



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:

Northern Savings Credit Union

Address of organization:

138 Third Ave. West  
Prince Rupert, BC V8J 1K8

\* 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: 12,500

Canadians affected:

Comments:

This is an approximate number based on what could have been accessed and is being included out of an abundance of caution. 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: 22-Dec-2021

End date of breach occurrence: 06-Jan-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 Northern Savings' insurer is CUMIS Group Ltd., Northern Savings' legal and breach counsel is MLT Aikins LLP, and Northern Savings' forensic and communications experts is Deloitte LLP. Northern Savings' key IT service providers with respect to the incident includes Central 1, CGI and Celero.

2. Based on the investigation to date, it appears that sophisticated email phishing campaigns using a spoofed domain name resulted in unauthorized access by unknown individuals to the email accounts of six Northern Savings employees. An investigation of the matter has not been conclusive as to what personal information was impacted during this time and so out of an abundance of caution Northern Savings is notifying all individuals who may be impacted to mitigate any potential risk to those individuals.

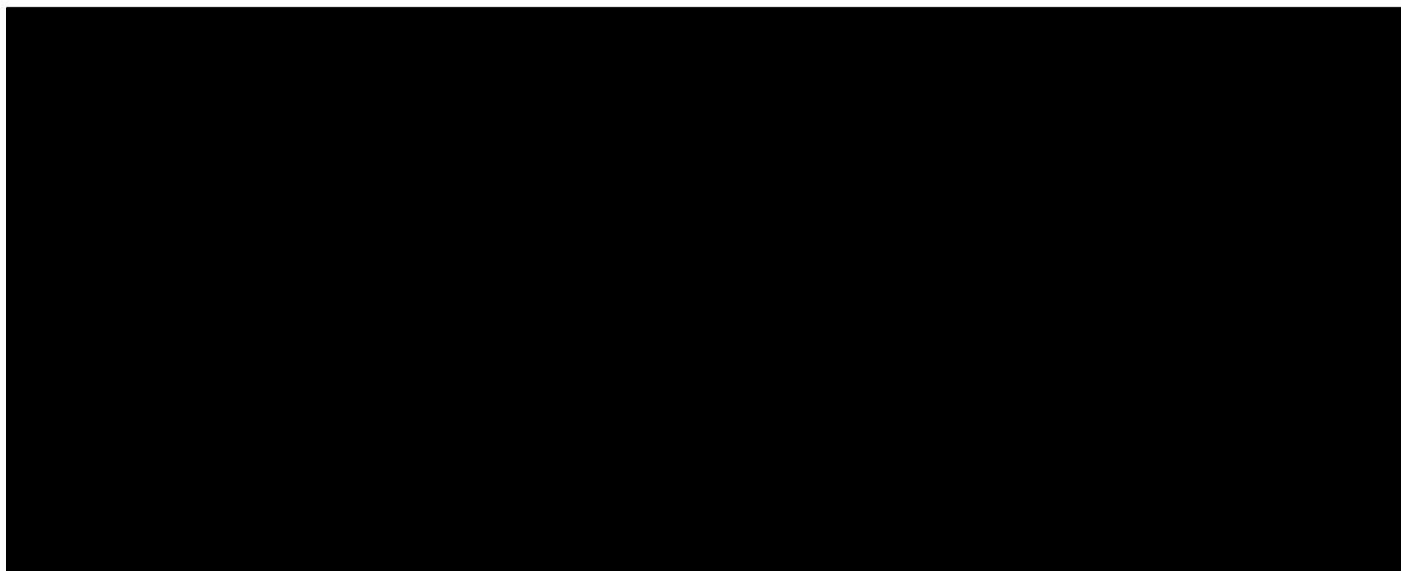
3. The incident was discovered on January 6, 2022 when recipients of the phishing emails reported them to Northern Savings.

4. The incident impacted employee email accounts and it is unclear where the unknown individuals are located.

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:**



**\* 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, non-members and employees of Northern Savings.

The information that may have been impacted differs depending on the individual but includes, for example, credit card information, SINS, identification information, account numbers, and contact information such as addresses and phone numbers. Some individuals may have additional information based on the nature of products they hold (for example, relating to their loans).

Additional information that may have been impacted for employees includes employment information such as income details and date of birth.



## 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):

06-Apr-2022

Date notification was completed:

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.

Northern Savings posted a general notice to its website when it discovered the phishing campaigns . Please see attached for a form of the notice that was posted to the website when the investigation was commenced.

Individuals who may have been impacted are being contacted through online banking, paper statements, and employee notifications to direct them to the Northern Savings website for more information about the incident. Please see attached for a form of the general notice to be posted to the website following the investigation at

<https://www.northsave.com/AboutUs/MediaCentre/FraudAwareness/EmailPhishing/>.



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, Northern Savings does not have or 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 most of the individuals who may have been impacted.

