NOTICE TO MEMBERS
Nº 076-23

June 12, 2023

REQUEST FOR COMMENTS

AMENDMENTS TO THE RULES OF THE CANADIAN DERIVATIVES CLEARING CORPORATION ON CYBERSECURITY

On February 2, 2023, the Board of Directors of Canadian Derivatives Clearing Corporation ("CDCC") approved certain amendments to CDCC's Rules in order to introduce cybersecurity requirements and to allow the Corporation to monitor Clearing Member's compliance with the requirements.

Please find enclosed an analysis document as well as the proposed amendments.

Process for Changes to the Rules

CDCC is recognized as a clearing house under section 12 of the *Derivatives Act* (Québec) by the Autorité des marchés financiers ("AMF") and as a recognized clearing agency under section 21.2 of the *Securities Act* (Ontario) by the Ontario Securities Commission ("OSC").

The Board of Directors of CDCC has the power to approve the adoption or amendment of the Rules of CDCC. Amendments are submitted to the AMF in accordance with the self-certification process and to the OSC in accordance with the process provided in the Recognition Order.

Comments on the proposed amendments must be submitted before July 13, 2023. Please submit your comments to:

Sophie Brault
Legal Counsel
Canadian Derivatives Clearing Corporation
1800-1190 av. des Canadiens-de-Montréal, P.O. Box 37
Montreal, Quebec H3B 0G7
Email: legal@tmx.com

A copy of these comments shall also be forwarded to the AMF and to the OSC to:

Me Philippe Lebel
Corporate Secretary and
Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640 Laurier boulevard, suite 400
Québec (Québec) G1V 5C1
Fax : (514) 864-8381
E-mail:consultation-en-cours@lautorite.qc.ca

Manager, Market Regulation
Market Regulation Branch
Ontario Securities Commission
Suite 2200,
20 Queen Street West
Toronto, Ontario, M5H 3S8
Fax: 416-595-8940
Email: marketregulation@osc.gov.on.ca

For any question or clarification, Clearing Members may contact Sophie Brault, Legal Counsel, at sophie.brault@tmx.com.

George Kormas
President

AMENDMENTS TO THE RULES OF THE CANADIAN DERIVATIVES CLEARING CORPORATION ON CYBERSECURITY

I. DESCRIPTION

In October 2021, the Bank of Canada ("BoC"), published updated regulatory requirements under the title: *Expectations for Cyber Resilience for Financial Markets Infrastructures* (the "ECR Document")[1].

Under section 3.3.1, the ECR Document specifies:

3.3.1 Risks from interconnections
Because of its systemic importance and unique position in the financial system, the FMI should implement protective measures to mitigate risks arising from the entities within its ecosystem. The appropriate controls for each entity will depend on the results of the risk assessment from the identification phase, incorporating the risk that arises from the connected entity and the nature of the FMI's relationship with the entity.

The BoC established its expectation for the Canadian Derivatives Clearing Corporation ("CDCC") to have enhanced cybersecurity related oversight with respect to external entities in its ecosystem (interconnectedness).

Since information and cyber security requirements are not explicitly mentioned in the existing Rules, CDCC wishes to propose amendments to the CDCC Rules in order to include cybersecurity requirements and monitoring with regard to the security controls expected to be put in place by Clearing Members. Additionally, CDCC proposes to modify its Rules to allow for penalties, other than non-conforming status (which may lead to suspension), related to these new cyber security requirements.

Unless otherwise defined herein, any defined term used in this analysis will have the meaning described in the Rules, Operations Manual, Risk Manual and Default Manual (the "Rules").

[1] https://www.bankofcanada.ca/wp-content/uploads/2021/10/expectations-cyber-resilience-financial-market-infrastructures.pdf

II. PROPOSED AMENDMENTS

CDCC hereby proposes to amend its Section 1A02 (Standard of Membership) under Rule A-1A and to add two new sections under Rule A-2 (sections A-225 and A-226) to introduce the notion of cybersecurity. The purpose of these amendments is to establish cybersecurity requirements and to allow the Corporation to monitor Clearing Member's compliance with the requirements.

CDCC's Operations, Risk, and Default Manuals are not impacted by any of the proposed changes.

III. ANALYSIS

a. Background

Within the ecosystem of the Canadian Derivatives Clearing Corporation ("CDCC") there are 2 main groups of external entities. These include vendor/service providers and Clearing Members. Vendors/service providers are comprehensively addressed under a variety of TMX and CDCC level internal policies and are not part of this review. However, CDCC did not have a similar process in place for Clearing Members. CDCC undertook a review of the cyber resilience risks its Clearing Members may create and has worked to put in place an appropriate mechanism to monitor the Clearing Members, and their cyber security controls as addressed in the ECR Document.

