Deanna Dobrowsky
Vice President, Regulatory
TMX Group
100 Adelaide Street West, Suite 300
Toronto, Ontario M5H 1S3
T (416) 365-8130
deanna.dobrowsky@tmx.com

July 17, 2019

VIA EMAIL: comments@osc.gov.on.ca; consultation-en-cours@lautorite.qc.ca

Alberta Securities Commission
Autorité des marchés financiers
British Columbia Securities Commission
Financial and Consumer Services Commission (New Brunswick)
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Nova Scotia Securities Commission
Nunavut Securities Office
Ontario Securities Commission
Officer of the Superintendent of Securities, Newfoundland and Labrador
Officer of the Superintendent of Securities, Northwest Territories
Office of the Yukon Superintendent of Securities
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island

The Secretary
Ontario Securities Commission
20 Queen Street West, 22nd Floor
Toronto, ON M5H 3S8

Me Philippe Lebel
Secrétaire général et directeur général des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Dear Sirs/Madams,

RE: Proposed Amendments to National Instrument 21-101 and Companion Policy 21-101

TMX Group Limited ("**TMX Group**") appreciates the opportunity to comment on proposed amendments to National Instrument 21-101 ("**NI 21-101**") and Companion Policy 21-101 ("**21-101CP**") published by the Canadian Securities Administrators (the "**CSA**") for public comment on April 18, 2019 (collectively, the "**Proposed Amendments**"). TMX Group owns four marketplaces that are subject to NI 21-101: Toronto Stock Exchange, TSX Venture Exchange, TSX Alpha Exchange, and the Bourse de Montreal. TMX Group is also required to make filings under NI 21-101 although it does not directly perform exchange activities.

In general, we support the Proposed Amendments that are focused on burden reduction. We are concerned, however, with certain Proposed Amendments that could increase the burden on marketplaces without commensurate benefit to the CSA.

Proposed Amendments to Reduce Regulatory Burden:

1) Amendments to Form 21-101F1 and Form 21-101F3

We commend the CSA for reducing the frequency for the requirement to file Form 21-101F1 from monthly to quarterly. We also commend the new option to incorporate information by reference in the annual updated and consolidated filings. Combined with the reduced frequency of reporting, this option will significantly reduce the size and complexity of the filed Form 21-101F1s, while ensuring that regulators maintain access to pertinent information. To achieve further efficiency, we urge the CSA to consider removing the requirement to file an annual consolidated Form 21-101F1. The annual filing is burdensome as it takes effort to consolidate periodic filings into one aggregate filing, and the annual filing does not provide any information that is not already filed during the periodic filings. As all filings are electronic, the value of consolidating the regular filings on an annual basis seems reduced as regulators already have access to all the information that an annual filing would contain.

We note that changing the reporting timeframe for non-significant changes from monthly to quarterly for Form 21-101F1 may result in unintended duplication in the contents of Form 21-101F3. As Form 21-101F1 will now be filed within 10 days of the quarter end and Form 21-101F3 is filed within 30 days of the same quarter end, both forms will cover the same filing period. Therefore, certain sections of the forms will now include very similar content. For example, in respect of information filed in the Form 21-101F1 during the reporting period, section A4 of Form 21-101F3 ask for a list of amendments filed and implemented, and section A5 of Form 21-101F3 ask for a list of amendments filed and not implemented. The changes caught by these sections A4 and A5 of Form 21-101F3 will also be filed and described in greater detail in the proposed quarterly Form 21-101F1. Though Form 21-101F3 will be filed after Form 21-101F1 during each quarterly filing month, the information contained in Form 21-101F1 will be substantially similar, as the reporting period for the forms will be identical. We believe that these Form 21-101F3 sections will be highly duplicative of the Form 21-101F1 filings made earlier during each filing month and we urge the CSA to consider removing these sections from the Form 21-101F3.

