INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÉRES

Marcel St-Amour
Directeur Régional
514 843-8950 / mstamour@iiac.ca

Barbara Amsden
Director, Special Projects
416 687-5488/bamsden@iiac.ca

August 23, 2011

Mr. Jean-Sébastien Desmeules
Directeur des affaires juridiques
575, rue St-Amable, Bureau 1.10
Québec (Québec) G1R 2G4
Tél : (418) 528-7741
Fax: (418) 529-3102
E-mail: cai.communications@cai.gouv.qc.ca

Ms. Chantal Bernier
Assistant Privacy Commissioner
Office of the Privacy Commissioner of Canada
112 Kent Street, Ottawa
Tel.: 613) 995-8210
Fax: (613) 947-6850
E-mail: chantal.bernier@priv.gc.ca

Dear Mr. Desmeules and Ms. Bernier:

Re: Privacy Questions re Proposed Amendments to TMX/The Bourse Rules 6 and 14

The Investment Industry Association of Canada (IIAC) is a member-based professional association with 180 members holding client assets of over 95% of Investment Industry Regulatory Organization of Canada (IIROC) registered organizations. IIROC is the national self-regulatory organization (SRO) that oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Our members are also subject to the oversight of provincial regulators including, in Quebec, the Autorité des Marchés Financiers (AMF). IIAC advances the growth and development of the Canadian investment industry, acting as a strong, proactive voice to represent the interests of our members and the investing public.

The Regulatory Division (the Division) of the Bourse de Montréal (the Bourse) has changed (pending certification or approval) their requirements for reporting on positions for derivative instruments and is now requiring the last four digits of social insurance numbers (SINs) to be provided (additional detail can be found in TMX/The Bourse Circular 109-2011, *Request for comments – Reports related to the accumulation of positions for derivative instruments – Amendments to articles 6654 and 14102* (the Circular), issued on June 16, 2011, pertaining to the Division's Large Open Position Reporting (LOPR) requirements). Those of our members that are Approved Participants (APs) of the Bourse will need to comply with the Division's amended rules.

We support the purpose of the amendments – that is, to better enable the Division to monitor for abusive market trading, which is in the public interest of a well-functioning derivatives market – but are not sure that the use of SIN is the most appropriate way to achieve the Division's objectives. We are attaching an excerpt from IIAC's submission to the Bourse on the rule

amendment and additional questions are provided below. As the effective date could be at any time on thirty days' notice, we hope that you will contact the Bourse directly if you have any concerns about the rule.

In light of the Division's request for such Personal Information as four digits of SINs, we reviewed the proposed changes in the context of Quebec's *An Act respecting the protection of personal information in the private sector*, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), Quebec's Charter of Human Rights and Freedoms, as well as other provincial privacy legislation and, in the case of SINs, the federal *Income Tax Act* (ITA). Our understanding is that, first and foremost, the SIN is a tax identifier. Although its use for identification purposes by private-sector organizations is not specifically prohibited by law, we understand that current privacy, securities and derivatives laws do not contemplate such use by investment dealers/APs or the Division. In order for APs to lawfully disclose client SINs to the Division for identification purposes, the APs need to have valid consent from their clients in compliance with provincial and federal privacy laws, with valid consent meaning that APs (i) explain the implications of such use/disclosure to their clients; (ii) obtain consent from clients; and (iii) allow clients to opt out of such use/disclosure.

We believe that the proposed rule amendments in the Circular may have a much broader implication than understood. This is because the amendments effectively require the use of the SIN as a linking identifier between not just accounts of the same individual in one financial institution, but also among that person's accounts and certain non-personal accounts at the institution, and then with such accounts of that individual at different financial institutions.

Based on our conversations, this is a much broader linkage than we believe has been examined and accepted by the CAI, the OPC and their counterparts in different provinces, in terms of the public interest or privacy principles. We therefore would appreciate understanding the CAI's, OPC's and their provincial privacy counterparts' views on the following:

- **Does the significant linking that will occur of an individual's financial involvements across multiple Canadian financial institutions introduce particular concerns?** In our view, the Division's required linking and aggregation of account information by financial institutions, and then subsequent aggregation of such data across financial institutions using SINs, could potentially be used as a precedent for other regulators to institute similar practices. This will mean that the Division, and any other regulators that adopt this practice, will be in possession of considerably more data on an individual's financial accounts, activities and connections than any of the federal or provincial government bodies or any one financial institution itself. Given the highly sensitive nature of financial information, our view is that this precedent should be considered carefully and that less privacy-intrusive methods of achieving the same objectives should be considered.