TMX Information Security Office ("ISO") conducted a full review of the manner in which Clearing Members connect to CDCC. This Threat Risk Assessment ("TRA") focused the TRA methodology on the effectiveness of safeguards which support the CDCC Clearing Member connections. The scope of the assessment included the assets that are used by CDCC Clearing Members to connect to CDCC and access data and reports relevant to their business. The nature of Clearing Member connectivity to CDCC limits the risk of a Clearing Member introducing cyber risk to CDCC. Based on this 'low' risk evaluation, ISO developed a set of required security controls based on both the ECR Document and the practice of similar Financial Market Infrastructures ("FMIs") in other jurisdictions[2].

Clearing Members will, starting in 2023 be required to attest annually that they have these required controls in place.

b. Objectives

The proposed changes to the Rules are expected to have three benefits: a) demonstrate CDCC compliance with the ECR regulatory expectations; b) give CDCC the authority to request that Clearing Members implement specified security controls and c) reduce the potential risks to CDCC due to inadequate cyber/technology security controls introduced to its operations by a Clearing Member(s).

[2] April 2012 report Principles for financial market infrastructures (the PFMI Principles) published by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions of the Principles for Financial Market Infrastructures - https://www.bis.org/cpmi/publ/d101a.pdf

c. Comparative Analysis

CDCC conducted a comparative analysis of publicly available information on cybersecurity best practices by similar FMIs. The objective of the comparative analysis was to determine the best approach to updating CDCC Rules to include security risk management requirements as mandated by the ECR Document.

The organizations surveyed include: Depository Trust & Clearing Corporation ("DTCC"), National Securities Clearing Corporation ("NSCC"), Options Clearing Corporation ("OCC"), CME CLearing ("CME") and Eurex Clearing ("Eurex").

Comparable clearinghouses do not share publicly details about the security controls that they require from their clearing members. However, the comparative analysis indicates that a commonly accepted practice is to request that the clearing members implement a strong security program and that the program effectiveness be attested to by an executive of the clearing member, such as a Chief Information Security Officer, Chief Information Officer or a Chief Technology Officer.

The members' security program must be regularly audited by an independent party. DTCC and NSCC include in their cybersecurity confirmation the requirement that the clearing members implement a security program based on one of the leading global or US-based security standards, such as ISO27001 or NIST. The security program must be continuously maintained and audited on a regular basis. Each member is required to complete the cybersecurity confirmation at least every two years, and they have 180 days to respond to any notices of non-conformance.

OCC uses a cybersecurity confirmation form and process similar to DTCC. They require that each clearing member complete and submit a form that confirms the existence of an information system cybersecurity program approved by senior management or the member's board of directors.

CME did not publish specific security requirements for their members. Virtually all the rules published on their website deal with business, legal requirements and enforcement of the rules, but no specific security related rules.

Eurex did not publish specific security requirements for their members. Eurex expects that members will have sufficient skilled staff including contacts to resolve emergency issues, but potential cyber security incidents are not mentioned. Members are 'obliged' to upgrade any technical standards as required by Eurex. These may include security requirements but the specific requirements (if available) are not publicly disclosed.

Conclusions

- The mechanism of an attestation (as opposed to detailed IT audits or technical onsite assessments) is the approach taken by the surveyed FMIs
- None of the surveyed FMIs has published an explicit list of cybersecurity control requirements. Reference is made to high level global security standards.
- In general, the timeframe allowed to correct any non-compliance issues is 180 days.

- Financial penalties for non-compliance are not specified.

d. Analysis of Impacts

i. Impacts on Market

The proposed amendments will not have any impact on the Market.

ii. Impacts on Technology

We do not anticipate any change in Technology as a result of the proposed Rule changes.
There may be a small human resources impact. Since the attestation process is new, and has to be managed in relation to all the Clearing Members, we anticipate that there will be a requirement to increase the resources in the client relationship management and information security functions.

iii. Impacts on trading functions

The proposed amendments will have no impact on the Bourse de Montréal trading systems or rules.

iv. Public Interest

CDCC is of the view that the proposed amendments are not contrary to the public interest. The proposed Rule changes will serve the public interest by reducing the risk that the trading and clearing functions could be impacted by a cyber security incident. The supplemental cyber security oversight is in the public interest as it adds additional oversight of potential risks to the FMI that may be introduced by external parties. The approach is consistent with the requests from the public and Clearing Members for clear rules that are consistent with the best practices of other clearing houses and are PFMI compliant.

