



November 1, 2023

Office of the Superintendent of Financial Institutions
255 Albert Street
12th Floor
Ottawa, Ontario
K1A 0H
Via pensions@osfi-bsif.gc.ca

To Whom It May Concern:

RE: OSFI Technology and Cyber Security Incident Reporting for Pensions

ACPM is the leading advocacy organization for a balanced, effective and sustainable retirement income system in Canada. Our private and public sector retirement plan sponsors and administrators manage retirement plans for millions of plan members, including both active plan members and retirees.

On June 30, 2023, OSFI issued a draft version of an advisory titled Technology and Cyber Security Incident Reporting (Pension Advisory) and its accompanying form (Incident Report). We agree that cyber risks are a key issue facing organizations generally, including pension plans, and OSFI should be aware of material incidents. However, we are concerned that the reporting for federally registered pension plans (FRPPs) is overly broad, would introduce inappropriate or duplicate reporting of incidents and would deplete resources at a critical time.

Principles

The Pension Advisory appears to originate from the Technology and Cyber Security Incident Reporting advisory for Federally Regulated Financial Institutions (FRFIs) published in August 2021 (FRFI Advisory). While the content has been revised somewhat, we believe further changes are necessary to reflect the differences in the technology and cyber risks faced by FRFIs and FRPPs. Whereas FRFI systems are a critical cog in the functioning of the Canadian economy, responsible for market infrastructure and liquidity across the country, for FRPPs, the primary technology and cyber related risks are much narrower, focused on plan beneficiaries and the pension fund itself, with limited knock-on impacts.

- **Plan beneficiaries:** For most FRPPs, the administrator of the plan is also the employer. For these FRPPs, the technology and cyber risks are similar to the risks that employers face in storing and transmitting employee data. As these employers are federally regulated organizations, subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), there already exists an established structure for reporting these types of incidents.

- **Pension fund:** As noted in the Pension Advisory, some risks pertain to the pension investments or operations, which may not be subject to PIPEDA. However, since pension plans generally work with and rely upon the services of FRFIs, the majority of these activities, such as pension payments from the plan, financial market settlements, or asset custody services, are already subject to OSFI FRFI reporting requirements.

For OSFI's reporting requirements to be efficient and effective, the Pension Advisory should strive to meet three objectives:

1. **Minimize duplication** – Where possible, existing structures should be leveraged. For example, OSFI could be alerted to a breach that meets the PIPEDA criteria and affects pensions. As well, all organizations must have cyber security protocols. Given that federally regulated industries include banking, transportation and crown corporations, many of these protocols are very rigorous. While technology and cyber risks are important to pension plans, there is nothing compelling or unique in the risks they face relative to the employers who sponsor the FRPP. OSFI should encourage employers to extend their cyber risk strategies to FRPPs, including appropriate documentation in the FRPP governance framework, rather than imposing an independent set of criteria.
2. **Remain within OSFI's jurisdiction** – Whereas FRFIs are under OSFI regulation, employers that administer FRPPs are only under OSFI jurisdiction when carrying out their pension administration responsibilities; their activities as employers are outside OSFI jurisdiction.
3. **Be material** – PIPEDA's notification provisions are triggered if a breach creates a real risk of significant harm. Relevant factors include the sensitivity of the information involved and the probability of it being misused. We recommend a similar threshold be applied for any OSFI reporting.

Criteria for reporting

In addition to defining a threshold, we have the following comments on the criteria laid out:

- Unlike FRFIs which are often linked and subject to contagion risks, technology or cyber risks that impact FRPPs will rarely have consequences for other FRPPs or the broader Canadian financial system. Arguably any contagion effects would take place at the level of an FRFI or other party providing a service to an FRPP – such as pension payment processing or financial market settlements;
- Impacts on employer operations, infrastructure, data, or systems are outside of OSFI jurisdiction. These incidents should only be reportable if they affect the operation of FRPPs;
- While having a resiliency plan for a FRPP is a good practice, such plans are typically embedded within the organizational resiliency plan; for example, every organization's resiliency plan was triggered during the pandemic and pension operations continued largely unscathed;
- The criteria of "A negative affect on the reputation of the plan administrator, employer or participating employers, and service providers is looming" is much too vague and in some cases may contravene securities legislation, without public disclosure;

