AMENDMENTS TO *POLICY STATEMENT TO REGULATION 21-101 RESPECTING MARKETPLACE OPERATION*

1. Section 6.1 of *Policy Statement to Regulation 21-101 respecting Marketplace Operation* is amended, in paragraph (6), by replacing "7 business days" with "15 business days".

2. Section 6.2 of the Policy Statement is replaced with the following:

"**6.2. Filing of Financial Statements**

Part 4 of the Regulation sets out the financial reporting requirements applicable to marketplaces. Subsections 4.1(2) and 4.2(2) respectively require an ATS to file audited financial statements initially, together with Form 21-101F2, and on an annual basis thereafter. These financial statements may be in the same form as those filed with IIROC. The annual audited financial statements may be filed with the Canadian securities regulatory authorities at the same time as they are filed with IIROC.

Section 4.3 requires recognized exchanges and recognized quotation and trade reporting systems to file interim financial reports within 45 days after the end of each interim period. In the view of the Canadian securities regulatory authorities, the term interim period means a period commencing on the first day of the recognized exchange's or quotation and trade reporting system's financial year and ending 9, 6 or 3 months before the end of the same financial year.

The Canadian securities regulatory authorities expect that financial statements and reports filed under subsections 4.2 and 4.3 should disclose the accounting principles used to prepare them. For clarity, financial statements and reports should include:

(a) in the case of annual financial statements, an unreserved statement of compliance with IFRS;

(b) in the case of an interim financial report, an unreserved statement of compliance with International Accounting Standard 34 *Interim Financial Reporting*.".

3. Section 14.1 of the Policy Statement is amended:

(1) by replacing paragraphs (1) to (3.1) with the following:

"(1) Paragraph 12.1(a) of the Regulation requires the marketplace to develop and maintain adequate internal controls over the systems specified. As well, the marketplace is required to develop and maintain adequate general computer controls. These are the controls which are implemented to support information technology planning, acquisition, development and maintenance, computer operations, information systems support, cyber resilience, and security. Recognized guides as to what constitutes adequate information technology controls may include guidance, principles or frameworks published by the Chartered Professional Accountants – Canada (CPA Canada), American Institute of Certified Public Accountants (AICPA), Information Systems Audit and Control Association (ISACA), International Organization for Standardization (ISO) or the National Institute of Standards and Technology (U.S. Department of Commerce) (NIST). We are of the view that internal controls include controls that support the processing integrity of the models used to quantify, aggregate, and manage the marketplace's risks.

"(2) Capacity management requires that a marketplace monitor, review, and test (including stress test) the actual capacity and performance of its systems on an ongoing basis. Accordingly, paragraph 12.1(b) of the Regulation requires a marketplace to meet certain systems capacity, processing capability and disaster recovery standards. These standards are consistent with prudent business practice. The activities and tests required in this paragraph are to be carried out at least once every 12 months. In practice, continuing

changes in technology, risk management requirements and competitive pressures will often result in these activities being carried out or tested more frequently.

"(2.1) Paragraph 12.1(c) of the Regulation requires a marketplace to promptly notify the regulator or, in Québec, the securities regulatory authority of any systems failure, malfunction, delay or security incident that is material. A failure, malfunction, delay or security incident is considered "material" if the marketplace would, in the normal course of operations, escalate the matter to or inform senior management ultimately accountable for technology. Such events would not generally include those that have or would have little or no impact on the marketplace's operations or on participants. Non-material events may become material if they recur or have a cumulative effect. With respect to the prompt notification requirement, the Canadian securities regulatory authorities expect that a marketplace will provide notification of a systems failure, malfunction, delay or security incident that is material, orally or in writing, upon escalating the matter to its senior management. It is expected that, as part of the required notification, the marketplace will provide updates on the status of the failure, malfunction, delay or incident and the resumption of service. The marketplace should also have comprehensive and well-documented procedures in place to record, report, analyze, and resolve all incidents. In this regard, the marketplace should undertake a "post-incident" review to identify the causes and any required improvement to the normal operations or business continuity arrangements. Such reviews should, where relevant, include the marketplace's participants. The results of such internal reviews are required to be communicated to the regulator or, in Québec, securities regulatory authority as soon as practicable. A security incident is considered to be any event that actually or potentially jeopardizes the confidentiality, integrity or availability of any of the systems that support the functions listed in section 12.1 or any system that shares network resources with one or more of these systems or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies. Any security incident that requires non-routine measures or resources by the marketplace would be considered material and thus reportable to the regulator or, in Québec, securities regulatory authority. The onus would be on the marketplace to document the reasons for any security incident it did not consider material. Marketplaces should also have documented criteria to guide the decision on when to publicly disclose a security incident. The criteria for public disclosure of a security incident should include, but not be limited to, any instance in which client data could be compromised. Public disclosure should include information on the types and number of participants affected.