- **Does the CAI's and OPC's authority extend to the Division as a private entity or as a public body?** While the Division may not be a public or government body, it derives its regulatory authority from l'Autorité des Marchés Financiers (AMF), which is a public body according to the CAI website. We have accordingly asked the Division to request a review of this initiative by both CAI and OPC, including discussions surrounding whether there is a less privacy-intrusive way of achieving LOPR's ends; the appropriateness of the data

aggregation requested; and the need for information accuracy and a robust security environment.

A privacy impact assessment of this initiative is particularly important since investors are unlikely to be aware of, or understand, the Rule changes' impact on the collection, use and disclosure of their Personal Information, or to be able to comment on the proposed rules on their own behalf. Our members and, we think, their clients, would like to understand any differences from a privacy perspective, in terms of CAI or OPC oversight, that exist among information requests made by a regulator that is a government body, a regulator or self-regulator that is overseen by a government body and a regulator that is a private-sector entity. As well, if the Division is a government body or under government body authority, we would appreciate knowing if privacy impact assessments have been completed and, if so, whether they were satisfactory.

- **Do data protection measures that must be applied by a regulator differ from those applicable by private sector entities?** The Division's proposed reporting mechanism is more secure than the methods currently employed and out of necessity must be considerably more secure given the unprecedented requirement for more frequent and additional client Personal Information, notably the last four digits of the SIN. Given the sensitivity of the information being requested, we believe that a robust security assessment is required prior to sharing the requested information. Our concerns in this area have been heightened by discussions with Bourse IT representatives, which indicate that the reporting mechanism and overall security environment at the Bourse may not fully meet the information security standards of APs responsible for the majority of transactions on the Bourse.

  We have therefore requested that the Division enter into a mutually-agreed-upon confidentiality agreement, and provide limited access to the Bourse's technology policies and a copy of the Bourse's most recent CICA 5970/SAS 70 – a report on the Bourse's controls – which we have not yet received. This is standard procedure for our member APs when dealing with third parties that will have possession of client Personal Information, but there is additional flexibility to change these terms/requirements given the importance of the Division as regulator of derivatives markets. In support of our ongoing discussions with the Division, we would appreciate the views of the CAI on the appropriateness of the Bourse's security standards.

- **Where does liability fall when a regulator requires regulated entities to provide data and the privacy of that data is breached after leaving the possession of the private company?** Our understanding is that, if APs are compelled by the Division (acting under the delegated authority of the AMF) to provide this information, the APs will not be accountable for any subsequent use or disclosure of this information by the Division. We would appreciate the CAI's and OPC's confirmation that APs would not be considered liable or accountable in the event of an inadvertent breach or misuse of the Personal Information under the Division's control.

Attached is a relevant excerpt from our July 18, 2011 submission to the AMF and Division with additional background that may be of relevance. We would appreciate an opportunity to understand your views on the important issues described above and in the attached that are of concern to our members. We hope to follow up with you in the near future with respect to our

questions so that we may help address the Division's valid regulatory concerns and our members' desire to protect their clients' privacy.

Yours sincerely,

Marcel St. Amour Barbara Amsden

Cc: Crizia Lippi (Crizia.Lippi@priv.gc.ca)
Robin Gould-Soil (Robin.Gould-Soil@priv.gc.ca)

Attachment

Excerpt from July 18, 2011 Letter to the Division and AMF

Background on IIAC Views on Proposed Amendments to TMX/The Bourse Rules 6 and 14

…

1. Confirmation that changes meet privacy principles

The Bourse has requested that firms provide additional account owner information, including a portion of clients' social insurance number (SIN) and account number. As, while the Bourse is located in Quebec, options and futures clients live across (and outside of) the country, we have considered the relevance of, as well discussed with and written to the Division regarding, the Division's request for such Personal Information in light of Quebec's *An Act respecting the protection of personal information in the private sector* (Quebec Privacy Legislation), the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as provincial privacy legislation in Alberta and B.C., and, in the case of SINs, the federal *Income Tax Act* (ITA). Quebec privacy legislation defines personal information as "information concerning a natural person which allows the person to be identified…" We believe that we are in agreement with the Division that providing Personal Information such as a client's SIN or other individual number is information about a now identifiable individual that does not fit into one of the exemptions to the prohibition on releasing such information without a person's knowledge or informed consent in section 18 of the Quebec Privacy Legislation or in subsection 7(3) of PIPEDA.