## 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:

- Passwords to accounts have been reset
- Password policies have been updated
- Updated training will be provided to all employees
- Dark web monitoring was conducted to monitor for evidence of misuse - no evidence has been found to date
- Free credit monitoring will be offered to individuals that may have been impacted
- Third parties were notified to assist in mitigating the harm including law enforcement, payment card providers/ credit card companies (where relevant), and other privacy regulators (where relevant).
- Northern Savings has implemented and is working with Deloitte to implement a number of additional security safeguards to mitigate the risk of similar incidents in the future
- A privacy assessment will be conducted to mitigate the risk of similar incidents in the future
- Northern Savings has taken steps to recover two spoofed/ squatted domains and to protect against 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, Northern Savings proactively notified the Office of the Privacy Commissioner of Canada (OPC) and the Office of the Information and Privacy Commissioner for British Columbia (OIPC) about the incident on February 15, 2022.

**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.



**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, 1<sup>st</sup> 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](#).

## Website Landing Page Content - Posted Wednesday, April 6

We identified an email phishing incident on January 6, 2022, that impacted six internal email accounts.

Upon discovery, we immediately initiated our standard incident response processes - rapidly shutting down access, introducing strengthened security measures, and bringing on external experts to support an investigation.

The incident was contained, and email systems are secure, with all operations running smoothly. As a precaution, the investigation continues, and we will provide further updates as necessary.

Out of an abundance of caution, we wanted to share that some personal information may have been accessed during the incident. This may include your account information, debit or credit card number, SIN, identification, and other financial information.

We took immediate and comprehensive action, including enabling multi-factor authentication, resetting employees' passwords, and blocking the malicious sender emails and/or domains identified during the incident. We will continue to take all reasonable steps to minimize any risks to you arising from the incident. Further, please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident, at this time.

In addition to the above, Northern Savings has reported the incident to law enforcement, appropriate privacy commissioners, and other organizations who can assist with mitigating any risks from the incident. Northern Savings has also implemented several additional safeguards to minimize risks to your information going forward.

Given the immediate and comprehensive actions already taken we consider the risk to members low. However, as a precautionary measure, Northern Savings is offering impacted members identity theft and credit monitoring solution free of charge for two years. To sign up for this service please send an email to [inquiries@northsave.com](mailto:inquiries@northsave.com) or call us at 250.628.0256 or toll-free at 877.656.9505. There are additional things we recommend you do to protect yourself and your online information:

- Use strong passwords - alphanumeric in nature (a combination of both upper and lowercase letters as well as numbers and special characters).
- Change your passwords regularly.
- 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 banking account has been accessed/used.
- Do not click on links, provide money, or confidential information where you cannot independently verify the authenticity of a request.

Thank you for your trust and support.

If you have any immediate questions or concerns, please contact: [inquiries@northsave.com](mailto:inquiries@northsave.com)

## Website Q&A - Posted Wednesday, April 6

### 1. What steps has Northern Savings taken to strengthen its email systems? How can you prevent this from happening again?

Below are some of the changes that we have implemented to best protect your information by strengthening our information security program:

- Northern Savings has reported the incident to law enforcement, appropriate privacy commissioners, and other organizations who can assist with mitigating any risks from the incident. Northern Savings has also implemented several additional safeguards to minimize risks to your information going forward.
- We have engaged third-party experts to objectively evaluate and make recommendations for

further process enhancements.

- We continue to monitor the dark web and other online locations. To date, no public disclosure of customer data from the attack has been identified.
- We have implemented strengthened cybercrime detection technology across the organization.
- Our teams, organization-wide, have/will participate in annual security and privacy awareness and training programs.

## **2. What services are you offering to protect my information/data?**

If you are or were a member or an employee of Northern Savings, some of your information in our e-mail system may have been accessed as a result of this incident. In particular, this may include your account information, debit or credit card number, SIN, identification, and other financial information.

There is no evidence of any public disclosure or misuse of your information. However, out of an abundance of caution, we are notifying you of the incident and as a precautionary measure, Northern Savings is offering identity theft and credit monitoring solutions free of charge for two years. To sign up for this service please send an email to [inquiries@northsave.com](mailto:inquiries@northsave.com) or call us at 250.628.0256 or toll-free at 877.656.9505.

## **3. What happened?**

We identified an email phishing incident on January 6, 2022. We initiated standard incident response processes, rapidly shutting down access, introducing strengthened security measures, and bringing on external experts to support an investigation. The incident was contained, and email systems are secure, with all operations running smoothly. As a precaution, monitoring continues, and we will provide further updates as necessary.

## **4. Is my information safe now?**

We took immediate and comprehensive steps, and we will continue to take all reasonable steps to minimize any risks to you arising from the incident. Further, please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident at this time.

## **5. Is the issue contained? Are you sure that any other systems haven't been compromised?**

Yes, the issue has been contained. With the help of best-in-class cyber security experts, we are implementing further safeguards to protect your information and reduce the risk of future incidents. Please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident at this time.

