CANADIAN SECURITY TRADERS ASSOCIATION, INC.
P.O. Box 3, 31 Adelaide Street East
Toronto, Ontario M5C 2H8

July 17, 2014

The Secretary
Ontario Securities Commission
20 Queen Street West
19th Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

and

M[e] Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
consultation-en-cours@lautorite.qc.ca

To Whom It May Concern:

Re: CSA Notice and Request for Comment re: Proposed Amendments to National Instrument 21-101 *Marketplace Operation*

The Canadian Security Traders Association, Inc. (CSTA), is a professional trade organization that works to improve the ethics, business standards and working environment for members who are engaged in the buying, selling and trading of securities (mainly equities). The CSTA represents over 850 traders nationwide, and is led by Governors from each of three distinct regions (Toronto, Montreal and Vancouver). The organization was founded in 2000 to serve as a national voice for our affiliate organizations. The CSTA is also affiliated with the Security Traders Association (STA) in the United States of America, which has approximately 4,200 members globally, making it the largest organization of its kind in the world.

This letter was prepared by the CSTA Trading Issues Committee, a group of 20 appointed members from amongst the CSTA. This committee has an equal proportional number of buy-side and sell-side representatives with various areas of market structure expertise and, as of July 2014, includes 1 independent member. It is important to note that there was no survey sent to our members to determine popular opinion; the committee was assigned the responsibility of presenting the opinion of the CSTA as a whole. The opinions and statements provided below do not reflect the opinions of all CSTA members or the opinion of all members of the Trading Issues Committee.

The CSTA appreciates the opportunity to comment on the proposed amendments to National Instrument 21-101. We have chosen to respond solely to the proposed changes to the provision in section 5.10 of NI 21-101 (the "Proposed Amendments"), which currently prohibits a marketplace from disclosing a marketplace participant's order and trade information to researchers without the marketplace participant's consent.

General Remarks

The CSTA has historically raised objections in various forums regarding the disclosure of proprietary data to researchers, due mainly to concerns regarding the recipients' ability to analyze this data, reverse engineer it and obtain insight into proprietary trading strategies. In the development of the CSTA's position on the Amendment, contributors expressed unanimous concerns around the costs and benefits of proprietary marketplace-originated data being provided for research purposes without the consent of the parties whose data is exposed.

We believe that data intended to be private from the public tape (such as trader IDs, broker attribution where the orders are declared anonymous, or private trade markers) are private for a reason. If some data is deemed to be too sensitive to include on the public tape, the sensitivity does not diminish if it is disclosed selectively to researchers claiming bona-fide uses for the data.

More generally, we believe that the private information content in order data, whether handled by a client, a dealer or a marketplace, represents risks and benefits to the originator of the data. The intermediaries handling such data are tasked with protecting the confidentiality of the end beneficiary. In other words, marketplace disclosure of proprietary data represents a breach of confidentiality, to the detriment of the party entering the order. Any benefits would accrue exclusively to the researchers at question, or the marketplace offering the disclosure. This transfer of costs and benefits represents a fairness concern for the originators of the data: the dealers entering orders onto marketplaces and their clients. This concern is magnified if the marketplace offering private data is being compensated directly or indirectly for this service.

We recognize that the Proposed Amendments attempt to assuage these concerns by imposing a requirement for contractual limitations on the use of private data disclosed by a marketplace for the purpose of research. However, while some Committee members feel that the proposal is a good start, we are collectively not satisfied that the proposal adequately protects the originator of the data. . We note that some contributors felt that all research should be reliant exclusively on publicly available information. If this limitation does not allow for the type of research the CSA is attempting to facilitate, we suggest that further controls are required. We have set out the specific concerns below, with suggested alternatives for a strengthening of controls.

Specific Concerns

We believe that a distinction (contemplated in the Proposed Amendments, 5.10(1.1)(a)(i)) between publication and receipt by a third party with confidentiality obligations does not resolve the problem of improper or inadvertent use. Once confidential data is disclosed to a third party, the action may not be undone and the risk of misuse is too high.

We submit that third party researchers requiring data granular to the Trader ID level implicitly require information identifying the trader and that trader's activities. It is difficult for us to reconcile the implication of providing an identifier to a trader's behavior with the prohibition on "reverse engineering" (Proposed Companion Policy, section 7.7 (1)) as we believe that any analysis specific to a particular trader, identified uniquely, would be predicated on attempting to understand the behavior of this strategy. The distinction between benign analysis and "reverse engineering" is unclear, rendering the provisions of the Proposed Amendments difficult or impossible to enforce.

As a practical matter, Trader IDs used today may contain identifiers and mnemonics that are difficult to link to the underlying client. Indeed, some within the Committee are aware of a situation where a particular trader's identity was inadvertently disclosed to a researcher using a mnemonic in the Trader ID. However, even with identifiers obfuscated, the party originating orders may be irrelevant; the nature of the strategy may be apparent to a researcher, leading to the potential for a breach of intellectual property. Furthermore, third party researchers that are not securities market experts may not be aware of the nature or significance of the information, leading to further dissemination of sensitive data. This type of inadvertent disclosure is not avoidable without very close supervision of all recipients.

