

SEPTEMBER 2022

Information Security Incident Reporting

Consultation Summary Report

Contents

Introduction	1
Background	1
Consultation Process Overview	2
Summary of Feedback	2
Table 1: Key Themes from Feedback	3
Summary of Consultation Outcomes and Next Steps	6



Production of this document included environmentally friendly best practices.
Please reduce, reuse, and recycle.

Introduction

In January 2022, BC Financial Services Authority (“BCFSA”) released a discussion paper seeking feedback from stakeholders on the policy issues related to BCFSA developing an Information Security Incident Reporting Rule. A 45-day consultation period followed this release.

This report summarizes the consultation feedback received from stakeholders and includes BCFSA’s responses and next steps. Several key themes emerged in the feedback from stakeholders, including:

1. Need for a Rule;
2. Need to harmonize with other regulators;
3. Reporting timelines;
4. Protecting sensitive information; and
5. Responding to incident reports.

Stakeholder feedback is an essential element to developing appropriate and effective regulatory policy and BCFSA thanks everyone who submitted comments in response to the discussion paper.

Background

In October 2021, BCFSA released its Information Security (“IS”) Guideline, which outlines principles for the effective management of IS risks. BCFSA’s strategic imperatives include safety, soundness, and consumer protection. The IS Guideline establishes both prudential and market conduct expectations to ensure that regulated entities are prepared to meet shifting risk drivers and that customers are treated fairly, in accordance with market conduct standards.

The IS Guideline established expectations for provincially regulated financial institutions (“PRFIs”) which include B.C. incorporated financial institutions and pension plans but excludes extraprovincially or federally incorporated financial institutions or pension plans (“extrapros”). BCFSA opted not to include extrapros in scope for the IS Guideline to avoid creating expectations for the management of IS risks that may conflict with those established by the extrapro’s primary regulator.

Consultation Process Overview

The January 2022 discussion paper on Information Security Incident Reporting Rule outlined the objectives and scope of a potential rule, possible triggers to report an IS incident to BCFSa, and the potential range of the reporting requirements.

The consultation was open for public comment for 45 days (January 10 to February 25, 2022). To support informed participation and raise awareness of the consultation, BCFSa shared information and resources with stakeholders and responded to questions throughout the consultation period. Additionally, credit unions, insurance companies, and trust companies were asked to provide BCFSa with both verbal and written comments on specific policy issues related to the reporting of information security incidents to the regulator.

Engagement activities undertaken by BCFSa during the consultation period included:

- Notifying all B.C. credit unions, insurance companies and trust companies of the opening of the consultation period and sharing the discussion paper via an Advisory;
- Publishing the discussion paper on BCFSa's website;
- Publishing a news release on BCFSa's website inviting the public and financial services sector stakeholders to participate in the consultation;
- Publishing a consultation webpage summarizing the objectives of the consultation and including links to key documents; and
- Meeting with several industry associations to increase understanding of the rationale and policy intent behind the proposed Rule, seek feedback, answer questions, and identify any unintended effects or potential issues that could arise because of proposals made in the discussion paper.

Summary of Feedback

BCFSa received over 20 separate submissions in response to the discussion paper. These included responses from individuals, financial institutions, and some industry associations which represent significant portions of the insurance and credit union segments including:

- Canadian Credit Union Association;
- Canadian Life and Health Insurance Association;
- Insurance Bureau of Canada;
- Canadian Association of Financial Institutions in Insurance; and
- Canadian Bankers Association.

Many submissions acknowledged the necessity for enhanced oversight of IS risks and reporting of material IS incidents.

The following table summarizes the key themes from the consultation feedback.

TABLE 1: KEY THEMES FROM FEEDBACK

Theme	Summary of Issue/Comment	BCFSA Response
Need for a Rule	There were concerns that BCFSA is moving too quickly to a rule. Given that BCFSA only recently issued the IS Guideline, and the effective date is not until September 30, 2022, some PRFIs stated they should be given the opportunity to demonstrate their ability to meet reporting expectations without the need for a Rule. Some extrapros indicated that since the IS Guideline did not apply to them, and this was the first time that BCFSA had indicated it expected them to report IS incidents, it was unfair to suggest that they would underreport or not report IS incidents. Some respondents argued that resorting to a Rule, with the associated potential for administrative penalties, was not justified at this stage. Both PRFIs and extrapros indicated that they would comply with established expectations to report IS incidents.	As the regulator, BCFSA requires awareness of material IS incidents, that is those that could have significant impact on a financial institution or its customers. BCFSA is aware that other regulators have observed an increase in reporting when reporting was made a requirement and underreporting of material events when not required. A rule would provide BCFSA with enhanced regulatory tools to deal with non-compliance especially for extrapros. However, BCFSA appreciates the concerns and issues raised during the consultation and the commitment to report material IS incidents to BCFSA. As such, BCFSA has decided to defer further work on an IS incident reporting rule to give PRFIs time to implement the expectations in the IS Guideline and BCFSA time to validate that reporting expectations are being met. With respect to the feedback from extrapros, BCFSA intends to bring forward a guideline that would communicate its expectations as they relate to incident reporting to BCFSA.