"(3) Subsection 12.2(1) of the Regulation requires a marketplace to engage one or more qualified external auditors to conduct an annual independent systems review to assess the marketplace's compliance with paragraph 12.1(a), section 12.1.1 and section 12.4 of the Regulation. The review must be conducted and reported on at least once in each 12-month period by a qualified external auditor in accordance with established audit standards and best industry practices. We consider that best industry practices include the "Trust Services Criteria" developed by the American Institute of CPAs and CPA Canada. The focus of the assessment of any systems that share network resources with trading-related systems required under paragraph 12.2(1)(b) would be to address potential threats from a security incident that could negatively impact a trading-related system. For purposes of subsection 12.2(1), we consider a qualified external auditor to be a person or a group of persons with relevant experience in both information technology and in the evaluation of related internal controls in a complex information technology environment. Before engaging a qualified external auditor to conduct the independent systems review, a marketplace is expected to discuss its choice of external auditor and the scope of the systems review mandate with the regulator or, in Québec, the securities regulatory authority. We further expect that the report prepared by the external auditor include, to the extent applicable, an audit opinion that (i) the description included in the report fairly presents the systems and controls that were designed and implemented throughout the reporting period, (ii) the controls stated in the description were suitably designed, and (iii) the controls operated effectively throughout the reporting period.

"(3.1) Section 12.1.2 of the Regulation requires a marketplace to engage one or more qualified parties to perform appropriate assessments and testing to identify

security vulnerabilities and measure the effectiveness of information security controls. We would expect a marketplace to implement appropriate improvements where necessary. For the purposes of section 12.1.2, we consider a qualified party to be a person or a group of persons with relevant experience in both information technology and in the evaluation of related internal systems or controls in a complex information technology environment. We consider that qualified parties may include external auditors or third party information system consultants, as well as employees of the marketplace or an affiliated entity of the marketplace but may not be persons responsible for the development or operation of the systems or capabilities being tested. The regulator or, in Québec, the securities regulatory authority may, in accordance with securities legislation, require the marketplace to provide a copy of any such assessment.";

(2) by repealing paragraph (4);

(3) by replacing paragraph (5) with the following:

"(5) Under section 15.1 of the Regulation, the regulator or, in Québec, the securities regulatory authority may consider granting a marketplace an exemption from the requirements to engage one or more qualified external auditors to conduct an annual independent systems review and prepare a report under subsection 12.2(1) of the Regulation provided that the marketplace prepare a control self-assessment and file this self-assessment with the regulator or, in Québec, the securities regulatory authority. The scope of the self-assessment would be similar to the scope that would have applied if the marketplace underwent an independent systems review. Reporting of the self-assessment results and the timeframe for reporting would be consistent with that established for an independent systems review.

In determining if the exemption is in the public interest and the length of the exemption, the regulator or, in Québec, the securities regulatory authority may consider a number of factors including: the market share of the marketplace, the timing of the last independent systems review, changes to systems or staff of the marketplace and whether the marketplace has experienced material systems failures, malfunction or delays.".

4. Section 14.3 of the Policy Statement is amended by inserting, in paragraph (1) and before the first sentence, the following:

"Business continuity management is a key component of a marketplace's operational risk-management framework.".