensure maintenance of its functions, systems and the ICE TR Service, and to

enable as far as possible the timely recovery of operations and back up facilities if necessary in the event of a loss or disruption of critical functions relating to the ICE TR Service. However, in an emergency situation, it may not always be possible to maintain the ICE TR Service and/or functions and systems.

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

2.7.2 Circumstances Requiring Invocation of Emergency Authority

Circumstances requiring the invocation of emergency authority include: (i) any occurrence or circumstance which ICE Trade Vault Europe 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 TR Service; (iv) any occurrence or circumstance which may materially affect the performance of the ICE Trade Vault Europe 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 Europe systems or the ICE TR Service; and (vi) any other circumstance which may impact ICE Trade Vault Europe in a materially adverse manner.

2.7.3 Emergency Authority Procedures

If the Executive Director, or any individual designated by the Executive Director or the Board of Directors (or otherwise in accordance with the Internal Policies and Procedures (including, but not necessarily limited to the business continuity policy and disaster recovery plan)), determines that an Emergency has arisen, the Executive Director or such designee, as the case may be, may, consistent with Internal Policies and Procedures (including, but not necessarily limited to, the business continuity policy and disaster recovery plan), and in consultation with the CCO and the Board of Directors where possible, declare an Emergency with respect to the ICE TR Service or the systems and facilities of ICE Trade Vault Europe and take or place into immediate effect a temporary emergency action or rule. Any such action or 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, where possible, in terms of the implementation of any emergency action or rule or any decision approving or disapproving the ongoing effectiveness of such action or rule. Any such action or rule may provide for, or may authorise ICE Trade Vault Europe, the Board of Directors or any committee thereof to undertake, actions deemed necessary or appropriate by the Executive Director or any designee to respond to the Emergency, including, but not limited to, the following:

- modifying or suspending any relevant provision of the ICE TR Service rules;
- extending, limiting or changing the operating hours of the ICE TR Service; or
- temporarily limiting or denying access to the ICE TR Service, including access to any relevant ICE Trade Vault Europe system or facilities.

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 Executive Director, or any designee, as appropriate, the physical functions of the ICE TR 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, in consultation, where possible, with the CCO, including suspending the ICE TR Service.

In the event the Emergency that gave rise to such action or rule has, in the view of the Executive Director, or any designee, as appropriate (in consultation with the CCO and the Board of Directors where possible and consistent with the Internal Policies and Procedures), sufficiently abated to permit the ICE TR Service and/or its systems and facilities to operate again in an orderly manner, such action or rule may be ceased or removed upon determination by the Executive Director, or designee, as appropriate; provided that any cessation or removal pursuant to this paragraph will be subject to review, and may be subject to modification or reversal by the Board of Directors, in consultation, where possible, with the CCO.

In accordance with Applicable Law, ICE Trade Vault Europe will notify ESMA as soon as practicable of any action or rule taken or implemented, or proposed to be taken or implemented, pursuant to this Rule 2.7.3. The decision-making process with respect to, and the reasons for, any such action or rule will be recorded in writing. ICE Trade Vault Europe will also notify Participants and Trusted Sources via an appropriate email address as provided by Participant or Trusted Sources from time to time, or such other means of communication as is possible, as soon as practicable of any action taken or implemented, or proposed to be taken or implemented, pursuant to this section.

2.8 Violations

2.8.1 Jurisdiction

ICE Trade Vault Europe retains the authority to conduct investigations and take action in respect of any violations of this Rulebook ("Violations") committed by Participants and Trusted Sources as provided in this Section 2.8. ICE Trade Vault Europe retains the authority to notify ESMA of any material breach of any policy or procedure including, but not limited to this Rulebook or the Internal Policies and Procedures, which may result in a breach of the conditions of ICE Trade Vault Europe's registration as a TR pursuant to Applicable Law.

2.8.2 CCO Powers and Duties

The CCO is responsible for enforcing the rules set forth in this Section 2.8 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 2.8.2. 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 Europe employees, including officers, and such other individuals (who possess the requisite independence) as ICE Trade Vault Europe may hire on a contract basis.

The CCO shall have the power to initiate an investigation of any suspected Violation and conduct investigations of possible Violations, prepare written reports with respect to such investigations, furnish such reports to the Board of Directors and undertake action in response to such Violations in accordance with this Section 2.8.

