Print form

PIPEDA breach report form

For use by private sector organizations reporting breaches of security safeguards to the Office of the Privacy Commissioner (OPC)

What is a breach of security safeguards (breaches)?

A breach of security safeguards is defined in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) as: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA or from a failure to establish those safeguards.

Am I required to submit a report to the OPC if it has had a breach?

On June 18, 2015 the *Digital Privacy Act* was passed into law. This Act includes an amendment to PIPEDA requiring organizations to report breaches of security safeguards to the OPC involving personal information under their control where it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

This requirement is effective as of November 1, 2018. Read our guidance for more information. The present form can be used by organizations that have experienced a breach to meet their legal obligations under PIPEDA and the Breach of Security Safeguards Regulations: SOR/2018-64.

I am an individual affected by a privacy breach. Should I use this form?

Individuals who would like to make a complaint about a breach of their privacy by an organization should not use this form. Instead, please consult the Report a concern section of our website.

Should I include personal information in this form?

No. The form need not include personal information other than the business contact information of the person(s) at the organization that the OPC can contact with any follow-up questions. For instance, the form need not include the names or other identifying details of affected individuals unless it's necessary to explain the personal information involved. It is intended to provide information about the breach and nature of information.

How quickly after a breach should I submit this form?

Organizations must report a breach of security safeguards to the OPC as soon as feasible after the organization determines that the breach has occurred, even if not all information (e.g. the cause, or planned mitigation measures) is known or confirmed. You can add or correct information as it becomes available.

What can happen after a breach is reported to the OPC?

When the OPC becomes aware of a breach, we might seek more information from the organization involved and then work to identify and resolve any compliance issues with PIPEDA and mitigate any of the incident's damaging effects.

How will the OPC handle information provided by organizations in a breach report?

The OPC generally has a duty to maintain the confidentiality of breach reports submitted to the Privacy Commissioner under PIPEDA. However, there are some exceptions to this obligation. For instance, the OPC may disclose information in a breach report to:

- domestic and international counterparts in accordance with information sharing agreements or arrangements; or to
- a government institution if the Commissioner has reasonable grounds to believe that the information could be useful in the investigation of a contravention of the laws of Canada or a province.

The Commissioner may also disclose information publicly where he believes it is in the public interest to do so. Public interest disclosures are considered carefully on a case-by-case basis. The Commissioner would normally not publicly disclose information that would pose a security risk.

Information provided to the OPC in a breach report could sometimes be used as the basis for initiating an investigation and in any ensuing investigation.

The Digital Privacy Act also amends the federal *Access to Information Act* (ATIA) to create a statutory exemption from the disclosure of any data breach of security safeguards report in response to access to information requests under the ATIA.

Where can I get more information on responding to a privacy breach?

Please see our office's guidance entitled What you need to know about mandatory reporting of breaches of security safeguards.

PIPEDA Breach Report

Throughout this form, the asterisk (*) denotes mandatory fields as required by law. Other fields are optional.

(•) original report

( ) amended or updated report

Information about the organization

* Legal name of the organization:
Cornerstone Credit Union Financial Group Limited
Address of organization:
P.O. Box 1210 Yorkton, SK S3N 2X3

*** Contact information of a person who can answer, on behalf of the organization, OPC's questions about the breach:**

*** Please choose one:**	( ) **Internal representative** (•) **External representative**
*** Name:**	Kristél Kriel
*** Title/position:**	External legal counsel
Country code: 1	*** Telephone:** (306) 347-8614 **Extension:**
*** Email:**	kkriel@mltaikins.com
*** Street address:**	Suite 1500, 1874 Scarth Street
*** City:**	Regina
*** Province/State:**	SK
*** Postal code:**	S4P 4E9
*** Country:**	Canada

Breach description

* **Number of individuals affected by the breach or, if unknown, the approximate number:** (If possible, please also provide the total number of Canadians affected by the breach)

* Total affected:	28,102
Canadians affected:	28,002

Comments:

There are approximately 100 individuals who currently reside outside of Canada - for these individuals, a copy of this notification will also be provided to the applicable privacy commissioner/authority (where required).

