JANUARY 2022

Discussion Paper:

Information Security Incident Reporting

BCFSA

Contents

Introduction 1

Objective: Why is Incident Reporting Important for Effective Regulation? 2

Scope 3

Compliance 3

Reporting Requirements 4

Introduction

As our economies and societies grow more dependent on digital technology, it is important to ensure that the associated risks are properly managed. On October 1, 2021, BCFSA released its Information Security ("IS") Guideline for financial institutions. The guideline outlines principles that regulated entities are expected to implement and follow to mitigate IS risks.

Like IS guidance in other jurisdictions, BCFSA's Information Security Guideline includes expectations to report specified IS incidents. However, BCFSA is aware that in some jurisdictions with IS incident reporting expectations, organizations have not been reporting these incidents to regulatory authorities.

Given the potentially serious implications for consumers, individual financial institutions, and the financial services sector, BCFSA is exploring stronger measures to ensure timely and accurate reporting of IS incidents. BCFSA is considering the establishment of a new rule under the *Financial Institutions Act* to require financial institutions to report material IS incidents to the regulator. As a first step, this document is intended to seek feedback from stakeholders including financial institutions on the policy issues related to the reporting of IS incidents to BCFSA. Key questions for consideration are highlighted throughout this Discussion Paper. Please submit feedback by February 25, 2022 to policy@bcfsa.ca.

Responses and feedback on this Discussion Paper will inform BCFSA's next steps, including seeking ministerial approval to conduct a separate public consultation on a draft Incident Reporting Rule.

Objective: Why is Incident Reporting Important for Effective Regulation?

BCFSA's role is to safeguard confidence and stability in B.C.'s financial sector by protecting consumers while also allowing the financial sector to take reasonable risks and compete effectively.

The objective of an Information Security Incident Reporting Rule would be to ensure that BCFSA is aware of material IS incidents at financial institutions authorized to do business in the province. Financial institutions would be required to notify BCFSA within specified timelines of a reportable IS incident that could: impair the operations of an individual financial institution; disclose confidential customer or corporate information; result in customers being unable to access their deposits and other accounts; or impact the stability of the financial services sector.

Receiving timely information about reportable IS incidents would enhance the ability of BCFSA to protect consumers and safeguard the stability of the financial services sector by:

- Supporting BCFSA to verify appropriate actions are being taken to mitigate impacts on customers and the financial institution when services are disrupted;
- Positioning BCFSA to conduct analyses across financial institutions aimed at improving guidance and adjusting supervisory programs to prevent similar incidents and to improve resilience after an incident has occurred;
- Allowing BCFSA to share sharing information with Financial Institutions on patterns or trends it detects through an analysis of IS incident reports, in an anonymized fashion; and,
- Improving BCFSA's awareness of risks arising in the financial services sector.

Q. Are you comfortable with BCFSA sharing information on patterns or trends it detects through an analysis of IS incident reports, in an anonymized fashion? How can BCFSA best share this information with financial institutions?

Scope

BCFSA is considering developing a rule that would apply to all credit unions, insurance and trust companies authorized to do business in B.C., including extraprovincial companies with customers in B.C. (collectively, "financial institutions").

For extraprovincial financial institutions, BCFSA would rely on the primary regulator of that financial institution's province or territory to determine the financial implications of an IS incident on the institution. However, BCFSA would need to be made aware of IS incidents in a timely manner to assess potential impacts on customers living in B.C. For this reason, the reporting requirements may vary by "class" of institution. For example, financial institutions incorporated and prudentially regulated in B.C. may be one class of institution while extraprovincial financial institutions may be another.

An Information Security Incident Reporting Rule would not apply to pension plan administrators as the *Pension Benefits Standards Act* does not provide rule-making authority. However, the reporting expectations outlined in the Information Security Guideline will remain and pension plan administrators are expected to report material IS incidents.

Compliance

Failure to comply with a rule is a contravention of the *Financial Institutions Act* ("FIA") and may subject the non-compliant financial institution to regulatory action by BCFSA. This includes, but is not limited to, an administrative penalty up to $50,000 for a corporation or $25,000 for an individual.

Reporting Requirements

The following section describes the potential range of proposed reporting requirements.

Reporting Criteria

Under a potential Information Security Incident Reporting Rule, an IS incident would include:

- Unauthorized, illegal, or accidental use, disclosure, access to, modifications, or destruction of personal information, business information, or data; and/or
- Impairment of network systems.

To avoid requiring financial institutions to report on all IS incidents, BCFSA's focus is on the reporting of material incidents with consideration for scope, impact, and significance.