If, in any case, the CCO (or another ICE Trade Vault Europe employee designated for this purpose by ICE Trade Vault Europe) 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 further action by ICE Trade Vault Europe; or

- negotiate a written settlement agreement with the Participant or Trusted Source, whereby the Participant or Trusted Source may agree to a suspension or revocation of TR privileges or a termination of Participant or Trusted Source status or other remedial action to address the Violation.

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 2.8.5.

2.8.3 Board of Directors' Powers

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 2.8.4 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 remedial action other than that recommended by the CCO); and/or (iii) take remedial actions that may include, but are not limited to, a warning or a suspension or revocation of TR privileges or a termination of Participant or Trusted Source status.

2.8.4 Notice of Action; Right to Hearing

Pursuant to instructions from the Board of Directors, the CCO shall serve a notice of action (a "Notice") on the Participant or Trusted Source responsible for a Violation (the "Respondent"). Such Notice shall state: (i) the acts, practices or conduct of the Respondent that are considered to be a Violation; (ii) how such acts, practices or conduct constitute a Violation; (iii) that the Respondent is entitled, upon written request filed with ICE Trade Vault Europe within twenty days of service of the Notice, to a formal hearing on the alleged Violation; (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 allegation 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.

2.8.5 Hearing on Alleged Violation; Failure to Request Hearing Deemed Acceptance of Alleged Violation.

In the event (i) the Respondent fails to file an answer or admits to or fails to deny any allegation of a Violation contained in the Notice or (ii) after a hearing conducted pursuant to Rule 2.8.4 the Board of Directors determines that any alleged Violation did in fact occur with respect to a Respondent, the Board of Directors shall find the Respondent to have committed each such Violation and may revoke the Respondent’s TR

privileges or terminate the Respondent's Participant or Trusted Source status. The CCO shall promptly notify the Respondent of any such action and of the Respondent's right to a hearing on the action. Failure to request a hearing on the action in a timely manner, absent good cause shown, shall be deemed to be acceptance of the action.

2.8.6 Liability for Expenses

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 Europe an amount equal to any and all out-of-pocket expenses incurred by ICE Trade Vault Europe in connection with the investigation and remedying of such Violations.

2.8.7 Effective Date of Remedial Actions

If a Respondent enters into a settlement agreement, the terms of which have been approved by the Board of Directors, any remedial actions 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 by the Board of Directors shall be the final decision of ICE Trade Vault Europe 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 action to become effective prior to the end of the fifteen day period.

2.9 Conflicts of Interest

Conflicts of interest, or potential conflicts of interest, can arise in many ways including but not limited to (i) conflicts between business considerations and compliance requirements or Applicable Law; (ii) conflicts between management, employees and/or members of the Board of Directors or any close links of such persons or between such persons and ICE Trade Vault Europe or any entity in its corporate group; (d) conflicts between ICE Trade Vault Europe and other entities in its corporate group.

As part of its Internal Policies and Procedures, ICE Trade Vault Europe has a conflicts of interest policy concerning the identification, management and disclosure of conflicts of interest, or potential conflicts of interest, as the case may be. ICE Trade Vault Europe also maintains an ongoing inventory of existing conflicts of interest and manages these on an ongoing basis. In addition to the Internal Policies and Procedures, this Section 2.9 shall apply to the Board of Directors, or any committee thereof, and any member of senior management of ICE Trade Vault Europe.

2.9.1 Definitions

For purposes of this Rule 2.9 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.

2.9.2 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 Europe 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.

2.9.3 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 Rule 2.9.2 with a Named Party in Interest.

2.9.4 Procedure and Determination

The CCO shall determine whether any member of the deliberating body is subject to a prohibition under Rule 2.9.2. Such determination shall be based upon a review of the following information: (i) information provided by the member pursuant to Rule 2.9.3, and (ii) any other source of information that is maintained by or reasonably available to ICE Trade Vault Europe.

3. Access, Connectivity and Safe Guarding of Data

3.1 Fair and Equal Access Policy

Consistent with Applicable Law, ICE Trade Vault Europe provides access to the ICE TR Service on a fair, open and equal basis to persons subject to an obligation to report derivative contract data to a TR pursuant to EMIR.

