ANNEX A

Amendments to
National Instrument 21-101 *Marketplace Operation*

1. National Instrument 21-101 Marketplace Operation is amended by this Instrument.

2. Section 3.2 is amended

(a) in subsection (2) by replacing "seven***" with "***15***",***

(b) in paragraph (3)(a) by replacing "month***" with "***calendar quarter***", and***

(c) by adding the following subsection:

(6) For purposes of subsection (5), where information in a marketplace's Form 21-101F1 or Form 21-101F2, as applicable, has not changed since the marketplace previously filed Form 21-101F1 or Form 21-101F2 under subsection (5), the marketplace may incorporate that information by reference into its updated and consolidated Form 21-101F1 or Form 21-101F2**..**

3. Subsection 4.2(1) is amended by deleting "the requirements outlined in***".***

4. Part 4 is amended by adding the following section:

4.3 Filing of Interim Financial Reports

A recognized exchange and a recognized quotation and trade reporting system must file interim financial reports within 45 days after the end of each interim period in accordance with paragraphs 4.1(1)(a) and (b)**..**

5. Subparagraph 12.1(a)(i) is replaced with the following:

(i) adequate internal controls over those systems, and**.**

6. Subparagraph 12.1(a)(ii) is amended by adding "cyber resilience, ***after "***information security,***".***

7. Subparagraph 12.1(b)(ii) is replaced with the following:

(ii) conduct capacity stress tests to determine the processing capability of those systems to perform in an accurate, timely and efficient manner,**.**

8. Paragraph 12.1(c) is replaced with the following:

(c) promptly notify the regulator or, in Québec, the securities regulatory authority and, if applicable, its regulation services provider, of any systems failure, malfunction, delay or security incident that is material and provide timely updates on the status of the failure, malfunction, delay or security incident, the resumption of service and the results of the marketplace's internal review of the failure, malfunction, delay or security incident, and**.**

9. Section 12.1 is amended by adding the following paragraph:

(d) keep a record of any systems failure, malfunction, delay or security incident and, if applicable, document the reasons why the marketplace considered the systems failure, malfunction, delay or security incident not to be material**..**

10. Section 12.1.1 is replaced with the following:

12.1.1 Auxiliary Systems - For each system that shares network resources with one or more of the systems, operated by or on behalf of the marketplace, that supports order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing, that, if breached, would pose a security threat to one or more of the previously mentioned systems, a marketplace must

(a) develop and maintain adequate information security controls that relate to the security threats posed to any system that supports order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing, and

(b) promptly notify the regulator, or in Québec, the securities regulatory authority and, if applicable, its regulation services provider, of any security incident that is material and provide timely updates on the status of the incident, the resumption of service and the results of the marketplace's internal review of the security incident, and

(c) keep a record of any such security incident and, if applicable, document the reasons why the marketplace considered that such security incident was not material**..**

11. Part 12 is amended by adding the following section:

12.1.2 Vulnerability Assessments - On a reasonably frequent basis and, in any event, at least annually, a marketplace must engage one or more qualified parties to perform appropriate assessments and testing to identify security vulnerabilities and measure the effectiveness of information security controls that assess the marketplace's compliance with paragraphs 12.1(a) and 12.1.1(a)**..**

12. Subsection 12.2(1) is replaced with the following:

(1) On a reasonably frequent basis and, in any event, at least annually, a marketplace must engage one or more qualified external auditors to conduct an independent systems review and prepare a report in accordance with established audit standards and best industry practices that assesses the marketplace's compliance with

(a) paragraph 12.1(a),

(b) section 12.1.1, and

(c) section 12.4**..**

13. In the following provisions "and***" is replaced with "***or***":***

(a) Paragraph 12.3(1)(a); and

(b) Paragraph 12.3(2)(a).