		BCFSA will monitor adherence to reporting expectations in current and future guidelines to confirm if there is a need for a rule due to underreporting.
Need to harmonize with other regulators	Extraprovincially incorporated insurance companies that conduct business across multiple jurisdictions, expressed a desire for BCFSA to work with other federal and provincial regulators to harmonize the IS incident reporting requirements to reduce compliance exceptions. Respondents also asked BCFSA to explore the idea of developing a common reporting template and/or sharing incident reports amongst regulators to reduce the incident reporting burden.	BCFSA's current incident reporting expectations for PRFIs are mainly aligned with requirements of the Office of the Superintendent of Financial Institutions ("OSFI"). The degree to which all reporting expectations can be fully harmonized will be limited by legislative requirements in some cases, and by the different mandates of each regulatory authority (e.g., BCFSA has a market conduct and prudential mandate). This may result in variances in some information collected. BCFSA will work with other regulators to harmonize definitions, triggers, and information requirements for reporting of material IS incidents to the extent possible. Specifically with the OSFI and the Autorité des Marchés Financiers ("AMF"), given that these two regulators have or will publish guidance on incident reporting. Regarding respondents' request for information sharing between OSFI and BCFSA, this could create privacy and security issues. Thus, financial institutions will need to report incidents to each regulator separately. BCFSA will continue to explore how harmonized reporting requirements could reduce

		administrative burden for financial institutions.
Reporting timelines	Several respondents asked for a longer reporting timeframe. They are concerned that the proposed 24-hour reporting timeline is too burdensome and would hinder their ability to respond to a material incident by diverting resources to incident reporting rather than the essential work of containing and remedying a security incident.	The current reporting expectations for PRFIs are outlined in the IS Guideline and include that BCFSa should be notified as soon as possible by email or phone call <u>once the determination has been made that an incident is 'material'</u>. Thereafter, an incident report should be provided within 72 hours. BCFSa continues to target alignment of reporting timelines with other Canadian regulators. BCFSa will consider feedback on reporting timelines received, including the desire to harmonize with other regulators, as part of its review and/or development of guidance.
Protecting sensitive information	Several respondents asked for confirmation that sensitive and confidential information provided in an IS incident report would be protected, and for further details on how information in an IS report would be transmitted and used. Specific concerns with sending reports via email were identified as emails present a large security vulnerability. A few respondents recommended the use of a secure portal as practiced by other regulators, including the federal and provincial offices of the Privacy Commissioner.	BCFSa takes all necessary steps to protect information in its custody and control to ensure compliance with its obligations under law and policy with respect to information security and confidentiality. For the reporting expectations outlined for PRFIs in the information security guideline, PRFIs are to file their incident reports through a BCFSa web portal called IRIS (Integrated Regulatory Information System), which is a safe and secure method for financial institutions to submit their confidential information.

Responding to Incident Reports	Many respondents stressed that BCFSa should continue building expertise and resource capacity in cyber and technology risk management. This is due to the serious nature of security incidents, as well as the potential financial implications for financial institutions. Respondents believe that increased expertise of BCFSa staff in this area would support broad confidence in the government-mandated systems that oversee consumer security.	BCFSa will apply the necessary resources to appropriately respond to IS incident reports and will continue to assess and develop its internal expertise and capacity in order to effectively respond to IS incident reports.
---------------------------------------	---	---

Summary of Consultation Outcomes and Next Steps

BCFSa would like to thank all those who responded to the discussion paper. The feedback was comprehensive, thoughtful, and well-articulated.

Based on the feedback from consultations as discussed above, BCFSa intends to take the following steps:

- 1) Defer work on an IS incident reporting Rule;
- 2) Work with federal and other provincial regulators to explore better harmonization of IS incident reporting across the country, particularly for extraprovincial:
 - BCFSa will continue to work with other regulators, specifically OSFI and the AMF to harmonize definitions, triggers, and information expectations for reporting of material IS incidents to the extent possible;
- 3) Following a period of implementation, work will be undertaken to update and clarify the existing IS Guideline for PRFIs with the following proposals:
 - Review reporting expectations based on BCFSa's work to harmonize definitions, triggers, and other information,
 - Include an expectation for PRFIs to keep a register of any IS incident regardless of severity and provide this list to BCFSa on request. The purpose of a registry would be to validate if a PRFI is reporting material IS incidents according to the expectations established through BCFSa Guidelines. Expectations for an IS incident registry would be consistent with those established by regulators in other jurisdictions, including the AMF,

- Clarify that all PRFIs would be expected to report within 24 hours once an incident has been determined to constitute a material incident. BCFSa understands that there would be a reasonable period between when a PRFI becomes aware of an incident and when it can conclude that the incident meets the materiality threshold,
 - Clarify that the initial stage report may contain a limited amount of confirmed and complete data. The subsequent report(s) would provide detailed reporting and follow in a timely manner as determined by BCFSa's relationship manager or pension advisor,
 - Clarify that with respect to third-party service providers, BCFSa would expect that PRFIs report a material incident within 24 hours of the PRFI becoming informed of the incident by the service provider and the PRFI having determined that the incident was material, and
 - Target Fall 2023 to discuss proposed revisions with PRFIs;
- 4) Publish and consult on a separate IS Incident Reporting Guideline for extraprovincially regulated financial institutions (excluding pension plan administrators) that are authorized to conduct business in B.C.:
- Communicate incident reporting expectations to BCFSa which reflect a harmonized approach with other regulators,
 - Clarify a proposed expectation to maintain a registry of IS incidents,
 - Target Spring 2023;
- 5) Build on BCFSa's existing secure reporting systems and augment existing systems and processes to ensure the continued safe and secure handling of IS incident reports; and
- 6) Apply existing BCFSa resources to address incident reports and continue to assess and develop internal expertise and capacity to respond to reported IS incidents.



600-750 West Pender Street
Vancouver, B.C. V6C 2T7

604 660 3555

Toll free 866 206 3030

info@bcfsa.ca