CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

CSA Staff Notice 11-338
CSA Market Disruption Coordination Plan

October 18, 2018

Executive Summary

The Canadian Securities Administrators (the **CSA** or **we**) are publishing CSA Staff Notice 11-338 *CSA Market Disruption Coordination Plan* (the Notice) to inform the public about the CSA's coordination process to address a market disruption, including one that stems from a large-scale cybersecurity incident.

The Notice reiterates the obligations of market participants with respect to market disruption incidents, including notification requirements to regulators and dissemination of information to the public. The Notice also provides a description of the role of authorities in a market disruption situation if fair and orderly markets have been compromised.

I. Introduction

A market disruption has the potential to cause considerable disruption to the Canadian capital markets. Market disruption events may impact marketplaces, clearing agencies and registrants, including market participants beyond the traditional securities sector, for example banks and pension funds. These events may impair the ability of market participants to promptly and reliably trade, clear and settle transactions. Consequently, a market disruption may compromise investor protection and the operation of fair, efficient and orderly markets in Canada.

Role of the CSA

The CSA oversee registrants, and regulated entities[1] (collectively, **Market Participants**). Market Participants face potential risks relating to systems integrity and the CSA have introduced rules related to systems requirements and cybersecurity aimed at mitigating those risks. For example, National Instrument 21-101 *Marketplace Operation* (**NI 21-101**) and National Instrument 24-102 *Clearing Agency Requirements* (**NI 24-102**) require marketplaces and clearing agencies to develop and maintain an adequate system of internal controls over their critical systems and adequate information technology general controls. Marketplaces and clearing agencies are also required to participate in industry-wide business continuity plan testing, which may include cyber incident scenarios. National Instrument 31-103 *Registration Requirements, Exemptions, and Ongoing Registrant Obligations* (**NI 31-103**) also includes internal controls and systems requirements applicable to registrants.

II. Background

The CSA have undertaken a number of initiatives to integrate incident management and cyber-related activities into its work and have also engaged with industry participants and other

[1] Regulated entities include marketplaces, clearing agencies, self-regulatory organizations, contingency funds and information processors.

stakeholders.

On September 26, 2013, the CSA published Staff Notice 11-326 *Cyber Security* (the **2013 Notice**).[2] The 2013 Notice stated that strong and tailored cybersecurity measures were an important element of Market Participants' controls. Market Participants were reminded that they should take the appropriate protective measures necessary to safeguard themselves and their clients or stakeholders.

On September 27, 2016, the CSA published Staff Notice 11-332 *Cyber Security*[3]. That notice further highlighted the importance of cyber risks for Market Participants, referenced existing published information and guidance on cybersecurity incident management, including work published by the Investment Industry Regulatory Organization of Canada (**IIROC**), the Mutual Fund Dealers Association of Canada (**MFDA**) and international regulatory authorities and standard-setting bodies, and communicated general expectations for Market Participants with respect to their cybersecurity frameworks.

The CSA hosted a roundtable on February 27, 2017 to explore cybersecurity issues and opportunities for greater collaboration, communication and coordination in the event of a large-scale market disruption event. We published CSA Staff Notice 11-336 *Summary of CSA Roundtable on Response to Cyber Security Incidents* on April 6, 2017 to provide an overview of the themes discussed and some of the main takeaways.

A key takeaway from the roundtable was that Market Participants appear to have comprehensive incident response plans and sufficient controls in place to address disruption events at the entity level, including disruptions caused by a cybersecurity incident. However, an opportunity was identified to clarify roles of Market Participants and regulators in the event of a market-wide disruption event, and to work towards more formal coordination processes beyond the existing processes that are in place, including coordination across sectors.

Since the roundtable, the CSA engaged in improving communication and information sharing between Market Participants and regulators in securities markets and, where relevant, other sectors in the event of a market-wide disruption event. To this end, the CSA developed more formal steps that we would follow in the event of a market-wide disruption.