- The reference to an incident that “has been reported to the Board of Directors, Senior/Executive Management, or the Board of Trustees” might serve to discourage prudent internal reporting;
- The inclusion of incidents that are reported to the Office of the Privacy Commissioner, another federal government department and other supervisory or regulatory organizations or agencies raises the concern of duplicative reporting, as noted above;
- The reference to “internal or external counsel” as a criteria for reporting is inappropriate. Rather, FRPPs should be encouraged to seek counsel for guidance without any reservation; and
- We agree that where plan members and beneficiaries have been widely notified of an incident, and the incident has not already been resolved, advising OSFI would be prudent. However, for breeches involving individuals or small groups which have been resolved under the PIPEDA framework, reporting seems unnecessary.

Notification requirements

The Pension Advisory requires an Incident Report be sent to OSFI within 24 hours to a general email box, provide regular updates and a post-incident review, including lessons learned.

We are concerned that the proposed real-time reporting framework will result in a diversion of resources away from incident management, and the creation of additional risk through the sharing of sensitive information. The resourcing and coordination associated with such reporting may be particularly burdensome for smaller plans.

Plan administrators, in their fiduciary capacity, are already accountable to have appropriate governance, risk management and data management frameworks that encompass the risks associated with information technology and the management of confidential or personal data and information, including where this is subject to delegation or service agreements with third parties.

Also, it does not address the provision of sensitive information to OSFI that is outside the scope of its regulatory authority, such as where the IT risk incident is not limited to the pension plan and its members, but also involves organizational information security and management. Some of the indicators listed are beyond the scope of the *Pension Benefits Standards Act (Canada)* (PBSA) and may not result in any actual impact to plan members.

The lack of confidentiality regarding the information OSFI is requesting (such as through a disclosure request under the PBSA, *Access to Information Act (Canada)* or *Privacy Act (Canada)*) could result in an inappropriate release of information about the cause, nature and status of incidents that is inconsistent with a pension plan administrator’s risk management governance and practices.

The proposed email transmission of sensitive information to a central OSFI email inbox is arguably inconsistent with prudent risk management practices.

Examples of Reportable incidents

Pension portals are not required under PBSA; therefore, unless payments to members or the confidentiality or integrity of information are affected, an incident affecting a pension portal should not be reportable. In addition, employer servers are (to the extent unrelated to the operation of the FRPP) outside the scope of the PBSA.

A material technology or cyber breach of a third party that affects pension data or the pension fund would generally be reportable by that third party, through PIPEDA or existing reporting requirements of FRFIs. In fact, the third party might provide the FRPP administrator with only limited details respecting a data breach.

An employer receiving an extortion message is outside the scope of the PBSA, unless the FRPP itself is implicated.

The examples of reportable incidents should be clarified, and the scope limited to only technology or cyber incidents affecting the servers of a pension plan administrator or a third party provider that are likely to materially impact pension payments or the confidentiality or integrity of information and are not otherwise reportable by a FRFI or under PIPEDA.

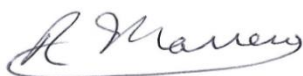
Incident Report Form

We suggest eliminating the Incident Report and instead determine principles where an FRPP should report a technology and cyber incident to OSFI:

- Ensure the FRPP has appropriate technology and cyber incident resiliency plans via documentation in the governance frameworks. In the rare case of a stand alone FRPP (separate legal entity from the plan sponsor), OSFI could take further action to audit the resiliency plan;
- Copy to OSFI when an incident involving the pension plan is reportable under PIPEDA subject to OSFI being able to receive personal information transmitted in an appropriate manner;
- FRPP to advise OSFI of an incident widely reported to pension plan members that has not been resolved in a timely manner; and
- OSFI to review FRFI reporting requirements to ensure FRPP issues are adequately addressed – for example a breach of custody and payment systems affecting pension beneficiaries.

We appreciate the consideration and are available if any further assistance is required.

Sincerely,



Ric Marrero
Chief Executive Officer
ACPM