LCU Privacy Breach Respo

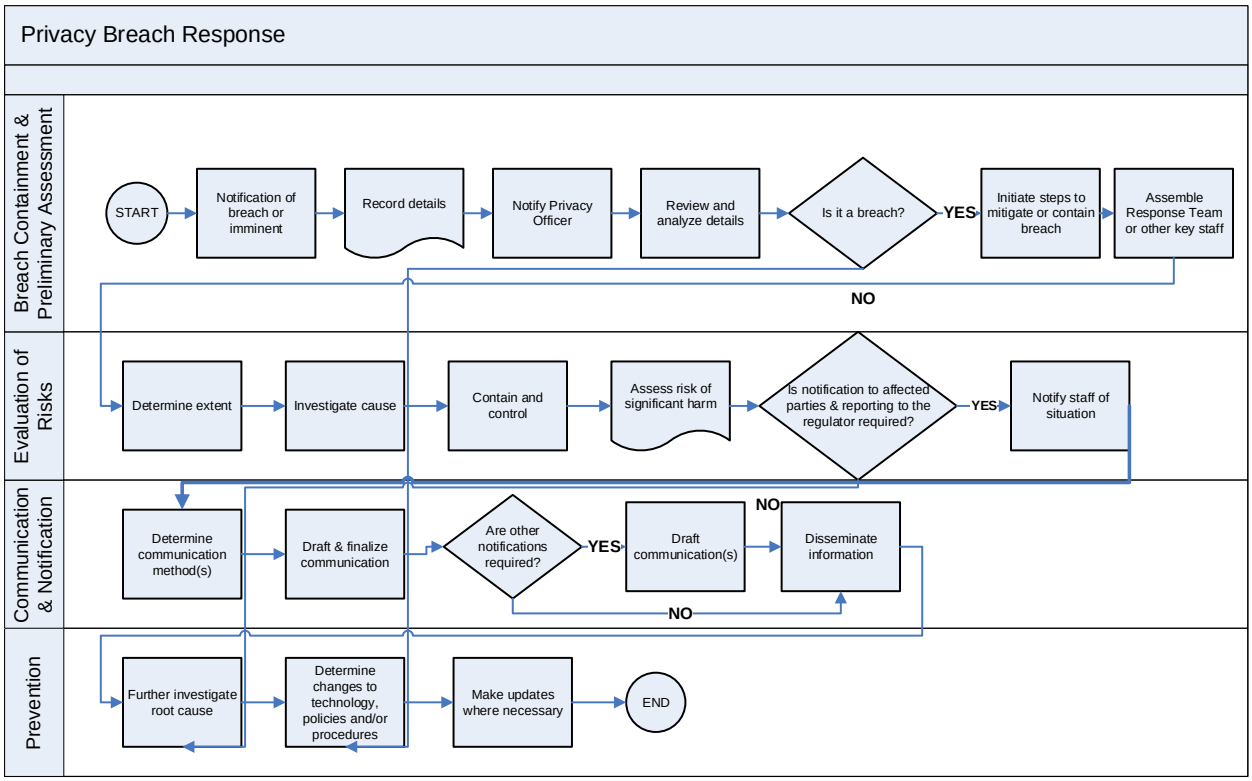
September 2018

Updated Dec 2021

Introduction

The Credit Union makes every effort to safeguard all personal information collected during the course of business and protect that which resides on the Credit Union's information systems and devices. The *Privacy Breach Response Plan* documents the policies and procedures related to planning for, responding to, and recovering from privacy breaches.

Process Overview



What is a Privacy Breach?

A privacy breach is the result of unauthorized access to, or collection, use or disclosure of personal information. Such is defined as "unauthorized" if it has occurred in contravention of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The acquisition of personal information by staff during the course of business is not considered a privacy breach providing the information is only used for the purposes for which it was intended. Additionally, personal information is only shared internally and externally on a need to know basis.