In this Notice, we provide an understanding of the main features of the CSA procedures and the role regulated entities and various authorities have in responding to, and coordinating in the event of, a market-wide disruption situation.

[2] Published at: http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm

[3] Published at: https://www.securities-administrators.ca/aboutcsa.aspx?id=1520

III. Overview of the CSA procedures

Types of Market Disruption Events
While it is not possible to anticipate every market disruption event, some types of market disruption events include those stemming from cybersecurity incidents, physical disasters, major geopolitical events, critical infrastructure disruptions, default of a key or integrated investment dealer, and disruptions on foreign marketplaces. The key principle guiding our actions is to ensure that markets continue to be fair, efficient and orderly, and overall market integrity is not compromised.

Scope
The CSA have implemented procedures that outline the role of applicable CSA staff[4] across jurisdictions and documented the steps CSA oversight staff would follow in a market disruption event.

According to our procedures, a market disruption event refers to an event, or a series of events, that impacts the ability of Market Participants to operate in a regular manner. CSA procedures set out guidelines to address circumstances in which there may not be fair and efficient markets due to a market disruption, for instance a considerable disruption to the ability of some or all Market Participants to promptly and reliably trade, clear or settle transactions.

It is important to clarify the interpretation of "incident' and "market disruption event". A material systems failure, malfunction, delay or security breach would qualify as an incident[5]. The CSA consider a failure, malfunction or delay to be "material" if the marketplace or clearing agency would in the normal course of operations escalate the matter to or inform its senior management ultimately accountable for technology[6].

Even if an incident is material and reportable to a regulatory body, it does not necessarily mean the Canadian capital markets ecosystem is in jeopardy. An incident may impact the ability of an affected regulated entity to operate in a regular manner; however, it may or may not come to be a market-wide disruption event.

The CSA procedures are designed to deal with a market-wide disruption that arises from an incident, or a series of incidents, that compromise market integrity in general—in other words, situations that cause Canadian capital markets to not operate in a fair, reliable, secure, accurate and efficient manner. Factors to be considered in determining whether an incident, or a series of

---

[4] CSA oversight staff includes representatives from the Market Structure & Exchange Oversight Committee, Clearing Agency, Trade Repository and Matching Service Utility Oversight Committee, Registrant Regulation Committee and SRO Oversight Committee.

[5] Subsection 12.1(c) of NI 21-101 requires marketplaces to promptly notify the regulator or, in Québec, the securities regulatory authority and, if applicable, its regulation services provider, of any material systems failure, malfunction, delay or security breach and provide timely updates on the status of the failure, malfunction, delay or security breach, the resumption of service and the results of the marketplace's internal review of the failure, malfunction, delay or security breach.
Subsection 4.6(c) of NI 24-102 requires a recognized clearing agency to promptly notify the regulator or, in Québec, the securities regulatory authority of any material systems failure, malfunction, delay or security breach, and provide timely updates on the status of the failure, malfunction, delay or security breach, the resumption of service, and the results of the clearing agency's internal review of the failure, malfunction, delay or security breach.

[6] Subsection 14.1(4) of Companion Policy 21-101CP and subsection 4.6(c) of Companion Policy 24-102CP.

incidents, has market-wide implications include the breadth of market stakeholders affected, prudential impacts and business continuity of Market Participants in the Canadian capital markets more generally.

In the event of a market disruption, CSA staff will identify the relevant actions that should be undertaken until an affected regulated entity has normalized operations. CSA staff have developed specific procedures for a cybersecurity event, that emphasize the speed at which the disruption advances, the risk of contagion and communication with other relevant federal and provincial organizations.