IV. PROCESS

The proposed amendments, including this analysis, must be approved by CDCC's board of directors and submitted to the Autorité des marchés financiers, in accordance with the regulatory self-certification process, and to the Ontario Securities Commission in accordance with the rules stated in Appendix "A" of Schedule "C" of CDCC Recognition Order dated April 8, 2014 (as amended from time to time). The proposed amendments and analysis will also be submitted to the Bank of Canada in accordance with the Oversight Agreement. Subject to public comments the proposed amendments are expected to take effect no later than the second quarter of 2023.

V. ATTACHED DOCUMENTS

- Appendix 1: Amended Rules

APPENDIX 1: PROPOSED AMENDMENTS TO THE RULES

BLACKLINE VERSION

CANADIAN DERIVATIVES CLEARING CORPORATION

RULES, 202X

[…]

RULE A-1A – MEMBERSHIP IN THE CORPORATION

[…]

Section -1A02 – Standards of Membership

Every applicant to become a Clearing Member must meet such standards as may be adopted from time to time by the Board, including the following:

(a) the applicant must meet the minimum financial resilience requirements then in effect, in accordance with Section A-301 or, in the case of an applicant to become a Limited Clearing Member, the minimum financial resilience requirements for admission as a Limited Clearing Member then in effect, in accordance with Section A-1B04;

(b) the applicant must be engaged, or propose to engage, in the clearance of Options or Futures which are the subject of Exchange Transactions or in the clearance of Fixed Income Transactions or other OTCI transactions through the facilities of the Corporation;

(c) the applicant shall demonstrate to the Corporation that it maintains adequate operations facilities and staff and has sufficient and competent personnel for the expeditious and orderly transactions of business with the Corporation and other Clearing Members, and to meet the requirements of these Rules;

(d) unless the applicable Entity is applying to become a Limited Clearing Member, the applicant has deposited with the Corporation its initial deposit with the Clearing Fund in the amount and at the time required by the Rules and has signed and delivered to the Corporation an agreement in such form as the Board shall require; and

(e) unless the applicable Entity is applying to become a Limited Clearing Member, the applicant has provided the Corporation with its initial Supplemental Liquidity Contributions to the Supplemental Liquidity Fund in the amount and at the time required by the Rules and the Risk Manual;

(f) the applicant must meet the cybersecurity requirements then in effect in accordance with Section A-225.

[…]

RULE A-2 – MISCELLANEOUS REQUIREMENTS

[…]

Section A-225 - Cybersecurity Requirements

A Clearing Member must maintain a comprehensive cybersecurity program and framework that considers potential cyber threats that may impact their organization and protect the confidentiality, integrity, and availability requirements of their systems and information.

A Clearing Member must (a) update its cybersecurity program and framework risk processes periodically based on a risk assessment or changes to technology, business activities, the threat environment, and/or regulatory environment and; (b) use industry best practices and major global security standards to protect the interface and/or connectivity between its systems and those of CDCC, in order to prevent the interruption or contamination of CDCC's systems in the event of a security incident at the Clearing Member.

In a manner and at a frequency that will be determined in its sole discretion, the Corporation may review the Clearing Member's cybersecurity program and framework and make any recommendations deemed necessary or desirable. The Clearing Member shall comply with any such recommendation within the timeframe prescribed by the Corporation.

Each Clearing Member shall indemnify and hold harmless CDCC, its affiliates and subsidiaries, and their respective partners, directors, trustees, officers, employees and agents, from and against any loss, damage, cost, expense, liability or claim (including the cost of legal counsel to advise on or defend against such claims) suffered or incurred by or made against it, them or any of them arising from a breach by a Clearing Member of the cybersecurity requirements.

In the event that the Corporation must correct or modify its systems, in any manner, due to a cybersecurity breach of a Clearing Member or a third party having access to the Clearing Member's systems, the Corporation shall be entitled to recover all costs and expenses incurred to make that correction or modification directly from such Clearing Member.

The failure to comply with such rule or procedures shall also subject such Clearing Member to disciplinary action pursuant to the Rules.

Section A-226 – Cybersecurity Remedies

The Corporation may in lieu of other measures contained in these Rules, impose the following remedies if it determines, that a Clearing Member is in breach of the cybersecurity requirements:

1. A fine not exceeding $50,000;
2. Require a Clearing Member to appoint, at its own expense, an auditor acceptable to the Corporation, to prepare a report on the Clearing Member's cybersecurity status and the corrective actions to be taken to meet the Corporation's cybersecurity requirements. The auditor's report shall be shared with the Corporation and Clearing Member.