Some examples of potential privacy breaches are:

- Unauthorized access to equipment, an application, or database;
- Loss or theft of an asset or device, i.e. stolen laptop; and
- Disposal of an asset or device without purging the information on the item.

Personal Information

Personal information is information about an identifiable individual. It may be linked directly or indirectly to an individual. Examples include home address; personal email address; Social Insurance Number (SIN); banking information (payment card number, bank account), health information, etc.

The Credit Union collects personal information in order to offer products and services to its members. The following chart details the types of personal information collected, used or disclosed by the credit union, where it is stored, how it is protected and third parties to whom the information is disclosed:

Application / Activity	Type of Information	Location	Security Measures	Third Party Disclosures
Membership Applications & Account Opening Loan applications and other credit services	Name, home address, email address, SIN, phone no.'s, driver license, health card number	Stored in vault or locked file room. Also stored on internal server	Stored in locked vault and/or loan file room. Electronic data is secured behind a firewall provided by Celero to Lafleche CU	Gov't regulatory, FINTRAC, Auditors, DGC, etc.

Roles & Responsibilities

Maintaining the privacy and protection of personal information at the Credit Union and includes the following responsibilities:

Staff

All staff will:

- Make every effort to safeguard personal information in their care;
- To the extent possible, minimize the amount of personal information saved in the cloud environment;
- Notify the Privacy Officer immediately upon discovering a potential breach;
- Contain or suspend any activity/process known to be at the root cause of a breach or as directed following an investigation;
- Seek guidance in situations where uncertainty of the nature of information exists.

Privacy Officer

The Privacy Officer will:

- Manage the privacy breach response process including containment, assessment, evaluation of risks and possible notification and reporting;
- Liaise with third parties contracted to assist with the breach (as applicable);
- Liaise with authorities including Privacy Commissioner and law enforcement if reporting required;
- Monitor related legislation and industry developments;
- Review effectiveness of processes, procedures and strategies for dealing with incidents.

Assessment Team

Members of the Assessment Team are responsible to:

- Participate in the assessment of the incident;
- Assist the Privacy Officer to obtain all known details about a breach;
- Provide guidance on next steps where extraneous circumstances exist.

Information Technology

Specific members of the Assessment Team will:

- Participate in the assessment of the incident;
- Assist in the investigation of a breach where technology related;
- Undertake actions where appropriate to contain a breach
- Take corrective actions to prevent future breaches if necessary.

Communications

Communications is responsible to:

- Determine strategies and communication vehicles to be used when notification determined to be necessary;
- Draft and/or review written communications;
- Act as spokespersons for all media inquiries.

Human Resources

General Manager is responsible for:

- Ensuring data access rights are revoked and credit union equipment and mobile devices are returned in the event that termination of employment is appropriate as a result of the data breach.

The members of the Response Team include:

Role	Staff Member	Office Telephone	Office Issued Cell
Privacy Officer	Tracy Johnson	306-472-5215	306-472-7695
Privacy Officer Backup Designate	Carmen Ellis	306-472-5215	306-472-7647
Assessment Team			
	Carmen Ellis	306-472-5215	306-472-7647
	Lori McLean	306-266-4821	
Communications Team			

The Privacy Breach Response Plan includes four stages:

1. Breach containment and preliminary assessment;
2. Evaluation of risks associated with the breach;
3. Communication and notification; and
4. Prevention of future breaches.

Breach Containment and Preliminary Assessment

Breach Containment

Immediate action to the situation is required to minimize potential damages. The first person to receive notification of a suspected breach shall:

1) Document details:
    a. Record the date, time and location of the potential breach;
    b. Record a general description of the incident;
    c. Document any steps or actions that have been taken to contain or remedy the breach;
    d. Record other relevant details as required.

⇨ Refer to Template: *Privacy Breach Assessment Form*

Preliminary Assessment:

2) Notify the Privacy Officer or designate in his/her absence.