In considering whether the wording of the Rule, which provides for the Bourse to require the last four digits of a SIN and account number, is appropriate, our attention was drawn to 2004 Office of the Privacy Commissioner of Canada (OPC) guidance on the subject, as well as to a ruling from the website of the OPC's counterpart, the Commission d'accès à l'information (CAI) (http://www.cai.gouv.qc.ca/index-en.html). It establishes that, while using SINs for other than authorized purposes is not *prohibited*, using a SIN, or indeed a part of a SIN, to link individuals is not *condoned* by the OPC. The Bourse's requirement therefore puts APs in an awkward position without guidance from privacy regulators, as we believe that the OPC's view applies whether the entity holding or receiving the Personal Information is a public or a private-sector entity.

In the case of public sector demands for Personal Information, it is a question of 'necessity' for federal entities, and there is a similar test used under Quebec Privacy Legislation and Quebec's Charter of Human Rights and Freedoms. The federal privacy commissioner uses four questions to assess 'necessity' (http://www.priv.gc.ca/information/pub/gd_exp_201103_e.cfm#toc2a), and our view as to whether the proposed Rule changes meet these tests in the case of Personal Information and of the SIN, in particular, is provided after each question below:

1. ***Is the measure demonstrably necessary to meet a specific need?*** While there is a need to prevent and address potentially manipulative market behaviour, and we were advised that there is no evidence that there has been abusive activity, we accept that some form of

LOPR reporting and monitoring is required in the current market environment. However, as discussed below, we do not believe that there has been a demonstration that four digits of a SIN are required for this reporting.

2. ***Is it likely to be effective in meeting that need?*** Partially. We believe that the use of SIN in aggregating information for LOPR will be only somewhat effective, as we suspect that abusive activity, should it arise, is likely to be enacted by sophisticated parties across multiple affiliates, names and identifying numbers. Operational concerns raised and the inability to cross-reference some client relationships will also limit the effectiveness of the initiative.

3. ***Is the loss of privacy proportional to the need?*** We do not think so. As noted above, we are not convinced that SINs will be effective in identifying potential abuse; we also have the following concerns regarding the proportionality of some of the possible outcomes on individuals' right to privacy.

   i. A LOPR submission time of 8:00 a.m. ET (5:00 a.m. PT) on the day following the trade (T+1) means the many firms using overnight batch processing for transactions and/or client name/address updates will, if an 8:00 a.m. ET time can be met at all, submit unreconciled data (with 'unreconciled' meaning transaction cancellations and corrections of inaccurate amounts and account numbers will not have been completed). This will result in the possible reporting of accounts that do not actually meet the reporting thresholds, leading to these accounts' holders' having their privacy breached by unnecessary reporting.

   ii. As holdings from joint accounts will be linked with holdings from individual accounts, there is a possibility that this linking could lead to inappropriate disclosure to one of the holders about the other's individual account (the LOPR requirements demand that holdings of an individual be linked with his or her holdings in a registered corporation or corporation owned exclusively by the individual, as well as those accounts in which he or she has a greater than 50% share (e.g., joint account, partnerships, investment clubs, registered entities other than corporations and corporations that are not 100% owned)).

   Another feature of the LOPR system – defaulting to a "speculator" designation when information is not available or cannot be known (e.g., when a retail client may use some option transactions to hedge and others to speculate), runs counter to the need for accuracy – one of the ten universal privacy and fair information practice principles of the Canadian Standards Association discussed in more detail below. We are persuaded that alternatives suggested in (4) below will make the risk of privacy loss more proportionate to the regulatory need without materially reducing the effectiveness of the reporting.

4. ***Is there a less privacy-invasive way of achieving the same end?*** Yes. As the Circular notes that alternatives have not been considered, we suggest the following ways that we believe will help mitigate privacy concerns. For example, the Bourse could:

   - Require aggregation by name and address including postal code, and then ask for additional information when needed as has been done for a number of years (there are

840,000 postal codes in Canada, which suggest 40 or so Canadians per postal code, and a relatively small number of possible aggregation questions for the Bourse);

- Allow reports to be filed after review and correction of errors (e.g., by close of business rather than at 8:00 a.m. ET (5:00 a.m. in B.C.) on T+1;

- Consider aggregation at the trading-agent rather than beneficial-owner level as we understand is done in the U.S., with follow-up contacts (as by the Division's U.S. counterpart) to the AP if there are questions regarding holdings, activity or clients.

In the case of private sector demands for Personal Information, requesting and using Personal Information is a question of receiving informed consent from the individual, which usually is obtained through the account-opening agreement with the client in the case of APs. The wording of account-opening agreements, which the Bourse reviewed as part of its due diligence, provides for information to be provided to regulators. When the account-opening documentation the Bourse reviewed was drafted, it was, among other things, to be consistent with a December 3, 2003 Joint Regulatory Notice on Federal and Provincial Privacy Legislation, to which the Bourse was party and which states that "Regulated Persons have obligations to produce or make available for inspection documents and information to SROs, *from time to time*, for regulatory purposes." (emphasis added).