Regulatory Organizations and Market Participants that May Be Involved
As discussed, the scope of our procedures covers Market Participants in order to ensure a holistic and cross-sectoral approach. With respect to coordination and communication, the CSA will be guided by the requirements of respective memorandums of understanding (**MOUs**) amongst CSA members[7] as well as MOUs entered into by certain CSA jurisdictions and other authorities[8]. Depending on the incident and the affected Market Participant, staff will contact other relevant authorities, regulatory organizations and contingency funds, including the Bank of Canada, IIROC, MFDA, the Office of the Superintendent of Financial Institutions (**OSFI**) and the Canadian Investor Protection Fund (**CIPF**), as appropriate, to work together to address the disruption event.

Notification Requirements
Under various rules, regulations and/or recognition orders, each regulated entity is required to notify its regulator when it experiences a material systems incident. Prompt notification of a material systems incident will put CSA staff on alert and, accordingly, they can consider whether the incident has market-wide implications, and thus qualify as a market disruption event.

Regulated exchanges and clearing agencies are subject to recognition or exemption orders issued by various CSA jurisdictions, which may contain requirements related to incident reporting. Regulated exchanges are also subject to incident reporting requirements under NI 21-101, and regulated clearing agencies to those found in NI 24-102. Additionally, systemically important clearing agencies are required to inform the Bank of Canada when they experience a market disruption event.

Similar to regulated exchanges, alternative trading systems (**ATSs**) are required to inform the CSA in order to comply with the incident reporting requirements under NI 21-101 for marketplaces. Additionally, ATSs conducting business in Canada are required to inform IIROC

---

[7] MOUs amongst CSA members include:

- Memorandum of Understanding respecting the Oversight of Exchanges and Quotation and Trade Reporting Systems
- Memorandum of Understanding Respecting the Oversight of Clearing Agencies, Trade Repositories and Matching Service Utilities
- Memorandum of Understanding Regarding Oversight of Investment Industry Regulatory Organization of Canada
- Memorandum of Understanding Regarding Oversight of the Mutual Fund Dealers Association of Canada
- Memorandum of understanding between the Canadian Securities Administrators and the Canadian Investor Protection Fund

[8] MOUs entered into by certain CSA parties and other authorities include:

- Memorandum of Understanding Respecting the Oversight of Certain Clearing and Settlement Systems

when they experience a material systems incident.

In cases where the requirement to 'promptly notify' regulators exist, the CSA's expectation is that a regulated entity will notify the CSA of a material systems issue, orally or in writing, upon escalating the matter to its senior management. Detailed reporting requirements exist for clearing agencies and some marketplaces. However, standardized requirements for all marketplaces are being developed and will be published in the coming months.

Market disruption event process
Steps taken by CSA staff in addressing a market disruption include identifying staff that will be involved in responding to a market disruption event, communicating with the CSA and external parties, including IIROC, MFDA, CIPF, OSFI and the Bank of Canada, where appropriate, and developing recommendations for determining an appropriate course of action.

In summary, the CSA will consider the materiality of an incident in making a decision on how to respond. The CSA will gather information about the developing situation and take action, if necessary. We will abide by the requirements of the MOUs we have agreed to and work with other relevant authorities, regulatory organizations and contingency funds to foster fair and efficient markets and contribute to the stability of Canada's financial system.

IV. Next Steps

The CSA will continue to monitor developments in incident management practices, including those related to cybersecurity, and take steps where appropriate to integrate incident management and cybersecurity related activities into its work and to interact with Market Participants and other stakeholders. The CSA will review and update its procedures on a regular basis.

V. Questions

Questions and comments may be referred to:

Herman Tan Senior Analyst, Market Structures Autorité des marchés financiers Herman.Tan@lautorite.qc.ca	Alex Petro Trading Specialist, Market Regulation Ontario Securities Commission apetro@osc.gov.on.ca
Paula Kaner Manager, Market Oversight Alberta Securities Commission paula.kaner@asc.ca	Doug MacKay Manager, Market and SRO Oversight British Columbia Securities Commission dmackay@bcsc.bc.ca
Paula White Deputy Director Compliance and Oversight Manitoba Securities Commission paula.white@gov.mb.ca	