14. Paragraph 12.3(3.1)(a) is amended by replacing "(2)(a)***" with "***(2)(b)***".***

15. Subsection 12.4(3) is replaced with the following:

(3) A recognized exchange or quotation and trade reporting system that directly monitors the conduct of its members or users and enforces requirements set under section 7.1(1) or 7.3(1) of NI 23-101 must establish, implement, and maintain policies and procedures reasonably designed to ensure that each system, operated by or on behalf of the recognized exchange or quotation and trade reporting system, that is critical and supports real-time market surveillance, can resume operations within two hours following the declaration of a disaster at the primary site by the exchange or quotation and trade reporting system**.**

16. Section 14.5 is amended by renumbering it as subsection 14.5(1).

17. Paragraph 14.5(1)(a) is amended

(a) in subparagraph (i) by deleting "an***",***

(b) in subparagraph (i) by deleting "system of***" after "***adequate***", and***

(c) in subparagraph (ii) by adding "cyber resilience,***" following "***information security,***".***

18. Subparagraph 14.5(1)(b)(ii) is replaced with the following:

(ii) conduct capacity stress tests of its critical systems to determine the processing capability of those systems to perform in an accurate, timely and efficient manner,**.**

19. Paragraph 14.5(1)(c) is replaced with the following:

(c) on a reasonably frequent basis and, in any event, at least annually engage one or more qualified external auditors to conduct an independent systems review and prepare a report in accordance with established audit standards and best industry practices that assesses the information processor's compliance with paragraph (a) and section 14.6,**.**

20. Subparagraph 14.5(1)(d)(ii) is amended by deleting "and***" following "***year end***,".***

21. Paragraph 14.5(1)(e) is replaced with the following:

(e) promptly notify the following of any systems failure, malfunction, delay or security incident that is material and provide timely updates on the status of the failure, malfunction, delay or security incident, the resumption of service and the results of the information processor's internal review of the failure, malfunction, delay or security incident:

(i) the regulator or, in Québec, the securities regulatory authority, and

(ii) any regulation services provider, recognized exchange or recognized quotation and trade reporting system monitoring trading of the securities about which information is provided to the information processor, and**.**

22. Subsection 14.5(1) is amended by adding the following paragraph:

(f) keep a record of any systems failure, malfunction, delay or security incident and, if applicable, document the reasons why the information processor considered the systems failure, malfunction, delay or security incident not to be material.

23. Section 14.5 is amended by adding the following subsection:

(2) An information processor must provide the regulator or, in Québec, the securities regulatory authority with a report by the 30th day after the end of the calendar quarter, containing a log and summary description of each systems failure, malfunction, delay or security incident referred to in paragraph (1)(f).

24. Part 14 is amended by adding the following section:

14.5.1 Vulnerability Assessments

On a reasonably frequent basis and, in any event, at least annually, an information processor must engage one or more qualified parties to perform appropriate assessments and testing to identify security vulnerabilities and measure the effectiveness of information security controls that assess the information processor's compliance with paragraph 14.5(1)(a).

25. Exhibit B of Form 21-101F1 is replaced with the following:

Exhibit B – Ownership

For an exchange or quotation and trade reporting system that is a corporation, provide a list of the beneficial holders of five percent or more of any class of securities of the exchange or quotation and trade reporting system. For each listed security holder, please provide the following:

1. Name.

2. Principal business or occupation and title.

3. Ownership interest, including the total number of securities held, the percentage of the exchange or quotation and trade reporting system's issued and outstanding securities held, and the class or type of security held.

4. Whether the security holder has control (as interpreted in subsection 1.3(2) of National Instrument 21-101 Marketplace Operation).

In the case of an exchange or quotation and trade reporting system that is a partnership, sole proprietorship, or other form of organization, please provide a list of the registered or beneficial holders of the partnership interests or other ownership interests in the exchange or quotation and trade reporting system. For each person or company listed, please provide the following:

1. Name.

2. Principal business or occupation and title.

3. Nature of the ownership interest, including a description of the type of partnership interest or other ownership interest.

4. Whether the person or company has control (as interpreted in subsection 1.3(2) of National Instrument 21-101 Marketplace Operation)**..**

26. Item 5 of section 1 of Exhibit C of Form 21-101F1 is repealed.

27. Exhibit D of Form 21-101F1 is amended by

(a) repealing Item 2 of section 2,

(b) repealing Item 5 of section 2, and

(c) repealing Item 6 of section 2.

28. Exhibit G of Form 21-101F1 is amended by replacing "are***" with "***is***" in Item 2 under "****IT Risk Assessment***".***

29. Exhibit B of Form 21-101F2 is replaced with the following:

Exhibit B – Ownership

For an ATS that is a corporation, provide a list of the beneficial holders of five percent or more of any class of securities of the ATS. For each listed security holder, please provide the following:

1. Name.

2. Principal business or occupation and title.

3. Ownership interest, including the total number of securities held, the percentage of the ATS's issued and outstanding securities held, and the class or type of security held.