Consistent with this apparent regulatory reference to infrequent and situation-specific delivery of Personal Information for regulatory purposes, we believe that clients expect their information to be transmitted on a periodic basis only in the case of, for example, audits, enforcement efforts or complaint resolution, rather than on a regular daily basis. We think that a client would be surprised to learn that values of his or her personal and non-personal accounts would be aggregated with values of third-party holders in an account majority-owned by the client, and then provided to regulators, possibly to be combined across financial intitutions, and when the APs that collected information from the client have concerns from an information security perspective.

The following are our specific areas of concern with our recommendations to address each. While some are beyond the wording of the Rule amendments, which remove specifics of the Personal Information to be transmitted and leave it to be prescribed, we believe that they each require resolution before the amendments to the Rules and/or the LOPR requirements are fully implemented.

- ***Privacy and account aggregation:*** The Bourse is effectively requiring the use of the SIN to link different types of holdings of individuals at an enterprise level (and with the stated intent of aggregating across APs) where personal and non-personal accounts are rarely if ever linked in the same relational database and, if so, not for regulatory purposes. If one regulator may require use of the SIN, including reporting of the last four digits for administrative purposes in fulfilling a regulatory mandate, it would be a precedent for other regulators also requiring this for administrative purposes of regulation. If the precedent were used by securities regulators and then be used as a precedent more broadly, it would affect significantly more people than meeting Bourse requirements alone. An OPC publication, *Expectations: A Guide for Submitting*

Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada, emphasizes the importance of the right to privacy, saying:

> "The risks of certain government programs and initiatives should be measured and assessed in the context of their potential impact on our democratic society, our civil liberties, and our fundamental human right to privacy as recognized in Canadian law, including the *Privacy Act*, the *Canadian Charter of Rights and Freedoms*, and the case law interpreting them. The *Privacy Act* sets out fundamental rights of Canadians in their interactions with the federal state. The Supreme Court of Canada has recognized on numerous occasions that privacy interests are worthy of protection under the *Charter* and has further stated that the *Privacy Act* has quasi-constitutional status."

Quebec's Charter of Human Rights and Freedoms similarly provides for "Every person to have a right to respect for his private life", including in terms of relationships with government bodies and, we believe, the organizations that derive their authority from these entities.

- ***Accuracy:*** Quebec Privacy Legislation requires "*any file held on another person [to be] up to date and accurate when used to make a decision in relation to the person concerned*". The federal *Privacy Act* requires all government institutions subject to that legislation to take "all reasonable steps to ensure that personal information is as accurate, up-to-date and complete as possible". In some cases involving LOPR, accurate information cannot be provided, notably, in creating a requirement where unreconciled/ unaudited/uncorrected information will have to be provided to meet the 8:00 a.m. ET on T+1 deadline with the possibility of reporting client Personal Information where it is not required by the Rule, but as a result of operational issues (and the LOPR mechanism has no correction mechanism for later in the day). As well, and as noted above, the LOPR mechanism requires the AP to default to Speculator when information is not known or varies from transaction to transaction.

- ***Inability to provide:*** Reporting to be required under the Rules mandates four digits of a SIN, however, an AP has no legal requirement to, and therefore should not, collect the individual's SIN if a customer's account were not of a type that earns interest or there were not some other legitimate reason to obtain it. As well, there is no obligation for the individual to supply it. Even where the SIN is to be used for tax reporting purposes, an AP must provide clients with a convenient mechanism to withdraw consent to SIN use other than for tax purposes [e.g., regulatory reporting]. In either case, the AP will not be able to report the last four digits of the SIN.

Recommendation 1*:* Please confirm that the Division's privacy-related need meets the expectations of the CAI and OPC and that these provisions are all completely in place at the Bourse before implementation of LOPR.

Recommendation 2: Please expand consultation on privacy and aggregation matters, which we believe is a matter of public interest. The change from ad hoc use of a small sample of information by a regulator to significantly more and more frequent aggregated information merits, we believe, more extensive discussion among privacy commissions, and possibly

broader public consultation specifically on the use of SINs and other matters, which would not have been easily evident to an uninformed person reviewing the Circular.

Recommendation 3: Please ensure that "Not available (N/A)" is an option in the reporting for the Speculator/Hedger field and implementation of the Rule amendments should not proceed, or the field should not be mandatory, until this is addressed.

