JUNE 2024

Information Security Incident Reporting Guideline

Extraprovincial Insurance Corporations and Extraprovincial Trust Corporations

Draft for Consultation

BCFSA

Contents

1. Introduction

As the digital transformation of financial services continues to increase in pace and scale, it brings with it heightened risks to British Columbia's citizens and economy, particularly from potential information security incidents that could compromise critical services or sensitive information.

As the financial services regulator in B.C., with a mandate to safeguard confidence and stability in the financial sector, BCFSA is introducing this guideline to ensure it is appropriately notified of information security incidents that impact British Columbians.

The incident reporting guideline for extraprovincial insurance corporations and extraprovincial trust corporations outlines expectations regarding the reporting of material information security incidents by insurance and trust corporations incorporated in other provinces, and federally regulated insurance and trust corporations, that are authorized to conduct business in B.C. ("extrapros"). This guideline does not apply to extraprovincial reciprocal or captive insurance corporations.

This guideline does not replace or substitute other applicable rules, guidance or law and does not require extrapros to act in a way that is incompatible with any legal or regulatory requirements.

2. Scope

Information security ("IS") incidents include, but are not limited to, unauthorized, illegal, or accidental use, disclosure, access to, modifications or destruction of data, or impairment of network systems, that have a detrimental impact on the operations of an extrapro including its confidentiality, integrity or the availability of its systems and information. The risk of unauthorized or illegal access to sensitive information or systems can come from employees, consultants, and others within the extrapro or external threat actors.

Data can be generated by the extrapros or provided by third parties to the extrapros. Data collection, storage and processing can be in any format (for example; paper, electronic, or video) or location (for example; onsite, offsite, or cloud service). Information systems include people, machines, methods of organization, and procedures which provide input, storage, processing, communications, output, and control functions in relation to information and data.

3. Communication with the Regulator

An extrapro is expected to be in communication with BCFSA in the event of a material incident.

- The extrapro should notify BCFSA as soon as is reasonable, but no later than 72 hours, after determining that an incident is material.
- For contents of the IS incident report please see next section titled “Information Security Incident Reporting Information Requirements.”
- Extrapros should ensure that all affected stakeholders, including clients and relevant privacy regulators, have been notified as necessary, and reasonable steps have been taken by the extrapro to limit harm to consumers.

Steps for submitting an incident report.

Step 1. Notification of intent to submit an incident report:

- Notify BCFSA of your intent to submit an incident report by sending an email to XXXX@bcfsa.ca. Please include name and contact information for the extrapro’s incident lead and liaison with BCFSA.
- Do not send the incident report or include any sensitive information about the incident in your notification email.

Step 2. Receive secure link to submit an incident:

- Once BCFSA receives the notification email, BCFSA will provide a secure SharePoint link and instructions on how to upload the incident report and other correspondence pertaining to the incident.

4. Information Security Incident Reporting Information Requirements

Details to report should include the following:

- Date and time the incident was discovered/detected;
- Date and time/period the incident occurred;
- Incident type (for example, internal breach, malware, data breach, extortion, etc.);
- Incident description, including:
    - Known direct/indirect financial and privacy impacts (quantifiable and non-quantifiable) including a description of the sensitive information covered by the incident,
    - Known impact to one or more business segment, business unit, line of business or regions, including any third party involved,
    - Whether the incident originated at a third party or has an impact on third party services, and
    - Number of customers affected who are resident in B.C.
- Indicators of compromise;
- Current status of incident;
- Date for internal incident escalation to senior management or Board of Directors;
- Mitigation actions taken or planned;
- Known or suspected root cause; and
- Name and contact information for the extrapro's incident lead and liaison with BCFSA.

Where specific details are unavailable at the time of the initial report, the extrapro should indicate "information not yet available." In such cases, the extrapro should provide best known estimates and all other details available at the time.

To facilitate incident reporting by regulated entities or individuals that are required to submit multiple incident reports, BCFSA will also accept being notified with a comparable form issued by another financial services regulator. If another equivalent form is used, it must include information on the number of customers affected who are residents of B.C.

5. Subsequent Reporting Requirements

Extrapros may be expected to provide BCFSA with regular updates as new information becomes available, and until all material details about the incident have been provided.

- The method and frequency of these updates, including final reporting expectations, should be established through discussions with BCFSA and should be commensurate with the severity, impact, and velocity of the incident, timelines established by the primary regulator, and the number of B.C. residents affected. In normal circumstances, if subsequent reports are requested, the cadence and content of follow up reporting would align with and should not exceed those of the primary regulator. BCFSA may request more information specific to the impacts on B.C. residents if warranted.
- Following incident containment, recovery, and closure, the extrapro may be expected to report to BCFSA on its post incident review and lessons learned.
- Upon receipt of the initial notification, BCFSA may determine that further reporting is not warranted.

6. Determining if an Information Security Incident is Material

An IS incident should be of a certain degree of severity for it to be reported to BCFSA.

- The determination of the severity of an event is made by the extrapro and should relate to the impact that the incident will have on the extrapro's users, consumers, or the general public.
- In assessing the severity of a specific incident, the extrapro may want to consider the following factors, among others.

Is this an incident that:

a. Has been reported, or is reasonably expected to be reported, to the media or to the extrapro's users, or participating organizations with potential for a negative reputational impact?

b. Is reported to senior management or the Board of Directors?

c. Results in significant operational impacts to key/critical information systems or data?

d Materially affects an extrapro's operational or customer data, including confidentiality, integrity, or availability of such data?

e Has a significant operational impact on internal users that is material to clients or business operations?

f Causes significant levels of system/service disruptions to critical business systems?

g Is affecting a significant or growing number of customers?

h Creates a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use, and the likelihood that such information will be used for injurious purposes?

i Will have a material impact on critical deadlines/obligations in financial market settlement or payment systems?

j May have a significant impact on a third party affecting the extrapro?

k Has been reported to another regulator or other authorities?

MATERIAL INCIDENT EXAMPLES

Scenario Name	Scenario Description	Impact
Cyber Attack	An account takeover botnet campaign is targeting online services using new techniques, and current defenses are failing to prevent customer account compromise.	• High volume and velocity of attempts • Current controls are failing to block attack • Customers are locked out • Indication that accounts have been compromised
Service Availability & Recovery	There is a technology failure at a data centre.	• Critical online service is down, and the alternate recovery option failed • Extended disruption to critical business systems and operations
Third Party Breach	A material third party's system is breached, and the extrapro is notified that the third party is investigating.	• Third party is designated as material to the extrapro • Material impact to the extrapro data is possible
Extortion Threat	An extrapro has received an extortion message threatening to perpetrate a cyber-attack (e.g. Distributed Denial of Service attack unless a Bitcoin payment is received)	• Threat is credible • Probability of critical online service disruption
Internal Breach	An employee or contractor has intentionally or inadvertently caused sensitive data to be accessed destroyed, modified, or made inaccessible.	• Indications that accounts have been compromised.

BC Financial Services Authority

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

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