3) The Privacy Officer (or designate) will assess the scope of the incident and undertake an assessment to determine if an actual breach occurred. This involves a review of all known facts with members of the Assessment Team, Communications staff as required. If a privacy breach is confirmed, the Privacy Officer (or designate) will initiate the steps required to mitigate or contain a privacy breach including consultation with all members of the Senior Management Team.

Evaluation of Risks Associated with the Breach

1) The Privacy Officer will determine the extent of the breach including identification of the:
    a. Source (network, personal device, hardcopy records);
    b. Number of individuals whose information is involved;
    c. Type of information compromised or at risk (names, financial account information, SIN numbers, etc.).

2) Determination of cause:
    a. Is this incident a systemic problem or an isolated incident?
    b. Is there a risk of ongoing breaches or further exposure of the information?
    c. What mitigation steps have been taken so far?

3) Risk Assessment:
    a. How sensitive was the personal information that was breached?
    b. What is the probability that the personal information has been, is being or will be misused?
    ⇨ Refer to Template: Privacy Breach Incident Report for communicating the breach to the Privacy Officer *(see Appendix A)*

4) Under the direction of the Privacy Officer, members of the Response Team as appropriate, will initiate steps to investigate the cause and extent of the breach as indicated in the chart:

Affected Area	Investigate	Contain and Control
Network	▪ Record system information such as operating systems, domain names and IP addresses. ▪ Scan network to determine point of compromise including test environments and the VPN. Review system and audit logs as necessary. ▪ Determine what measures were in place at the time of the incident (access limitations, encryption, passwords, etc.).	▪ Shutdown applications or reconfigure firewalls. ▪ Change authentication information (IDs, passwords); disable account in the case of an unauthorized intruder/user. ▪ Isolate the compromised system from the network but leave it on and intact. ▪ Monitor the network and/or systems for further intrusion or unauthorized activity. ▪ Maintain network and audit logs for evidence. Document all actions undertaken by those staff members involved. ▪ Determine if new hardware/software is required.

Missing Asset (laptop, Smartphone)	▪ Determine the nature of the loss (theft, misplaced). Document the chronology of events proceeding. ▪ Determine what measures were in place at the time of the incident (locks, alarm systems). ▪ Document the inventory: what types of information were present.	▪ Disable asset from network services, i.e. mobile device wiped clean and device PIN reset. ▪ Deactivate service from provider (smartphone). ▪ Depending on the extent of personal use, change your online passwords to help prevent compromised accounts. ▪ Report loss of the asset to the General Manager (for asset management inventory purposes). ▪ Notify insurance provider (CUMIS) if deemed necessary. ▪ If theft or other criminal activity is suspected, notify the police.
Hardcopy records	▪ Determine nature of loss (including an inventory of records compromised, actions that led to loss, method used to access the records and what safeguards were in place to prevent loss at the time of the compromise).	▪ Determine if procedures are required or existing ones require changes. ▪ Determine if physical safeguards need amendment to ensure against future breaches; ▪ Determine if training is required.

Communication & Notification

Regular, open and honest communication is fundamental to the response process. The key areas of communication include:

Internal staff

The effective dissemination of information to applicable staff is critical during a privacy breach. Once a privacy breach is confirmed:

1) The Privacy Officer (or designate) will provide an email notification advising staff of the situation as necessary;
2) All external inquires will be directed to the Privacy Officer (or other designated spokesperson);
3) Regular updates shall be provided to staff on progress and/or next steps.

Reporting to the Office of the Privacy Commissioner of Canada

As of November 1, 2018, the Breach of Security Safeguards regulations under PIPEDA will require credit unions to report to the Office of the Privacy Commissioner (OPC) data breaches that pose a "real risk of significant harm" to affected individuals. "***Significant harm*** includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

When the risk assessment determines that there is a real risk of significant harm to those affected, a report must be provided to the OPC. The same legal threshold has applied to credit unions operating in Alberta, who have been required to report privacy breaches to the Alberta Information and Privacy Commissioner since 2010.