If a Clearing Member continues to be in breach of any cybersecurity requirements or fails to take corrective actions at the Corporation's satisfaction, the Corporation may take any other measure contained in Section A-226 or such other action as provided in the Rules.

APPENDIX 1: PROPOSED AMENDMENTS TO THE RULES

CLEAN VERSION

CANADIAN DERIVATIVES CLEARING CORPORATION

RULES, 202X

[…]

RULE A-1A – MEMBERSHIP IN THE CORPORATION

[…]

Section -1A02 – Standards of Membership

Every applicant to become a Clearing Member must meet such standards as may be adopted from time to time by the Board, including the following:

(a) the applicant must meet the minimum financial resilience requirements then in effect, in accordance with Section A-301 or, in the case of an applicant to become a Limited Clearing Member, the minimum financial resilience requirements for admission as a Limited Clearing Member then in effect, in accordance with Section A-1B04;

(b) the applicant must be engaged, or propose to engage, in the clearance of Options or Futures which are the subject of Exchange Transactions or in the clearance of Fixed Income Transactions or other OTCI transactions through the facilities of the Corporation;

(c) the applicant shall demonstrate to the Corporation that it maintains adequate operations facilities and staff and has sufficient and competent personnel for the expeditious and orderly transactions of business with the Corporation and other Clearing Members, and to meet the requirements of these Rules;

(d) unless the applicable Entity is applying to become a Limited Clearing Member, the applicant has deposited with the Corporation its initial deposit with the Clearing Fund in the amount and at the time required by the Rules and has signed and delivered to the Corporation an agreement in such form as the Board shall require; and

(e) unless the applicable Entity is applying to become a Limited Clearing Member, the applicant has provided the Corporation with its initial Supplemental Liquidity Contributions to the Supplemental Liquidity Fund in the amount and at the time required by the Rules and the Risk Manual;

(f) the applicant must meet the cybersecurity requirements then in effect in accordance with Section A-225.

[…]

RULE A-2 – MISCELLANEOUS REQUIREMENTS

[…]

Section A-225 - Cybersecurity Requirements

A Clearing Member must maintain a comprehensive cybersecurity program and framework that considers potential cyber threats that may impact their organization and protect the confidentiality, integrity, and availability requirements of their systems and information.

A Clearing Member must (a) update its cybersecurity program and framework risk processes periodically based on a risk assessment or changes to technology, business activities, the threat environment, and/or regulatory environment and; (b) use industry best practices and major global security standards to protect the interface and/or connectivity between its systems and those of CDCC, in order to prevent the interruption or contamination of CDCC's systems in the event of a security incident at the Clearing Member.

In a manner and at a frequency that will be determined in its sole discretion, the Corporation may review the Clearing Member's cybersecurity program and framework and make any recommendations deemed necessary or desirable. The Clearing Member shall comply with any such recommendation within the timeframe prescribed by the Corporation.

Each Clearing Member shall indemnify and hold harmless CDCC, its affiliates and subsidiaries, and their respective partners, directors, trustees, officers, employees and agents, from and against any loss, damage, cost, expense, liability or claim (including the cost of legal counsel to advise on or defend against such claims) suffered or incurred by or made against it, them or any of them arising from a breach by a Clearing Member of the cybersecurity requirements.

In the event that the Corporation must correct or modify its systems, in any manner, due to a cybersecurity breach of a Clearing Member or a third party having access to the Clearing Member's systems, the Corporation shall be entitled to recover all costs and expenses incurred to make that correction or modification directly from such Clearing Member.

The failure to comply with such rule or procedures shall also subject such Clearing Member to disciplinary action pursuant to the Rules.

Section A-226 – Cybersecurity Remedies

The Corporation may in lieu of other measures contained in these Rules, impose the following remedies if it determines, that a Clearing Member is in breach of the cybersecurity requirements:

1. A fine not exceeding $50,000;
2. Require a Clearing Member to appoint, at its own expense, an auditor acceptable to the Corporation, to prepare a report on the Clearing Member's cybersecurity status and the corrective actions to be taken to meet the Corporation's cybersecurity requirements. The auditor's report shall be shared with the Corporation and Clearing Member.

If a Clearing Member continues to be in breach of any cybersecurity requirements or fails to take corrective actions at the Corporation's satisfaction, the Corporation may take any other measure contained in Section A-226 or such other action as provided in the Rules.