A reportable IS incident would include one that has caused or has the potential to cause material harm to consumers, or financial or reputational damage to financial institutions[1] *or the financial services sector.*

Examples of what BCFSA would consider to be a reportable IS incident could include incidents that have already or may adversely affect:

- The operations of critical information systems or data;
- A financial institution's operational or customer data, including confidentiality, integrity, or availability of such data;
- Internal users that are material to customers or business operations;
- Systems or services impacting customers or business operations;
- A financial institution's reputation (for example, public/media disclosure);
- Critical deadlines/obligations in financial market settlement or payment systems (for example, Financial Market Infrastructure);
- A third-party deemed material by the financial institution; and

[1] As noted in the Outsourcing Guideline, outsourcing service providers are expected to comply with BCFSA's Information Security Guideline including reporting of material IS incidents affecting the FI. Material incidents reported to an FI by an outsourcing service provider would be required to be reported to BCFSA.

- Other financial institutions or the B.C. financial services sector.

This is not an exhaustive list of all incidents that financial institutions may be required to report; however, BCFSA has included examples consistent with those provided by other Canadian financial services regulators.

An IS incident report to the regulator could be triggered by the actions of a financial institution in response to an IS incident. A financial institution may be required to report an IS incident if the incident was:

- Reported, or is reasonably expected to be reported, to the media or to the financial institution's members, users, customers, or participating organizations;
- Escalated to internal or external legal counsel, senior management, or Board of Directors;
- Reported to the Office of the Privacy Commissioner, law enforcement agencies, other regulatory authorities; or
- Reported to a cyber-insurance company.

Q. Is the definition of what constitutes a material incident clear? If not, why?

Q. Do the identified triggers provide sufficient guidance on when reporting is required?

Q. Based on the above definition and triggers, how many IS reports would you estimate that you might complete on an annual basis?

Notification Requirements

Initial Notification

In the event of a reportable IS incident, BCFSA's Incident Reporting Rule would require a financial institution to report the incident to BCFSA as soon as possible and no later than 24 hours after the incident is identified.

Incident Report

As previously noted, the incident reporting requirements may vary by class of financial institution. BCFSA proposes two classes:

(i) B.C. incorporated financial institutions (where BCFSA is the primary regulator); and
(ii) extraprovincially incorporated financial institutions (where a jurisdiction other than BCFSA is the primary regulator).

When reporting an information security incident to BCFSA, a financial institution would be required to do so in writing. Where specific details are unavailable, the institution would be required to provide best known estimates and all other details available at the time of reporting.

For financial institutions incorporated in B.C., an incident report would include the following:

- Date and time the incident was detected;
- Date and time the incident took place;
- Incident type (for example, denial of service, malware, data breach, extortion, or internal breach);
- Incident description, including:
  - Known direct/indirect impacts,
  - Extent and sensitivity of information released,
  - Known impact to one or more business segments, business units, lines of business or regions, including any third party involved,
  - Technologies affected,
  - Site/location affected,
  - Description of sensitive information compromised or at risk (for example, customer and financial information),
  - Whether the incident originated at a third party, or has impact on third party services, and
  - Number of clients impacted;
- Primary method used to identify the incident;
- Status of incident;
- Date of internal incident escalation to legal counsel, senior management, or Board of Directors;
- Mitigation actions taken or planned;
- Known or suspected root cause;
- External notifications (for example, cyber insurance providers, other authorities, customers); and

- Name and contact information for the IS incident executive lead and the principal contact for BCFSA.

For extraprovincially incorporated financial institutions, an incident report would include information related to customers residing in B.C., including:

- Date and time the incident took place;
- Incident description, including:
    - Known direct/indirect impacts,
    - Extent and sensitivity of information released, and
    - Known impact to one or more business segments, business units, lines of business or regions, including any third party involved;
- Incident type (for example, denial of service, malware, data breach, extortion, or internal breach);
- Known direct/indirect privacy impacts;
- Number of B.C. customers affected;
- Mitigation actions taken or planned;
- External notifications (for example, cyber insurance providers, other authorities, or customers); and
- Name and contact information for the IS incident lead and the principal contact for BCFSA.

Subsequent Reporting Requirements

With a reporting rule, all financial institutions would be required to provide updates at intervals determined by BCFSA as new information becomes available, including any short-term and long-term remediation actions and plans. These updates would be required until the incident is resolved.

Following containment, recovery, and resolution of the IS incident, financial institutions would be required to report to BCFSA on its post-incident review, including lessons learned.

Q. Are these reporting timelines reasonable? Which elements would be difficult for an FI to respond to within the timelines and why?

Q. Is the content of the incident report and subsequent report clear and reasonable?

Q. Are there any other considerations you want to share with us that we have not addressed in the document?

BC Financial Services Authority

600-750 West Pender Street
Vancouver, BC V6C 2T8

604 660 3555
Toll free 866 206 3030
info@bcfsa.ca