The means of reporting are:

E-mail	Phone	By Mail
notification@priv.gc.ca	819-994-5444 Toll-free: 1-800-282-1376	Notification Officer Office of the Privacy Commissioner of Canada 30 Victoria Street Gatineau, Quebec K1A 1H3
Details Required	The Privacy Breach Incident Report Form when completed can be referenced to obtain the necessary details for the report to the OPC and meets record keeping requirements if retained for 24 months.	

Affected Individuals

If the breach has been determined to create a real risk of significant harm or risk to the individual(s), notification should be provided. The decision to notify would be made on a case-by case basis after undertaking a risk assessment (see details on Page 7).

If deemed that notification is to be provided, the following guidelines will be used:

Notification		Recommended Practice
Timeframe		▪ As soon as reasonably possible; ▪ If law enforcement is involved guidance will be sought to ensure the investigation is not compromised.
Communication Methods	Direct	By phone, letter or email direct to the individual(s) or in person.
	Indirect	Conspicuous notices posted on website for a minimum of 90 days, or by means of an advertisement that is likely to reach the affected individuals – can be used only when direct methods: ▪ Could cause further harm; ▪ Would result in undue hardship for the organization i.e. when direct notice would be cost prohibitive; ▪ When contact information is unknown.
Responsible party		The party/organization having the direct relationship with the individual(s).
Information Required		▪ Description of the circumstances of the breach; ▪ The day on which, or period during which, the breach occurred; ▪ A description of the personal information involved; ▪ Summary of the steps undertaken to reduce or control the risk; ▪ How to access additional assistance provided by Lafleche CU to resolve the issue and/or further mitigate or eliminate the risk (i.e. the provision of free credit monitoring for a period of time). ▪ A toll-free number or email address that the affective individual can use to obtain further information about the breach; ▪ Information about The Lafleche CU's internal complaint process and about the affected individual's right, under the Act, to file a complaint with the Privacy Commissioner.

Other Notifications

Other notifications may include:

Organization	Circumstances
Law Enforcement	If a crime is suspected
Insurers; business partners	If contractually obligated or if a claim will be filed
Regulatory bodies	If required by law, standards, rules or contract
Financial Institutions, Credit Card companies	If assistance or expertise is required or if necessary to mitigate risk

Prevention

After steps have been undertaken to resolve the breach, a detailed investigation shall be performed to determine if the breach was an isolated incident or systematic issue. Actions may include:

- Information systems audit;
- Training and awareness programs;
- Updates to processes, policies or procedures;
- Review of related service level agreements or other contractual obligations, and/or
- A review of insurance coverages.

Communication on new processes or changes to organizational practices where relevant will be provided to staff.

Plan Management

Effective plan management is one of the most important elements in the process. Plan management and maintenance are outlined in this section.

Availability of the Plan

This plan is available through the following means:

- Available in electronic format on the Credit union's website

Monitoring & Review

This *Privacy Breach Response Plan* is a living document. The Lafleche CU management team is responsible for the updating of this document as required.

This document will be reviewed by the Legal and Governance Department to determine if any amendments are required:

- On an bi-annual basis;
- Following legislative/regulatory changes to ensure continued compliance; and
- Following any privacy breach.

Amendments

Amendments to the Privacy Breach Response Plan will be provided to the Lafleche CU Board of Directors as they occur.

PRIVACY BREACH INCIDENT REPORT

Completed by:	Date:	Time
Description of the incident:		
Day on which incident occurred or the period during which the breach occurred:		
Description of personal information involved:		
The estimated number of individuals to whom the breach creates a real risk of significant harm:		
Description of the harm that could result and the probability of such harm:		
Actions taken to reduce risk of harm to each affected individual or to mitigate that harm:		
Actions taken to notify each affected individual:		
Contact person/title:		
Other Information (as applicable):		