4. Whether the security holder has control (as interpreted in subsection 1.3(2) of National Instrument 21-101 Marketplace Operation).

In the case of an ATS that is a partnership, sole proprietorship, or other form of organization, please provide a list of the registered or beneficial holders of the partnership interests or other ownership interests in the ATS. For each person or company listed, please provide the following:

1. Name.

2. Principal business or occupation and title.

3. Nature of the ownership interest, including a description of the type of partnership interest or other ownership interest.

4. Whether the person or company has control (as interpreted in subsection 1.3(2) of National Instrument 21-101 Marketplace Operation)**..**

30. Item 5 of section 1 of Exhibit C of Form 21-101F2 is repealed.

31. Exhibit D of Form 21-101F2 is amended by

(a) repealing Item 2 of section 2, and

(b) repealing Item 5 of section 2.

32. Exhibit G of Form 21-101F2 is amended by replacing "are***" with "***is***" in Item 2 under "****IT Risk Assessment***".***

33. Section 6 of Part A of Form 21-101F3 is replaced with the following:

6. Systems – A log and summary description of systems failures, malfunctions, delays or security incidents during the quarter in respect of any systems, operated by or on behalf of the marketplace, that support order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing and a log and summary description of each security incident during the quarter for any system that shares network resources with one or more of the systems, operated by or on behalf of the marketplace, that supports order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing that, if breached, would pose a security threat to one or more of the previously mentioned systems.**.**

34. Section 1 of Part B in Chart 1 of Form 21-101F3 under the heading "Exchange-Traded Securities***" is amended by***

(a) deleting row 1, and

(b) deleting row 2.

35. Section 1 of Part B in Chart 3 of Form 21-101F3 is amended by

(a) by deleting row 2, and

(b) by deleting row 7.

36. Section 1 of Part B of Form 21-101F3 is amended by repealing Item 5 and Chart 5.

37. Item 5 of section 1 of Exhibit C of Form 21-101F5 is repealed.

38. The Instrument comes into force on [●], 2019.

Schedule 1

Changes to
Companion Policy 21-101CP *Marketplace Operation*

1. Companion Policy 21-101CP Marketplace Operation is changed by this Document.

2. Subsection 6.1(6) is changed by replacing "seven***" with "***15***" immediately before "***business days before the expected implementation date***".***

3. Section 6.2 is replaced with the following:

Filing of Financial Statements

Part 4 of the Instrument 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 nine, six or three 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*.

4. Section 14.1 is changed by replacing subsection (1) with the following:

(1) Paragraph 12.1(a) of the Instrument 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**.**

5. Section 14.1 is changed by replacing subsection (2) with the following:

(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 Instrument 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**.**

6. Section 14.1 is changed by replacing subsection (2.1) with the following:

(2.1) Paragraph 12.1(c) of the Instrument 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, the 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, the 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**.**

7. Section 14.1 is changed by replacing subsection (3) with the following:

(3) Subsection 12.2(1) of the Instrument 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 Instrument. 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 company or a group of persons or companies 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**.**

8. Section 14.1 is changed by replacing subsection (3.1) with the following:

(3.1) Section 12.1.2 of the Instrument 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 company or a group of persons or companies 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**.**

9. Section 14.1 is changed by deleting subsection (4).

10. Section 14.1 is changed by replacing subsection (5) with the following:

(5) Under section 15.1 of the Instrument, 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 Instrument 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**.**

11. Section 14.3 is changed by replacing subsection (1) with the following:

(1) Business continuity management is a key component of a marketplace's operational risk-management framework. Section 12.4 of the Instrument requires that marketplaces develop and maintain reasonable business continuity plans, including disaster recovery plans. Business continuity planning should encompass all policies and procedures to ensure uninterrupted provision of key services regardless of the cause of potential disruption. In fulfilling the requirement to develop and maintain reasonable business continuity plans, the Canadian securities regulatory authorities expect that marketplaces are to remain current with best practices for business continuity planning and to adopt them to the extent that they address their critical business needs**.**

12. These changes become effective on [•], 2019.