* **When the breach occurred:**
(Please describe the day on which the breach occurred, or the period during which the breach occurred, including a date range, if applicable)

* Start date of breach occurrence:	08-Jun-2022
End date of breach occurrence:	08-Jun-2022

Comments:

Type of breach:
(Please select the option that best fits from the list below.)

Unauthorized access by malicious or potentially malicious actor(s)

*** Description of the circumstances of the breach, and, if known, the cause:**

1. Description of all organizations involved in the breach including their role(s) with respect to the personal information in question,
2. How and why the breach occurred (please include some technical detail regarding the breach including an explanation of the methodology of the attack if one took place),
3. When the breach was discovered,
4. Where the breach occurred,
5. Who may have had access to the personal information (to the extent known)

1. With respect to this incident Cornerstone's insurer is CUMIS Group Ltd., Cornerstone's legal and breach counsel is MLT Aikins LLP, and Cornerstone's forensic and communications experts are Deloitte LLP. Celero Solutions Inc. is one of Cornerstone's managed service providers.

2. Based on the investigation to date, it appears that unknown individuals gained access to Celero's systems and through that access gained access to Cornerstone's systems. The investigation determined that unknown individuals gained interactive access to one of Cornerstone's servers that may have contained personal information.

Even though the investigation discovered no proof that information had been accessed or exfiltrated, Cornerstone decided out of an abundance of caution to notify the potentially impacted individuals.

3. The incident was discovered on June 8, 2022 when Celero, a managed services provider of Cornerstone notified Cornerstone that they had experienced an incident. Celero confirmed that they took immediate action to block the incident to limit the impact on their clients and began investigating the assess what information may have been compromised. Out of an abundance of caution, Cornerstone also launched an investigation into the incident.

4. The breach occurred on one of Cornerstone's servers. Please see above for more information.

5. The identity of the individual(s) who may have had access to personal information as a result of the above is unknown.

Description of relevant security safeguards in place at the time of the breach to prevent the type of incident that occurred:

Industry standard protections against these types of threats including, for example:

- Contracted a Managed Network Provider who manages all in branch routers and firewalls and first level dark web monitoring

- Endpoint Protection Alerting through a reputable product (AlertLogic)

- Endpoint Protection for Antivirus/Malware through a reputable product (Microsoft Defender)

- Annual Cyber Security Training is mandated for all employees and regular Phishing tests were in place

- Workstation/Laptop Patch Management through Microsoft SCCM

- Security Policies including
    - Microsoft Safelinks for Email
    - External Email Flag – All external emails were flagged as external to help prevent Phishing attacks
    - Workstation/Laptop Bitlocker Encryption

- Employed a dedicated Security Analyst position and Manager whose responsibilities included security

- External access to Cornerstone's Microsoft environment requires multi-factor authentication

- Geoblocking in place for Cornerstone's Microsoft environment

*** Description of the personal information that is the subject of the breach to the extent known:**

Describe the type and nature of the personal information that was breached (for instance, name, phone number, email address, account number, social insurance number, etc.). Please specify if client or employee information was accessed.

IMPORTANT: This section need not include any identifying information, unless it is necessary to explain the nature and sensitivity of the information.

Please see above relating to the circumstances of this incident.

Individuals that may have been impacted include members of Cornerstone..

The information that may have been impacted differs depending on the individual but includes, for example, name, member number, account number, date of birth, or social insurance number.

Notification

The Breach of Security Safeguard Regulations stipulate that any notification where the breach represents a Real Risk of Significant Harm (RROSH) must contain specific elements laid out in Section 3 of the Regulations.

*** Description of the steps that the organization has taken or intends to take to notify affected individuals:**

* Have affected individuals been notified?

(•) Yes ( ) No

Date notification began (or is planned):	30-Aug-2022
Date notification was completed:	30-Aug-2022

Method of notification used for affected individuals (Please select one of the options below):

Some individuals notified directly, some notified only indirectly

*** Describe the form of notification:**

(For example, this can include directly by letter, email, telephone; indirectly via newspaper announcement, etc.)

IMPORTANT: Do not include any identifying personal information.