We also commend the CSA for removing certain reporting requirements from Form 21-101F3 that duplicate information that is already collected and made available to the CSA by the Investment Industry Regulatory Organization of Canada ("**IIROC**"). We believe that the CSA could also remove these reporting requirements, as the information is also available from IIROC:

i. Chart 3: Order information
ii. Chart 4: Most traded securities
iii. Chart 9: Concentration of trading by marketplace participant

2) Provisions related to the requirement to report 5% shareholders in Form 21-101F1

The revisions to Exhibit B of Form 21-101F1 include a requirement to report beneficial holders of 5 percent or more of any class of securities for an exchange that is a corporation and to include disclosure of the class of securities held. We note that as a publicly traded corporation, it is not practical to obtain ownership information for 5 percent shareholders given that specific ownership percentages can change quickly as a result of shares being publicly traded, and that the identity of beneficial owners may be difficult (if not impossible) to obtain. For example, if the beneficial owner is an individual, this person may hold the shares in the name of his or her broker and may be an Objecting Beneficial Owner ("**OBO**"), in which case TMX Group would be unable to ascertain ownership. Similarly, the current requirement for publicly traded exchanges to disclose information regarding their registered owners is not practical. For registered owners, shares are typically registered in the name of CDS (this is the case for TMX Group, where the majority of our outstanding shares are registered in CDS's name), thus TMX Group would be unable to readily ascertain ownership. Given that we would only be able to provide disclosure of 5 percent shareholders if

the shareholder is not an OBO and has the shares registered specifically in their own name, we submit that the proposed requirement would likely not produce any information for regulators.

We would also note that securities law already imposes a disclosure obligation on shareholders who beneficially own 10 percent or more of a public company, and the TMX Group recognition order issued by the OSC prohibits ownership of more than 10 percent of the TMX Group shares without OSC approval. We question the requirement to collect and report information of holders below levels that are considered reportable under securities law and would like to obtain clarification on the intended purpose of the information being collected. An alternative could be to create a carve-out for a marketplace that is a public company.

Proposed Amendments that bring New Requirements:

1) Provisions Related to Notification of "Security Incidents" and New Reporting Obligations

The Proposed Amendments include changes to certain notification and reporting obligations for "**Systems**" and "**Auxiliary Systems**" as described below. We are concerned that the Proposed Amendments may have unintended consequences in that they: (i) impose a quarterly reporting requirement of non-material events that, combined with the new definition of "security incident" will result in over-reporting that will be burdensome for marketplaces and not useful for regulators; and (ii) introduce in 21-101CP a broad definition of "security incident" and references to materiality that raise confusion rather than clarity for marketplaces, and may result in a notification regime that is unwieldy and uncertain for marketplaces. We believe that through changes to the Proposed Amendments, particularly in 21-101CP, the CSA could introduce clearer language that would confirm that it should be the impact of the event on key business processes of the marketplaces that should determine the regulatory notification process and any subsequent reporting.

New Notification and Reporting Requirements

Currently, section 12.1(c) of NI 21-1021 requires marketplaces to notify regulators of "any material systems failure, malfunction, delay or security breach." The CSA proposes to change this notification requirement to capture "any systems failure, malfunction, delay or security incident that is material". At the centre of this change is the concept of "security breach", which is proposed to be broadened to "security incident". The main challenge related to this proposed change is the proposed language in section 14.1(2.1) of 21-101CP, which creates confusion rather than clarity. The 21-101CP drafting challenges include: (i) a description of "material" based on internal marketplace reporting activities rather than the impact of the event; (ii) a statement that non-material events may become material events if they reoccur or have a cumulative effect; and (iii) new language which captures events that "potentially" jeopardize the confidentiality, integrity or availability of an information system, and are material. While we believe that the purpose of the Proposed Amendments in 21-101CP is to provide clarity, we are concerned that the Proposed Amendments will, in fact, have the unintended consequences of adding confusion and will result in marketplaces focussing inappropriately on events that are not impactful.

The CSA also proposes to add a new requirement to section 6 of Form 21-101F3, which will require marketplaces to provide a log and summary description of system failures, malfunctions, delays or security incidents. A similar requirement for information processors is being added to section 14.5(2) of NI 21-101. The Proposed Amendments, if enacted, would impose a new mandatory regulatory reporting obligation related to all events regardless of materiality, even where there is no impact to external stakeholders and no impact to marketplace business processes. These new requirements have the effect of adding a new obligation on marketplaces and information processors to classify each security incident, which will divert important technology staff resources from functional work to administrative tasks, solely for the purposes of regulatory notifications. They will also divert resources to the administrative task of documenting non-material system failures, malfunctions, and delays. In our view, creating logs of non-material events solely for regulators is a burden on marketplaces and information processors without a commensurate benefit to our stakeholders.

