VIA EMAIL

October 29, 2025

Mr. David Fountain
Chief Information Officer
Canadian Securities Administrators
20 Queen St. W.
Toronto, Ontario
M5H 3S8

Dear Mr. Fountain:

Re: Canadian Securities Administrators' data privacy policies

We are reaching out to you regarding the recent Canadian Investment Regulatory Organization (**CIRO**) cybersecurity incident. This incident raised broader concerns regarding the Canadian Securities Administrators' (**CSA**) data collection and retention policies, and the sharing of information among members of the CSA and with CIRO.

We understand that the CSA are monitoring the handling of the cyber breach as part of their oversight of CIRO, and expect you are in the process of conducting a full-scale review of the CSA's data protection risks to avoid a future security breach of the National Registration Database (**NRD**) or other CSA member systems.

The intent of this letter is to highlight some of the key privacy concerns the CIRO cyber breach raised and to recommend, as part of your review, some areas of prioritization for the CSA.

CIRO incident

We initially spoke to you about this incident on September 10 and you referred us to CIRO staff. We spoke with CIRO staff (Jennifer Armstrong, GC and Corporate Secretary and Elsa Renzella, SVP Compliance and Registration) on September 17, and they were very helpful in responding to our questions. We appreciate the work that CIRO has been doing to respond to this incident, and its prompt communication with members and industry representatives, including PMAC. The FAQ on the CIRO

website is very helpful, and we note that it has been updated to respond to additional questions. CIRO staff informed us that they have been in regular contact with your team at the CSA regarding the breach and CIRO's response plan.

Information sharing

When we spoke with CIRO Staff, they informed us that the CSA provides CIRO with access to the NRD, and that CIRO receives a daily download of information from NRD regarding individuals registered with CIRO or a CIRO-related entity (MFDA, IIROC, IDA). This includes previous registrants; it seems that CIRO has records going back several decades.

In response to our questions about the information that is shared with CIRO from the NRD system, we were told that CIRO receives only historical information related to CIRO registration, and that current NRD information (for individuals who are currently only registered with a CSA-registered entity) is not included.

Our concerns

This incident raised broader concerns about the CSA's data collection and retention policies for NRD and other systems, and with the sharing of this information among CSA jurisdictions and with CIRO. We are particularly concerned about personal information that may pose more identity fraud risk and that may not be needed for regulatory purposes, beyond a certain length of time. We understand that CIRO is conducting an evaluation of its data collection polices and expect that the CSA and CSA member jurisdictions are also conducting a review of their policies. We have outlined below some suggested areas for possible examination.

1. **Types of personal data collected**

Consideration should be given as to whether all of the personal information collected in Form 33-109F4 is necessary for regulatory purposes, such as individuals' personal attributes (height, weight, hair colour, etc.), passport number, immigration information and other personal information as defined by applicable privacy legislation.

2. **Purpose of collection and use**

We recommend that the CSA and member jurisdictions' policies on data collection state the purpose of the data being collected and how it is relevant to the CSA and relevant jurisdictions' mandates. Unless this information serves a specific regulatory purpose, we would recommend that it not be collected.

3. Data retention and destruction

If it is determined that the personal information is required, we recommend limiting the length of time the information is maintained in NRD and other systems, with consideration of a maximum 7-10 year retention period. We were informed by CIRO staff that some CSA members keep records for many decades. This seems excessive, especially where the individuals are no longer employed in the securities industry.

The CSA and member jurisdictions' policy reviews could include a consideration of whether certain information collected from registrants during the registration process can be destroyed after a period of time, even while they remain registered. We also recommend improved transparency with respect to record retention policies.

4. Data sharing and transfers

a. Sharing information with CIRO

Many of our individual members who were previously registered with a CIRO entity were not aware that their historical registration information was being provided to CIRO. Any instances of data-sharing with third parties, including the security measures for such transfers, would be important information to share with registrants.

We do not believe that CIRO has a regulatory need for data related to individuals who are no longer registered with a CIRO-registered firm. We ask that the CSA discontinue sharing this information and that CIRO delete the information from its systems.

b. Sharing information across CSA jurisdictions

We are also concerned about similar sharing of information between CSA jurisdictions on NRD. For example, if an individual is registered in only one CSA jurisdiction, is their information being shared across the CSA, and is there a regulatory need for this sharing of information?

c. Sharing information with staff

Moreover, we are not aware of the current policy with respect to sharing information with CSA and CIRO staff. We are concerned that individual employees within the CSA and CIRO may have access to information that is not relevant to their specific functions.

Granting employees access to individuals' personal information carries inherent risks, including the potential for misuse or unauthorized disclosure.[1] To mitigate these risks, best practice would be to strictly limit access to roles and functions where it is essential for the performance of job responsibilities. Additionally, access should be subject to appropriate oversight, including supervision and monitoring mechanisms, to detect and prevent any potential abuse or violation of data protection policies.

5. Other information

While this letter has focused on the personal information of individual registrants, we understand that firm and client information was also compromised during the CIRO incident. If firm and client information is also being collected and retained by CSA members, we recommend that a review of data security and retention policies also be conducted with respect to this information.

6. Communication and next steps

This data breach has caused considerable concern amongst the industry. It would be helpful for the CSA to provide a notification (via NRD, for example) regarding any precautions individuals should be taking to protect their personal information, and what steps the CSA is taking on their behalf.

In terms of next steps, it is our firm belief that any plans to delegate further responsibilities to CIRO with respect to the registration function must be paused and reconsidered at this stage to allow the CSA and CIRO to complete their review of this breach, to implement necessary changes, and to focus on their core regulatory responsibilities.

We trust that these concerns will be addressed in your review and that the CSA and CIRO will take this opportunity to modernize their data collection, retention and sharing policies. We also expect that the CSA and CIRO will provide additional transparency, which we believe is essential to re-building the trust that has been impacted by this unfortunate incident.

[1] See Posadzki and Haws, *RBC employee accused of accessing Carney's bank profile in alleged wider scheme*, Globe & Mail, September 25, 2025

We would be pleased to discuss the foregoing with you and to lend our support to your work.

Yours truly,

PORTFOLIO MANAGEMENT ASSOCIATION OF CANADA

"*Katie Walmsley*"

Katie Walmsley, President

cc. Jennifer Armstrong, *General Counsel and Corporate Secretary, Canadian Investment Regulatory Organization*

Stan Magidson, *Chair, Canadian Securities Administrators, Chair and Chief Executive Officer, Alberta Securities Commission*

David Cheop, *Vice-Chair, Canadian Securities Administrators, Chair and Chief Executive Officer, Manitoba Securities Commission*