Cornerstone has posted a general notice to its website.

Members are being contacted through email notification and electronic and paper banking statements to direct them to the Cornerstone website for more information about the incident. Cornerstone will use other channels as appropriate to connect with members (e.g. social media, online banking banner, etc.).

Please see attached for a form of the general notice posted to the website.

If possible, please attach a copy of the notification (or script of notification) and confirm if the notification conforms to the requirements stipulated in the Regulations.

If you have chosen to notify indirectly, describe the rationale for doing so as well as the type of indirect notification used (i.e. how it was delivered to the target audience}:

In some cases, Cornerstone does not have current contact information for impacted individuals. The variety of notifications and communications being used was determined to be the most effective way of reaching as many of the individuals who may have been impacted as possible.

Risk mitigation

*** Description of any steps (apart from notification to affected individuals) taken by the organization to reduce the risk of harm to affected individuals, or to mitigate that harm:**

For example, this can include:

- taking steps such as resetting passwords, offering credit monitoring services where appropriate, recovering misdirected information, seeking confirmation from unintended recipients that they have destroyed and not circulated the information; and
- notifying third parties or organizations that can reduce the risk of harm, such as the police, payment processors or credit card companies.

A number of steps have been taken including the following key examples:

- Dark web monitoring was conducted to monitor for evidence of misuse - no evidence has been found to date.

- Free credit monitoring is being offered to individuals that may have been impacted.

- Third parties were notified to assist in mitigating the harm including law enforcement and other privacy regulators (where relevant).

- Cornerstone has already implemented additional security measures and is working with Deloitte to determine if there any additional security safeguards that can be implemented to mitigate the risk of similar incidents in the future.

Description of any organizations and/or government institutions notified about the breach not mentioned above (for example, professional bodies or other privacy commissioners' offices):

Name of organization(s):

Date(s) notified:

See above. In addition, Cornerstone has notified the following organizations:
-Law Enforcement
-Credit Union Deposit Guarantee Corporation (CUDGC)
-Other privacy commissioners as relevant

Description of the steps taken to reduce the risk of a similar event occurring in the future:

For example:

- an experienced IT security firm has been hired to review the organization's security program and we are committed to making any recommended improvements;
- all new contracts with web service providers will include the following quality control provisions…,
- a privacy training module has been developed and is now mandatory for all staff;
- all laptops will be encrypted;
- software change management protocol has been updated; etc.

A number of steps have been taken including the following key examples:

- Free credit monitoring will be offered to individuals that may have been impacted

- Currently in the process of selecting a Managed Cyber Security Partner to complement our internal security team and provide additional cyber security scale. This will include:
  - Increased Managed Endpoint Detection & response (MDR)
  - Managed SEIM/SOAR
  - 24X7X365 Security Operations Centre (SOC)
  - Virtual CISO - Cyber Security Risk Management & Roadmap
  - Vulnerability Scanning
  - Dark Web Monitoring / Managed Risk
  - Continued Staff Cyber Security Training and phishing tests

- Managed Network Provider Improvements
  - Prioritizing security roadmap items like DLP (Data Loss Protection) and the NDR (Network Detect Respond) solution
  - Driving improvements to incident response processes and testing those improvements as an organization to validate them against real-world scenarios

- Improved managed network security by implementing improved branch firewalls at each of Cornerstone's locations and providing branch level Intrusion Detection & Prevention and Malware/antivirus Detection

- Upgraded Microsoft 365 Licensing –Upgraded all Microsoft 365 Licensing to E5 to take advantage of the highest level security features offered by Microsoft and E5 Defender suite
  - Started to implement Data Loss Prevention policies across platform to provide additional safeguards to protect Member Data.