3.1.1 Participant and Trusted Source Access

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

When enrolling with ICE Trade Vault Europe, Participants and Trusted Sources must designate a master user ("Administrator"). The Administrator will create, permission and maintain all user IDs for their firm with regard 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.

Participants and Trusted Sources shall only have access to their own data and data that ICE Trade Vault Europe is required by Applicable Law to make publicly available and has made publicly available ("Public Data").

Participants and Trusted Sources shall be entitled to access and correct in a timely manner any information on a contract to which they are a party.

3.1.2 Public Access

Public users (including those who are neither Participants nor Trusted Sources) will have the ability to access the ICE Trade Vault Europe website to view Public Data in accordance with Applicable Law at www.icetradevault.com.

3.1.3 Regulator Access

Any Regulator requiring or requesting access to the ICE TR Service should contact the CCO (via email: TradeVaultEUChiefComplianceOfficer@theice.com) to request access and provide the legal basis upon which such Regulator is relying to gain access to the ICE TR Service.

Following receipt of such request for data access from a Regulator and confirmation by ICE Trade Vault Europe that the request is within scope of the relevant Regulator's jurisdiction and rights under Applicable Law, and due execution or validation of any necessary documentation, ICE Trade Vault Europe shall provide direct and immediate access to the requested data consistent with Applicable Law. Each Regulator's designated master user ("Regulator Administrator") will manage the Regulator's user access to the ICE TR Service. Such access may include, where applicable, proper tools for the monitoring, screening and analyzing of derivative contract data, including, but not limited to, web-based services and services that provide automated transfer of data to Regulators, and the ability to view individual Participants' data and aggregated data sets.

ICE Trade Vault Europe shall record information regarding the scope of the data accessed by a Regulator and a reference to the legal provision granting access to such data under Applicable Law.

3.1.4 Transfer of Data in Relation to Brexit

Effective after the end of the Transition Period, ICE Trade Vault Europe will no longer be registered with ESMA as a trade repository under Article 55 of EMIR, because entities established outside the EU are not eligible for such registration.

Pursuant to Applicable Laws and ESMA guidelines, ICE Trade Vault Europe has been requested and directed by ESMA to transfer a copy of all data relating to all historic and present transactions reported prior to the end of the Transition Period by all current and former users (whether EU or UK based), to another trade repository incorporated in the EU or to ESMA on or around the end of the Transition Period.

As a result, and further to Rule 7.1 and its obligations under Applicable Laws, ICE Trade Vault Europe will transfer all data as so required, either to another trade repository or ESMA on or around the end of the Transition Period. The transfers described in this Rule 3.1.4 will be deemed to be within the scope of the licence granted to ICE Trade Vault Europe under section 3(a) of the Participant Agreement. They will also be deemed to be released by section 7(b)(iv) of the Participant Agreement from the restriction against disclosure in section 7(a) of the Participant Agreement.

3.1.5 Third-Party Service Providers; Transparency About Access

Each third-party service provider that provides a service of a particular nature (a "Relevant Service") in connection with ICE Trade Vault Europe will be subject to the same procedures governing access to information maintained by ICE Trade Vault Europe as each other provider of the same Relevant Service. However, no third-party service provider will have access to any information maintained by ICE Trade Vault Europe (other than Public Data) unless and until the relevant counterparties have consented to such third-party service provider accessing the

relevant data. The CCO will review and confirm that sufficient evidence of the relevant consents has been obtained.

As a condition to its access to information maintained by ICE Trade Vault Europe, each third-party service provider agrees that it will not, with respect to any such information, act or omit to act in any manner that would cause ICE Trade Vault Europe to be in breach of the confidentiality, integrity and data protection requirements that apply to trade repositories under Applicable Law. Each third-party service provider that provides a Relevant Service will, with respect to information maintained by ICE Trade Vault Europe, comply with the confidentiality terms prescribed by ICE Trade Vault Europe with respect to providers of that Relevant Service.

3.2 Revocation of Access

Revocation or limitation of access shall only be permitted to the extent necessary to control risk to data stored by ICE Trade Vault Europe. Prior to implementing any limitation or revocation of a Participant's or Trusted Source's access to the ICE TR Service or data maintained by ICE Trade Vault Europe, the CCO shall review the basis for the limitation or revocation for compliance with Applicable Law, the Internal Policies and Procedures and the rules of the ICE TR 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 would be discriminated against unfairly if the proposed revocation or limitation were implemented, the CCO shall take such actions as are necessary to ensure that Participant's or Trusted Source's access to such service or data remains unaffected.