Additionally, third party researchers may be independent at the time of receipt of data, but subsequently become employed by market participants and marketplaces. Certainly in the case of marketplaces, a conflict is then created with regards to the amount of scrutiny associated with any request. Today's research partner in the academic sphere is tomorrow's capital markets expert tasked with maximizing the value of the intelligence obtained through access to sensitive data for further gain.

We offer the following analogue for contrast with the issue at hand. If a dealer were to offer client trading information to a third party for research purposes under a non-disclosure agreement, such practice would be seen as dangerously prone to abuse, and a breach of client confidentiality. However, the Proposed Amendments contemplate precisely the same arrangements, whereby marketplace participants (the clients of a marketplace) would have their service provider (the marketplace) disclose their trading to a third party (a capital markets researcher). Such arrangements offered by a dealer would be seen as universally unacceptable; why are marketplaces held to a lower standard of care over sensitive client information?

We also note that the Proposed Amendments refer to "capital markets research" without a satisfactory definition for what may constitute such research. We note that in some circumstances, marketplaces may be incented to engage a third party for the purpose of conducting "capital markets research" intended to further the marketplace's commercial goals (and only publish such research if the results are favourable). We do not believe that an exemption for proprietary data disclosure under such circumstances is appropriate, yet the Proposed Amendments leave open the possibility. At a minimum, the term "capital markets research" must be clearly defined.

Finally, Proposed Amendments section 5.10(b) indicate that marketplaces have the right to take enforcement action "in the marketplace's sole discretion" in the event of a data breach – either in disclosure, or misuse. We do not believe that all marketplaces are properly equipped or incented to enforce contracts related to the misuse of third party data, even though all marketplaces have access to sensitive data. Moreover, violations of the terms of the agreement would amount to a breach of contract and would not result in more serious legal consequences. Any remedy would, presumably, be owed to the marketplace, as party to the contract, rather than the parties harmed (marketplace participants whose data was misused).

Suggestions and Alternatives

We believe that provisions relating to sensitive marketplace data must include a requirement that the information provided should match the intention of the research, limiting the extent of sensitive data disclosed. Further, Trader IDs (commonly referred to as "STAMP IDs") should not be provided under any circumstances.

We believe that the Proposed Amendments should be revised to expressly prohibit that third parties receive data that would enable the recipient of this data to – directly or indirectly – identify the origin of any order. In practical terms this would primarily prohibit the disclosure of STAMP IDs. However, in certain situation, other fields (such as significant shareholder or insider trade markers) may be used in combination with public shareholder disclosures to identify the activities of large institutional investors. Such information may be extremely harmful to the parties affected. Therefore, all private data fields must be carefully evaluated for their potential of providing identifying information content.

Alternatively, if the provision of private data is to be granted, a marketplace should be required to make a formal request via the regulators to the industry on a case by case basis. The application process should include details of exactly who would receive the data, how it will be kept, the nature of the private data being disclosed, etc. As it stands, the Proposed Amendments do not impose a due diligence standard on marketplaces in evaluating the recipients of any private data. We believe it is inappropriate to offer a blanket exemption allowing any marketplace to disclose data to researchers simply on the claim that the researcher has bona-fide capital markets research purposes and no further motive.

Finally, we note that IIROC has developed infrastructure for granting access to certain data to researchers (who are screened and evaluated) under controlled circumstances. Given this investment, we believe it is appropriate to defer the management of third party research relationships to IIROC under a common framework.

Given IIROC's investment in research, we believe that the best alternative to banning the provision of non-public data to researchers is to centralize the management of such research at IIROC. Under this model, all data would remain housed within IIROC's systems; IIROC would serve as the sole source of (consolidated) market data for properly vetted research under carefully considered safeguards (such as obfuscated Trader IDs to the extent Trader IDs are deemed necessary at all), and with clear disclosure of the parties involved. This approach would resolve the conflict of interest inherent in marketplaces providing data to researchers, given the propensity to further the marketplace's own commercial goals, and the insufficient incentive or means to enforce any breach of non-disclosure contracts. Additionally, this approach would enable a recognized regulatory body – IIROC – to ensure that any sensitive data offered for research is not replicated away from IIROC's facilities, or is otherwise left open to future compromise.

We appreciate the opportunity to comment on this matter.

Respectfully,

"Signed by the CSTA Trading Issues Committee"

c.c. to:

OSC:
Ms. Susan Greenglass, Director, Market Regulation
Ms. Tracey Stern, Manager, Market Regulation
AMF:
M^{e} Anne-Marie Beaudoin, Secrétaire générale
BCSC:
Ms. Sandra Jakab, Director, Capital Markets Regulation
IIROC:
Ms. Susan Wolburgh Jenah, President and CEO
Ms. Wendy Rudd, SVP, Market Regulation & Policy
Mr. Victoria Pinnington, Vice President, Trading Review and Analysis
Ms. Deanna Dobrowsky, Vice President, Market Regulation Policy
Mr. Mike Prior, Vice President, Surveillance