- Upgraded Identity Management – Moved exclusively to Microsoft Azure Active Directory for Identity Management.
  - Implemented Multi Factor Authentication for all employees
  - Implemented Windows Hello biometric authentication
  - Implemented strong passwords (8 character minimum)
  - Added security policies including impossible travel..etc
  - Removed domain replication to Celero for Celero application authentication

- Microsoft Endpoint Manager – Elevated Endpoint Management Capabilities using Microsoft Endpoint Manager to manage all assets. This includes all workstations, laptops, mobile devices..etc.
  - Compliance policies implemented for all Endpoints including mobile
  - Patch Management
  - Workstation Bitlocker Encryption
  - Workstation Security Hardening

- Legacy Infrastructure – Taken the opportunity to eliminate legacy infrastructure that is no longer required

- Implemented DMARC to minimize risk of email spoofing

- Consultant completed security analysis on our new environment and we are actioning all outcomes

Please submit this form through one of the following means:

By Secure breach reporting portal:

Submit a privacy breach report
(We encourage all organizations to submit their breach report through our online secure breach reporting portal)

By postal mail or by hand:

PIPEDA breach response officer
Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, QC K1A 1H3

Should you require additional information about breach reporting requirements under PIPEDA, please see our office's guidance entitled What you need to know about mandatory reporting of breaches of security safeguards.

As previously communicated, Cornerstone Credit Union was recently impacted by a cybersecurity incident that was experienced by one of our managed service providers.

Please be assured that there is no evidence that any personal information was misused and key systems accessing member accounts, being our core banking and digital (online & mobile) banking were not affected, as well as communication channels such as email.

Out of an abundance of caution, we want to make our members aware that unknown individuals may have gained unauthorized access to some personal information as a result of this incident.

Cornerstone Credit Union takes the privacy and protection of your information extremely seriously.

Notification | FAQ

IMPORTANT MEMBER UPDATE

Notice of Cybersecurity Incident

Cornerstone Credit Union ("Cornerstone") takes the privacy and security of its members very seriously.

To that end, we want to provide an important update on a recent cybersecurity incident experienced by a managed services provider that offers a range of information technology and related services to Cornerstone. As previously communicated, the cybersecurity incident impacted Cornerstone and resulted in us commencing our own investigation and response to this incident, as set out further below.

What Happened

On June 8, 2022, the managed services provider notified us that they had experienced a cybersecurity incident. They confirmed that they took immediate action to block the incident to limit the impact on their clients and began investigating to assess what information may have been compromised.

Out of an abundance of caution, we also launched an investigation into this incident. From this investigation, we have implemented additional security measures to further protect your information.

What Information Was Involved

There is no evidence that any personal information was misused as a result of this incident, and given the immediate and comprehensive actions taken, we consider the risk to members low. Key systems to access member accounts, such as our core banking system and digital banking, as well as communication systems such as email, were unaffected. However, as a precautionary measure, we wanted to let you know that some of our employees' and members' personal information may have been accessed during the incident. For some members, this may include name, member number, account number, date of birth (DOB), or social insurance number (SIN).

What We Are Doing

We have alerted law enforcement and appropriate privacy commissioners and have engaged leading cybersecurity experts to support the investigation and our response.

As a precautionary measure, we wanted to notify you and also offer you **complimentary identity theft and credit monitoring solutions** free of charge for 24 months from TransUnion. Through this, you will be able to receive regular alerts to notify you if there are significant changes to your credit report.

If you would like more information on this incident and/or you are interested in this service, please send an email to memberfeedback@cornerstonecu.com or call 1.855.875.2255 to access it.

In order to protect against fraudulent access to credit report information, you will be subject to a verification and authentication process.

What You Can Do

While there is no evidence that any personal information was misused as a result of this incident, we always recommend that members take the following additional steps to protect yourself and your information online:

- Monitor your financial accounts with care. If you see any transactions you do not understand or that appear suspicious, or if you suspect fraudulent activity has occurred involving a credit or debit card, contact your financial institution.
- Regularly change and create strong passwords for any online accounts, particularly those that use or relate to your social insurance number.
- Be cautious of any unsolicited communication (phone call, email, etc.) that asks for your personal information or refers you to a Web page asking for personal information.
- Do not click on links or provide money or confidential information where you cannot independently verify the authenticity of a request.
- Clear your browsing history regularly and at the conclusion of any online banking or other transactions where you make online purchases.
- Sign up for banking alerts that will notify you when your password has been changed or your bank account has been accessed/used.
- Contact the appropriate authorities if you notice any suspicious activity.
- Sign up for the credit monitoring services being offered above.