3.3 Reinstatement of Access; Revocation or Modification of Other Actions; Termination of Status

A Participant or Trusted Source that has had access revoked or limited 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 Europe 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 whose access has been so limited or revoked does not appeal within twenty (20) days after the commencement of such limitation or revocation, or if such Participant or Trusted Source shall have so applied and the Board of Directors shall have rejected the application, any decision to limit or revoke such access shall be upheld. The Board of Directors may terminate such Participant's or Trusted Source's user 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 the Internal Policies and Procedures and other 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 TR Service through a web-based front-end that requires user systems to (a) satisfy ICE Trade Vault Europe 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. Trusted Sources may connect to the ICE TR Service through direct electronic access via an API.

4. Acceptance of Data and Reporting Procedures

4.1 Asset Classes

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

4.2 Trade Data and Data Processing

4.2.1 General

Participants and Trusted Sources reporting derivative contract data to the ICE TR Service will be required to comply with Applicable Law.

4.2.2 Required Submissions

Applicable Law requires that Participants and Trusted Sources report to a trade repository prescribed details of any derivative contract concluded and any modification or termination of a derivative contract.

The frequency of reports and the details to be reported are set out in Applicable Law, and will differ depending on whether a Participant is a Financial Counterparty, a Non-Financial Counterparty referred to in Article 10 of EMIR, or another Non-Financial Counterparty, and whether the derivatives contract is cleared or not cleared and the type of derivative contract and underlying product.

ICE Trade Vault Europe recognises that Participants may need to update data submissions or correct data submissions that contain errors. ICE Trade Vault Europe transaction data submissions may be corrected by Participants in a timely manner. Continuation data (as described in Rule 4.2.4) will require reporting to ICE Trade Vault Europe within the time periods set out under Applicable Law. However, in all cases such corrections and continuation data submissions are required to conform to the applicable LEI, UPI and UTI requirements and any other requirements under Applicable Law. Disciplinary actions may be taken for ongoing and excessive corrections or where such corrections or continuation data submissions are not made in good faith by the relevant Participant.

4.2.3 Confirmation Data

Participants or Trusted Sources must report the details of the Confirmation for an OTC derivative contract ("Confirmation Data") as part of the required submissions described in Rule 4.2.2, as prescribed by Applicable Law. "Confirmation" means the documentation of the legally binding agreement of the counterparties to all the terms of a derivative contract. Participants may agree to use the ICE eConfirm Service for OTC derivative transaction Confirmation, or they may use other services for such Confirmations.

4.2.4 Continuation Data

Participants and Trusted Sources must report all continuation data for derivative contracts previously reported to the ICE TR Service as prescribed by Applicable Law. Continuation data is the set of data generated in connection with lifecycle events that occur prior to, and including, a derivative contract's termination date as required by Applicable Law. The term "lifecycle events" includes, but is not limited to, trade cancellations (busted trades), modifications, novations and early terminations.

4.2.5 LEI Changes Due to Mergers, Acquisitions and Name Changes

In accordance with TR Question 40 of the EMIR Q&A, Participants and Trusted Sources must provide ICE Trade Vault Europe with the following documentation no later than 30 calendar days prior to the effective date of any merger, acquisition and/or name change affecting the Participant or Trusted Source: (i) a valid copy of any merger, acquisition and/or name change documentation from the relevant public agency. The aforementioned documentation should describe the relevant names of the affected entities and the date on which such merger, acquisition and/or name change is scheduled to take effect; and (ii) a copy of the correspondence from the Participant or Trusted Source to the relevant local operating unit requesting an update to the Participant's or Trusted Source's legal entity identifier.

If a Participant or Trusted source fails to provide the aforementioned documentation before 30 calendar days prior to the effective date of any merger, acquisition and/or name change, ICE Trade Vault Europe may reject the Participant's or Trusted Source's trades until such time the GLEIF website (www.gleif.org) is updated with the Participant's or Trusted Source's new LEI. A Participant's or Trusted Source's old LEI will be rejected after the GLEIF website is updated.