## **6. Should I change my password to my online banking account and app?**

Our investigations indicate that our online banking portals and internal systems were not impacted by this incident. However, as best practice, there are additional things we recommend you do to protect yourself and your online information:

- Use strong passwords - alphanumeric in nature (a combination of both upper and lowercase letters as well as numbers and special characters).
- Change your passwords regularly.
- 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 banking account has been accessed/used.
- Do not click on links, provide money, or confidential information where you cannot independently verify the authenticity of a request.

## **7. How do I get in contact with a privacy commissioner to learn about my rights?**

While you are entitled to file a complaint with the privacy commissioner, we have already notified them of this incident. Those who have questions about their rights can learn more by contacting the

privacy commissioner in their respective jurisdiction.



## Email Phishing Notification

### January 2022 - Email Phishing

Northern Savings has recently learned of email phishing scams that we wish to make you aware of. The scams attempt to lure individuals to provide personal information. For example, some emails have the subject line "NSCU RFP 2022" and are attempting to impersonate current and former employees of Northern Savings.

Please be advised that these emails were not generated from an official Northern Savings email domain and did not come from Northern Savings employees.

If you have received one of these emails:

- If you have received a phishing email (the content may vary slightly) you should DELETE IT IMMEDIATELY.
- Do not click on any links or open any attachments.
- Do not provide any data or information.
- If you have clicked on a link or provided information (e.g., personal or company usernames or passwords) please change those usernames or passwords immediately (or ask your IT department to do so).

Northern Savings takes information security very seriously and we are investigating the matter and will provide an update should one be warranted.

If you have any immediate questions or concerns, please contact: [inquiries@northsave.com](mailto:inquiries@northsave.com)

**Northern Savings will never send you an email or text asking you for private information such as passwords or login credentials.**

### What is phishing?

You may get an email or text that looks like it's from a real company. It could ask you for private information, such as your date of birth, passwords, login credentials, or credit card details. Sometimes the email will tell you to visit a fake website.

### What to do if you suspect phishing?

If you get this kind of email or text, don't click on any links or give any information about yourself. If you have any doubts about where the email came from, make sure to check the identity of the sender by looking up their company phone number or website. Do not call or email the sender using the contact information contained in the email.

[Learn more about fraud awareness](#)

## Phishing and smishing





## Fraud Awareness

As COVID-19 continues to spread globally, watch out for associated scams. Fraudsters want to profit from consumers' fears, uncertainties and misinformation. Fraudsters are exploiting the crisis to facilitate fraud and cyber-crime.

**Northern Savings will never send you an email or text asking you for private information such as passwords or login credentials.**

[Email Phishing Notification](#)

### Email Scams - Phishing

You may get an email that looks like it's from a real company. It could ask you for private information, such as your date of birth, passwords, login credentials, or credit card details. Sometimes the email will tell you to visit a fake website.

If you get this kind of email, don't click on any links or give any information about yourself. If you have any doubts about where the email came from, make sure to check the identity of the sender by looking up their company phone number or website. Do not call or email the sender using the contact information contained in the email.

### Watch Out For...

- Spoofed government, healthcare or research information
- Unsolicited calls, emails and texts giving medical advice or requesting urgent action or payment - if you didn't initiate contact, you don't know who you're communicating to
- Suspicious links and attachments (never respond or click on these)
- Never give out your personal or financial details
- Unauthorized or fraudulent charities requesting money for victims, products or research - don't be pressured into making a donation/verify that a charity is registered
- High-priced or low-quality products purchased in bulk by consumers and resold for profit
- CRA through texts that encourage the receiver to click on a link to access an emergency benefit. CRA NEVER uses texts to communicate. Delete the text immediately as the link harbours malware.

If you are a victim of fraud or think your personal financial information may have been compromised, [contact us immediately >](#)

### Reported Scams

Fraudsters have been reported as posing as:

- Cleaning or heating companies - offering duct cleaning services or air filters to protect from COVID-19
- Local and provincial hydro/electrical power companies - threatening to disconnect your power for non-payment
- Centers for Disease Control and Prevention or the World Health Organization - offering fake lists for sale of COVID-19 infected people in your neighbourhood
- Public Health Agency of Canada - giving false results saying you have been tested positive for COVID-19 tricking you into confirming your health card and credit card numbers for a prescription
- Red Cross and other known charities - offering free medical products (e.g. masks) for a donation
- Government departments - sending out coronavirus-themed phishing emails tricking you into opening malicious attachments tricking you to reveal sensitive personal and financial details
- Financial advisors - pressuring people to invest in hot new stocks related to the disease, offering financial aid and/or loans to help you get through the shut downs
- Door-to-door sales people - selling household decontamination services
- Private companies - offering fast COVID-19 tests for sale. Only health care providers can perform the tests, no other tests are genuine or guaranteed to provide accurate results

## Protect Yourself From Digital Fraud & Scams



### Trusted Websites and Resources

- [Canadian Anti-Fraud Centre](#)
- [RCMP Cybercrime Unit](#)
- [Reporting Cyber Fraud](#)
- [Canadian Centre for Cybersecurity](#)