Recommendation 4: Please confirm that the prescribed reporting form and requirements will formally recognize that the last four digits of the SIN (or equivalent Personal Information) may not be provided for valid reasons.

2. Data protection confirmation required

Were a CAI privacy impact assessment done and/or an assessment under the federal Directive on Privacy Impact Assessment completed for LOPR Requirements, we believe that they would reveal the majority of risk areas identified would be material, or levels 3 or 4 of 4 levels in the case of the federal assessment, meaning the more likely it is that specific risk areas will need to be addressed in a more comprehensive manner, particularly in terms of data protection. Consistent with this, and in the absence of a signed confidentiality agreement with the Bourse that respects the Bourse's regulatory mandate and responsibilities as market regulator, we had requested and have not yet received limited access to Bourse information security policies or results of the Bourse's CICA 5970/SAS 70 audit of its internal controls to help ensure the ongoing privacy of Personal Information. We have been provided with the TMX Group Inc. Employee Code of Conduct, which is very thorough, however, our members believe that privacy legislation requires them to make every reasonable effort to ensure that collection, storage and destruction of Personal Information occurs to a very high standard. As recent cases attest, at least the OPC's findings generally are that the party that originally collected the Personal Information remains ultimately liable for its protection when under the auspices of others.

Recommendation 5: Please confirm that:

1. Bourse/Division privacy-related information security protection measures – both systems and procedures – meet the expectations of the CAI and OPC from a data protection perspective given the heightened sensitivity of the increased Personal Information that the Bourse will receive and store; and

2. These provisions are all completely in place at the Bourse/Division before implementation of LOPR.

Also, we would also appreciate confirmation of the Bourse's/Division's liability if there were to be an inadvertent privacy breach while the Personal Information is within the Bourse's/Division control.

3. Conditional acceptance only of removing reporting provisions from Rule

- ***Consultation:*** The draft rule amendments, which remove detail of the Personal Information required up until now, would not provide for automatic formal discussion of any future changes in the reporting fields required for LOPR reporting, notably requests for additional Personal Information. The Division has advised that changes in prescribed reporting is a matter the Division will discuss with the Autorité des marchés financiers (AMF) and then determine if any change may be problematic, in which case consultation would be undertaken. We believe that it may not always be evident when a change will be problematic, whether from a legal standpoint (e.g., original proposal to use the full SIN) or technical perspective (e.g., the LOPR vehicle was designed for a two-digit country code whereas the industry mailing address standard, for the data used for LOPR, is three characters).

  Recommendation 6*:* Please add provision for before-the-fact (at the start of a project that may require systems changes) meaningful consultation, or at least a 30-day comment period requirement, to the Rule amendments or as a written, publicly available general policy. We believe that this would, at worst, delay process improvements by 30 days (trivial to the extent that we believe the Bourse has powers to address any immediate risks), while at best save regulators, APs and their service providers missteps and expense. Such consultation is also consistent with the *Governance Statement of the Autorité des marchés financiers* (http://www.lautorite.qc.ca/files/pdf/a-propos-autorite/codes-ethique-gouvernance/enonce-gouvern-an.pdf), including the organizational value of active listening to stakeholders and the governance principle of openness, which, we presume, would both apply equally to the self-regulatory organizations, such as the Division, that the AMF oversees.

- ***Transparency:*** Given the sensitivity of AP client Personal Information requested, we believe, as said in our May 5th meeting with the Bourse on confidentiality issues, that it is important that there be a Rule requiring the information to be provided; that the process leading to the new requirements be public and clear; and that information on the Personal Information to be required by APs be widely obtainable through the Bourse's website. If the required information on the form is to be "prescribed", it must be made clear what the evidence of "prescription" is – the circular with attached data points. It is important for our members' and their clients' purposes that there to be an explicit link or connection between the Rule and what is prescribed – including reference to the requirement for the last four digits of the SIN.

  Recommendation 7: We suggest that the Bourse and Division websites transparently hyperlink the Rule to the instrument prescribed under the Rule and that the Division provide a website-accessible plain-language version of the prescribed reporting under the Rule for investors explaining what the Personal Information requirements under LOPR are, why the Division is requiring the data to be collected, used and disclosed, and how it is being stored, shared and disposed of once at the Division.

… [letter continues; full copy available at :
http://www.iiac.ca/system/resources/3948/original/IIAC%20Letter%20to%20the%20Bourse%20and%20AMF%20on%20Draft%20Large%20Open%20Position%20Reporting%20(LOPR)%20Rule%20Amendments-%20July%2018%202011.pdf?1311342196]