4.3 Data Translation and Default Data

Proprietary trade data values submitted by Participants and Trusted Sources must be converted to ICE TR Service standard data value(s) in order to process trade records in a standardised format. Participants and Trusted Sources may utilise the web-based front-end to map proprietary data values to a standard set of ICE TR Service data values. Once defined, a Participant's, Appointed Reporting Entity's or Trusted Source's data map is applied to each trade record subsequently received and processed by the ICE TR Service.

Participants and Trusted Sources may also utilise the default data value facility provided with the ICE TR Service for certain product default fields. This facility allows Participants and Trusted Sources to utilise, within the ICE TR Service, a default standard data value by product. Prior to processing the trade, all required fields of a trade record must contain a standard data value for that product type. In the event that the Participant or Trusted Source submits no data value for a required field for a trade record, the ICE TR Service uses the agreed default data value for that field.

4.4 Verification of Single-Sided Trade Data

When a trade is not electronically matched, ICE Trade Vault Europe must rely on the reporting entity to confirm the accuracy of the trade.

4.5 No Invalidation or Modification of Valid Derivative Contract Data

In accordance with Applicable Law, ICE Trade Vault Europe has Internal Policies and Procedures in place to ensure that the production environment in which the recording process of the ICE TR Service operates does not invalidate or modify the terms of a valid derivative contract. These controls are regularly audited and prevent any unauthorised, unsolicited changes to derivative contract data submitted to ICE Trade Vault Europe through system-wide protections related to the processing of data associated with the ICE TR Service and ICE Trade Vault Europe platform.

4.6 Correction of Errors in Trade Records

Participants and Trusted Sources are responsible for the timely resolution of transaction record errors. ICE Trade Vault Europe provides Participants and Appointed Reporting Entities electronic methods to correct transaction record errors and to extract data for trade data reconciliation.

4.7 Duty to Collect and Maintain Derivative Contract Data

Consistent with the requirements of Applicable Law, ICE Trade Vault Europe has the capacity to collect and maintain all derivative contract data recorded as part of the ICE TR Service in accordance with Applicable Law. In this regard the ICE TR Service performs both (i) standard derivative contract data collection and maintenance and (ii) specific tasks based on ad hoc requests of Regulators in a manner consistent with Applicable Law.

5. Public Reporting

5.1 Public Data Aggregation

ICE Trade Vault Europe provides publication of certain aggregate derivative contract data through the ICE Public Data Aggregation Service. The architecture and functioning of the ICE Public Data Aggregation Service is based on the requirements of Applicable Law. The ICE Public Data Aggregation Service displays aggregate data for the following categories:

- aggregate open positions per derivatives class;
- aggregate transaction volumes per derivatives class;
- aggregate values per derivatives class;

The data shall be published on the www.icetradevault.com website and updated weekly.

6. Unique Identifiers

6.1 Unique Trade Identifiers (UTIs)

Applicable Law states that counterparties to a derivative contract are responsible for generating UTIs for that transaction.

The Participant, Appointed Reporting Entity or Trusted Source reporting derivative contract data to the ICE TR Service must provide the relevant UTIs with their transaction data submissions.

6.2 Legal Entity Identifiers (LEIs)

ICE Trade Vault Europe has the ability to map entities to their 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 Law requires UPIs to be created and processed in a centralised registry. ICE Trade Vault Europe shall, where necessary, issue UPIs (at no cost to Participants), maintain reference data representation of each product, including schema definitions, and disseminate the representation to

Participants. If the industry creates and adopts a UPI taxonomy and registry, or to the extent there is an applicable existing UPI, 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 Europe in order to receive a new UPI code and product schema.

7. Data Retention; Business Continuity

7.1 Data Retention, Access and Recordkeeping

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

With the exception of cleared futures trades reported by any entity of the ICE Group,[1] Participants' individual trade data records remain available to Participants and Trusted Sources at no charge for online access through the ICE TR 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 TR Service data will be available to Regulators at no cost via real-time electronic access. After the initial five-year period, Participants' trade data will be stored off-line and remain available to Participants, upon a three-day advance request to ICE Trade Vault Europe, at no cost until ten years following the termination of the relevant derivative contract. Participant will retain unimpaired access to its online and archived trade data even in the event of Participant's discontinued use of the ICE TR Service.

Regulators shall be granted access to relevant data by ICE Trade Vault Europe at no cost in accordance with Rule 3.1.3. In addition ICE Trade Vault Europe shall co-operate with Regulators in accordance with Applicable Law, including, where required by and in accordance with Applicable Law, taking such action as may be necessary to enable such Regulator to carry out investigations.