TMX Concern

The proposed requirement for reporting security incidents that are material is, as per our understanding, referring to any security incident that is critical enough to be escalated to senior management but not necessarily causing a material breach, unauthorized access or compromise of any information assets. TMX Group's cybersecurity incident response standard ("**IR Standard**") has been designed based on the computer security incident handling guide prepared by the National Institute of Standards and Technology ("**NIST**") and also incorporates additional industry best practices and standards. The IR Standard classifies a security incident based on multiple factors with a priority assessment that is represented by severity levels. The priority assessment takes into account confidentiality, integrity, and availability impact assessments to determine the severity level of a security incident in addition to the assessment of the potential and current impact of the occurrence and impact to the business unit or service.

The escalation of a security incident, therefore, is driven by the severity level of the "incident" as per the IR Standard. The IR Standard outlines the severity level at which a security incident would be considered critical and be escalated to senior management as well as to a crisis management team. The new requirement in the Proposed Amendments is not consistent with the current and widely accepted NIST guidelines, which we utilize for our IR Standard. We would note that these NIST guidelines do not currently define "material" "security incidents" and there is no generally accepted definition for a "material" "security incident" that we are aware of. As there is no such concept, there is no severity or impact assessment guidelines currently in place for assessing whether a security incident is "material". If a security incident were to reach a certain level of criticality and impact, it is then handled as per the IR Standards, which drive progressive escalation as required. It is our opinion that notification to regulators for security incidents that would not be reportable events under generally accepted information security standards, will be an inappropriate use of our key resources within the cyber security, information security, risk, and operational teams. In the case of a potential adverse cyber event, resources should be allocated quickly to identify pre and post severity levels, mobilize required internal and external teams and start response and recovery efforts rather than spending time on non-critical security incidents which do not impact stakeholders.

In terms of the new reporting requirements for logs of security incidents found in the aforementioned amendments to Form 21-101F3 and NI 21-101, we would like to confirm that, as per our Security Incident Framework, every incident regardless of severity level, is already documented and kept in the appropriate repository for forensics, audit and regulatory requirements. Additional reports are also created as per the framework and distributed to stakeholders. These are high level summaries of incidents that are automatically generated by our monitoring system and include even the most insignificant false-positive security incident events such as log-in errors or inappropriate website visits. The monitoring systems also attach severity assessments to these incidents, flagging certain events for further investigation and subsequent escalation of security assessments as required. Converting these records into formats easily accessible to regulators would be excessively costly, given the relatively low value of the information such records could convey, and the requirement to perform this conversion on a quarterly basis would divert valuable resources away from more significant tasks. We believe that an unintended consequence of the Proposed Amendments therefore will be the over-reporting of low-level severity incidents that do not impact key business processes. Imposing additional burden on regulated entities without commensurate benefit to regulators and to the industry is a poor outcome, and is inconsistent with work being done by a number of CSA members to reduce unnecessary regulatory burden.

We would be pleased to work with the CSA to revise the wording in the Proposed Amendments related to "security incident" and the definition of "material", to ensure that marketplaces' focus for incident management can continue to be appropriately directed at the incidents that could have a material impact on key business processes. We would like to discuss with the CSA the use by marketplaces of an impact-driven incident reporting methodology that we believe would provide our regulators with the most relevant information in the most efficient manner for both regulators and marketplaces. If we were to agree on the components of the impact-driven incident reporting methodology, we could then collaboratively review with the CSA the Proposed Amendments, and remove any language that causes confusion or that could have the unintended consequence of importing unnecessary regulatory burden into the marketplace oversight regime.

2) Provisions related to annual system reviews – vulnerability assessments

We understand that the new obligation to perform vulnerability assessments would allow for qualified TMX Group staff to perform the assessment and that regular regulatory reporting is not required. As such, we support the provision.

We would also ask that the CSA provide additional clarification on the meaning of the word "models" as used in section 14.1(1) of 21-101CP where the Proposed Amendments include the following statement:

> "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 risk".

Final Remarks

Given that the Proposed Amendments, and in particular, the proposed changes in section 12 of NI 21-101 would impact areas of our enterprise that are highly technical in nature, we would be pleased to discuss these comments with CSA staff.

Sincerely,

Deanna Dobrowsky
Vice President, Regulatory