AIMA Canada
56 Temperance Street,
7th Floor,
Toronto, ON,
M5H 3V5
+1 416 364 8420
canada@aima.org

To: Canadian Investment Regulatory Organization
(CIRO) and Canadian Securities Administrators (CSA)

February 5, 2026

Re: Request for Enhanced Data-Retention and Data-Governance Requirements in Light of Emerging Cybersecurity Risks

Dear CIRO and CSA,

AIMA[1] is writing in response to the recent CIRO cybersecurity breach in August 2025. We were concerned to hear from registrants – both currently and previously registered - that their data had been both compromised and retained for lengthy periods of time, raising questions around the appropriate collection, purpose, use and retention of data, as well as the need for sufficient infrastructure to house it securely.

AIMA appreciates the work of CIRO and CSA to strengthen the resilience of Canada's capital markets, particularly in the face of escalating cybersecurity threats. As regulatory agencies globally confront the operational, privacy, and systemic risks associated with large stores of digital information, retention policies have emerged as a critical—yet often under-specified—component of supervisory cybersecurity frameworks. In this context, we respectfully urge you to adopt clearer and more risk-sensitive rules governing the retention, storage, accessibility, and eventual disposal of regulatory data, with a particular emphasis on personally identifiable information (PII) and other sensitive records.

It is our understanding that since the National Registration Database (NRD) was created in the early 2000s, and its data is replicated across multiple systems, including CIRO, with legacy fields and storage formats that are not always encrypted. This results in large-scale duplication of highly sensitive personal information being held in legacy storage and archival environments that may not meet modern encryption and data segmentation standards. Our understanding is that NRD contains information relating to registrants' full personal profiles—including height, weight, hair and eye colour, past residences, and extensive employment and financial records—which information is retained for up to ten years or more, with no clear purpose limitation, even for individuals who have long ceased to be registrants. By contrast, global regulators, including the SEC, generally require retention of five

[1] The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than US$3 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programs and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 250 members that manage over US$1 trillion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialized educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For more information, visit www.aima.org

to seven years, tied directly to supervisory need, and FINRA applies similar principles for retail brokers.

International practice is converging around two themes: regulators generally require finite, purpose-bound retention periods, and PII is subject to heightened protection. IOSCO's Information Collection and Record Retention Compendium notes that most securities supervisors require records to be held for three to six years, with the first two years "easily accessible." IOSCO's own Personal Data Protection Policy provides a more specific benchmark for PII: it should be retained only for as long as necessary for the purpose collected, then blocked or deleted, with an outer horizon not exceeding six years. Similar purpose-limited retention rules apply at ESMA and the FCA, while the SEC requires brokers to preserve key records for at least six years, with two readily accessible. The direction of travel is clear: regulators are reducing unnecessary data accumulation, clarifying retention horizons, and differentiating standard supervisory data from higher-risk personal data.

This international trajectory reflects the growing reality that cybersecurity threats magnify the consequences of extended data retention. Large, long-term data repositories create attractive high-value targets for malicious actors. Sensitive information—PII, client identifiers, beneficial-owner data, transaction logs with personal details, employment or disciplinary records—carries disproportionately higher privacy, fraud, and financial-crime risks. Without clear deletion timelines and tiered retention rules, data may be retained longer than necessary, increasing exposure and complicating cross-border privacy expectations. Regulators such as the FCA have responded by adopting data-classification frameworks and retaining PII only for short, purpose-bound periods (such as last contact plus three years) unless needed for enforcement.

The current Canadian approach—effectively keeping 25 years of information in some cases—raises clear cybersecurity, privacy, and governance concerns, magnified by the sheer volume of information collected through NRD, NRD pin resets, and other related filings. When regulators accumulate such large stores of registrant data, they must also review, protect, and govern it, which paradoxically slows regulatory processes and heightens the magnitude of any cyber incident or negligence. More is not better; modern retention rules must reflect purpose, necessity, and risk, consistent with Canada's own privacy law principles and the direction of travel internationally.

AIMA encourages you to consider modernizing its record retention regime built around clear data classification, tiered retention periods, and rigorous governance. Standard supervisory data could follow a finite horizon consistent with global practice—such as five or seven years—while sensitive personal categories would be subject to shorter retention unless there is an active enforcement rationale. Data required to be "easily accessible" would remain so only for an initial period (typically two years), after which it would move into secure archival storage with stricter access controls. To reduce long-term cyber exposure while preserving supervisory value, CIRO could also allow or require anonymization or de-identification once the relevant legal horizon has passed. Clear protocols for access controls, encryption, multi-factor logins, audit logging, and cross-border data handling—consistent with IOSCO confidentiality principles—would further strengthen the framework.

Codifying a modern, risk-sensitive retention framework would bring Canada into closer alignment with international regulatory practice, materially reduce cybersecurity vulnerabilities, and provide clearer, more consistent compliance expectations for registrants. AIMA and its members would welcome the opportunity to discuss potential retention models, implementation details, and opportunities for harmonization with global regimes.

Thank you for considering these recommendations. We look forward to continued engagement with CIRO and the CSA on this important topic.

Sincerely,
AIMA (Alternative Investment Management Association) Canada