Nothing in this Rule 7.1 will require a Participant to pay fees associated with ICE Trade Vault Europe's standard regulatory reporting and access obligations. However, if a Participant or its Regulator requests or requires archived trade data from ICE Trade Vault Europe to be delivered other than via the web-based front-end or the API or in a non-standard format, ICE Trade Vault Europe reserves the right to require Participant to reimburse ICE Trade Vault Europe for its reasonable expenses in producing data in response to such request or requirement as such expenses are incurred. Similarly ICE Trade Vault Europe 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 Europe, whether such production is required at the instance of such Participant or at the instance of another party in relation to a Participant's data.

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

[1] ICE Trade Vault Europe archives all cleared and canceled futures trades reported by ICE exchanges and clearinghouses that are older than 45 days. A Participant or Trusted Source may request to retrieve these archived trades as needed by contacting TradeVaultSupport@theice.com.

other hand, in such manner and for such periods of time as ICE Trade Vault Europe may deem necessary and appropriate to comply with Applicable Law.

Further, in accordance with Applicable Law, ICE Trade Vault Europe will record and maintain (i) a copy of the Internal Policies and Procedures; (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, Applicable Law 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 Europe '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

As part of its Internal Policies and Procedures, ICE Trade Vault Europe maintains a business continuity policy and disaster recovery plan to ensure maintenance of its functions, systems and the ICE TR Service, and to enable as far as possible the timely recovery of operations and back up facilities if necessary in the event of a loss or disruption of critical functions relating to the ICE TR Service, including planned and unplanned interruptions, unavailability of staff, inaccessibility of facilities, and disruption or disastrous loss to one or more of ICE Trade Vault Europe'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 ESMA will be notified as soon as it is reasonably practicable of ICE Trade Vault Europe's invocation of its emergency authority, any material business disruption, or any threat that actually or potentially jeopardises automated system operation, reliability, security or capacity in a material way.

7.3 Outsourcing ICE TR Service Functions

ICE Trade Vault Europe may, from time to time, outsource to another entity in its group, or to a third party, one or more of its functions that enable it to carry out the ICE TR Service. Any such outsourcing will be permitted only in accordance with Applicable Law and the Internal Policies and Procedures.

8. Data Confidentiality; Sensitive Information and Security

ICE Trade Vault Europe is committed to protecting and safeguarding the personal data of Participants. The terms on which ICE Trade Vault Europe processes personal data in compliance with applicable data protection laws are available in Annex B of the Participant Agreement. The ICE Member and User Privacy Notice can be found at: https://www.theice.com/data-protection.

ICE Trade Vault Europe recognises its responsibility to ensure data confidentiality and dedicates significant resources to information security to prevent the misappropriation or misuse of Article 9 Information and any other TR Information maintained in the ICE Trade Vault Europe systems that is not subject to publication by the ICE Public Data Aggregation Service pursuant to Applicable Law. ICE Trade Vault Europe does not, as a condition of accepting derivative contract data from Participants, require the waiver of any privacy rights by such Participants.

ICE Trade Vault Europe 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 Europe application servers are housed in a demilitarised zone behind external firewalls. A second set of internal firewalls further isolate ICE Trade Vault Europe 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 Article 9 Information and any other TR Information maintained in the ICE Trade Vault Europe systems that is not subject to publication by the ICE Public Data Aggregation Service. ICE Trade Vault Europe annually completes an internal audit for adherence to the data security policies. The audit tests the following applicable controls, among others, to ICE Trade Vault Europe systems: (i) logical access controls; (ii) logical access to databases; (iii) physical and environmental controls; (iv) back-up procedures; and (v) change management.

In accordance with the Internal Policies and Procedures, ICE Trade Vault Europe has procedures in place to prevent natural persons who have a close link with ICE Trade Vault Europe, or legal persons who are in the same corporate group as ICE Trade Vault Europe, using confidential information recorded by ICE Trade Vault Europe, including Article 9 Information and any other TR Information maintained in the ICE Trade Vault Europe systems that is not subject to publication by the ICE Public Data Aggregation Service, for commercial purposes. ICE Trade Vault Europe itself will also not use such information for commercial purposes.