Additional tips and resources for protecting your identity are available at: https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca03025.html

For More Information

We know you may have more questions, and we are here to support you. Please email memberfeedback@cornerstonecu.com or call 1.855.875.2255.

We take this incident, and the privacy and protection of your information, extremely seriously. We are profoundly grateful for your understanding and support, and we regret any impact this incident may have had.

Thank you for your trust and support.

Sincerely,

Doug Jones
CEO
Cornerstone Credit Union

INCIDENT FAQs

What happened?

On June 8, 2022, a managed services provider notified us that they had experienced a cybersecurity incident. They confirmed that they took immediate action to block the incident to limit the impact on their clients and began investigating to assess what information may have been compromised.

Out of an abundance of caution, we also launched an investigation into this incident. From this investigation, we have implemented additional security measures to further protect your information.

When did this incident occur?

On June 8, 2022, a managed services provider notified us that they had experienced a cybersecurity incident. They confirmed that they took immediate action to block the incident to limit the impact on their clients and began investigating to assess what information may have been compromised.

What type of incident was this?

It was a cybersecurity incident that originated within a managed service provider we contract with for information technology services.

Were you hacked / what was the impact of the incident?

We were impacted by a cybersecurity incident experienced by a managed services provider that offers a range of information technology and related services to Cornerstone.

How did you respond to the incident?

Out of an abundance of caution, we launched an investigation into this incident. From this investigation, we have implemented additional security measures to further protect your information.

We have alerted law enforcement and appropriate privacy commissioners and have engaged leading cyber security experts to support the investigation and our response.

While we have no evidence that personal information was misused as a result of this incident, out of an abundance of caution, we are also offering members and employees complimentary identity theft and credit monitoring solutions free of charge for 24 months from TransUnion. Through this, they will be able to receive regular alerts to notify you if there are significant changes to your credit report. If interested in this service, please send an email to memberfeedback@cornerstonecu.com or call 1.855.875.2255 to access it.

What is my risk?

There is no evidence that any personal information was misused as a result of this incident, and given the immediate and comprehensive actions taken, we consider the risk to members low.

What information was involved?

We have no evidence that member information was misused and given the immediate and comprehensive action taken, we consider the risk to members low. Key systems accessing member accounts being, core banking and digital (online & mobile) banking systems were not impacted, as well as communication channels such as email. However, for some members, some information may have been accessed including, name, member number, account number, date of birth (DOB), or social insurance number (SIN). If you would like to discuss this further, please email memberfeedback@cornerstonecu.com or call 1.855.875.2255.

What can I do to protect myself?

While there is no evidence that any personal information was misused as a result of this incident, we always recommend that members take the following additional steps to protect yourself and your information online:

- Monitor your financial accounts with care. If you see any transactions you do not understand or that appear suspicious, or if you suspect fraudulent activity has occurred involving a credit or debit card, contact your financial institution.
- Regularly change and create strong passwords for any online accounts, particularly those that use or relate to your social insurance number.
- Be cautious of any unsolicited communication (phone call, email, etc.) that asks for your personal information or refers you to a Web page asking for personal information.
- Do not click on links, provide money, or confidential information where you cannot independently verify the authenticity of a request.
- Clear your browsing history regularly and at the conclusion of any online banking or other transactions where you make online purchases.
- Sign up for banking alerts that will notify you when your password has been changed or your bank account has been accessed/used.
- Contact the appropriate authorities if you notice any suspicious activity.
- Sign up for the credit monitoring services being offered above.

Additional tips and resources for protecting your identity are available at:
https:/www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca03025.html

How do I access credit monitoring?

To access complimentary identity theft and credit monitoring solutions free of charge for 24 months from TransUnion, please send an email to memberfeedback@cornerstonecu.com or call 1.855.875.2255 to access it.

In order to protect against fraudulent access to credit report information, you will be subject to a verification and authentication process.

I am looking for more details on the incident – how can I find out more?

We know you may have more questions, and we are here to support you. Please contact email memberfeedback@cornerstonecu.com or call 1.855.875.2255.