Data Safety in Alberta

The Serious Problem created
by Alberta Republicans sharing
Private Information Publically

and what you need to do
now to protect yourself

CFTG.CA

RADIO FREE CANADA

If you believe your information is being misused, report it to the Canadian Anti-Fraud Centre:

- **Phone:** 1-888-495-8501
- **Online:** antifraudcentre-centreantifraude.ca

Keep the reference number. It creates an official record that can support future fraud claims with your bank, credit bureau, or police.

How ALL Albertans are now at risk

Danielle Smith did this... because our Constitution effectively blocked the referendum question and protected us - so Danielle Smith used the Notwithstanding clause to override the Constitution and keep the hate going.... Darin Howard - Editor
The Article:

The moment this database went live, automated systems started finding it.

Not hackers in hoodies just regular web crawlers, search engines, security scanners, and data brokers doing what they do. Within hours, someone somewhere had downloaded the whole thing. Maybe multiple someones. By the end of day one, copies existed in places the original owners didn't even know about.

Within 24 hours, that data was getting cleaned up, sorted, and matched against other leaked databases phone numbers, emails, birth dates, property records, social media profiles. Your "voter list" entry became part of a full profile.

Within a day or two, copies were moving through private channels. Group chats. Telegram channels. Scammer forums. Invite-only marketplaces. The dark web. The data doesn't stay in one place. It fragments and spreads like dandelion seeds.

By day three, fraudsters were already capable of using it. Fake government notices that know your real name and address. Bogus Elections Alberta follow-ups. Banking scams. Phishing that references your actual voter registration. Identity verification scams. Intimidation. Harassment. Stalking.

Within a week, sophisticated actors didn't need the whole database anymore. They could pull out specific vulnerable groups. Seniors living alone. Rural residents far from police help.

People with unusual names who are easier to impersonate. Political donors. And most chillingly domestic violence survivors, protected witnesses, anyone trying to keep their location hidden. Their addresses are now exposed.

After that first week, this becomes nearly impossible to undo. You can take down the original website.

You can't claw back every copy, screenshot, mirror, spreadsheet, or resale. The information persists. It gets sold, traded, and reused for years.

Dean Blundell

Substack.

How to protect yourself and everyone else

Contact and location data cannot be replaced. **Your name, home address, and phone number are fixed identifiers.** They do not expire. And they are the inputs that make fraud, impersonation, phishing, and account-takeover attacks more effective.

Someone with access to your name, address, and phone number can:

- Construct a convincing impersonation of your bank, phone carrier, CRA, or a government office
- Use your details to answer identity-verification questions on account-recovery processes
- Attempt a SIM-swap, redirecting your phone number to a device they control in order to receive your verification codes
- Apply for credit in your name
- Contact you in ways you have not consented to

People whose home address being known creates a personal safety risk — including domestic violence survivors and others who keep their location private — face specific and serious consequences from this exposure.

The steps below address these risks directly.

Step 1: Apply verification discipline to all unsolicited contact

Do not confirm personal information, click links, or act on instructions from any unsolicited contact — calls, texts, or emails — claiming to be from your bank, CRA, Elections Alberta, Service Canada, or any government or financial institution.

If you receive such contact, end it and call back using a number from the organization’s official website or the back of your card — not a number provided in the message.

Watch for:

- Messages claiming to be from Elections Alberta or CRA asking you to verify your identity
- Unexpected password-reset emails or one-time codes you did not request
- Calls or messages referencing your address or other personal details to establish credibility
- Any contact that creates pressure to act immediately

Step 2: Protect your phone number

Contact your phone carrier and request:

- **Port protection or a number lock** on your account, which adds a verification step before your number can be transferred to another carrier. The name of this feature varies by carrier — Telus calls it port protection and will send you a text confirmation before any port is processed; Rogers operates a similar confirmation process. Ask your carrier what they offer and have it added to your account.
- A **verbal PIN or account passcode** so that no account changes can be made without it.

These two measures reduce the risk of a SIM-swap, where someone transfers your phone number to a SIM card they control in order to intercept verification codes sent to your number.

Step 3: Secure your accounts, starting with email

Your email account is one of the highest priorities. Access to your email typically allows an attacker to reset credentials on your bank, financial accounts, and most other services.

For your email account and all other important accounts:

- Set a **strong, unique password** on each account. If you reuse passwords across accounts, change them. A password manager makes this practical — search “free password manager” to find options.
- Enable **two-factor authentication** using an **authenticator app** rather than a code sent to you by text message. If someone has taken over your phone number, text-based codes go to them, not you. Search “authenticator app” to find options.
- Review the **active login sessions** on your email and financial accounts. Revoke any sessions from devices or locations you do not recognize.

Step 4: Place fraud alerts with both credit bureaus

A fraud alert or identity alert tells lenders there may be fraud risk and asks them to verify your identity before approving credit. Credit grantors may still exercise discretion.

In addition to a fraud alert, you may choose to place a credit freeze or credit lock on your file. This restricts access to your credit report, making it significantly harder for new credit accounts to be opened in your name without your authorization.

In Canada, availability and terminology vary by bureau:

- TransUnion Canada offers a credit freeze option that limits access to your credit file until you choose to lift or manage it
- Equifax Canada must be contacted separately to apply its equivalent protections or restrictions

A credit freeze is more restrictive than a fraud alert. It may affect your ability to apply for new credit, rent housing, or complete identity checks until it is temporarily lifted. Consider this option if you want a higher level of control over how your credit information is accessed.

Step 5: Pull your credit reports and review them

You are entitled to a free credit report from both Equifax and TransUnion.

Request them and look for:

- Accounts you did not open
- Credit inquiries you did not authorize
- Address changes you did not make

If you find anything you cannot account for, file a police report and document everything. Some fraud victim designations and stronger protective measures require a police report number.

Step 6: Report suspected fraud to the Canadian Anti-Fraud Centre

If you believe your information is being misused, report it to the Canadian Anti-Fraud Centre:

- **Phone:** 1-888-495-8501
- **Online:** antifraudcentre-centreantifraude.ca

Keep the reference number. It creates an official record that can support future fraud claims with your bank, credit bureau, or police.

If your personal safety is at risk

If you are a domestic violence survivor, if you keep your address private for safety reasons, or if your location being known creates a specific risk for you, take the following additional steps:

- Contact your bank, phone carrier, and relevant services and ask them to require additional identity verification before any changes are made to your accounts
- Consider a secondary phone number for public-facing contact. Apps such as Google Voice or a prepaid SIM provide a layer of separation.
- Review your social media privacy settings and restrict anything that discloses your location or daily patterns
- Inform trusted people in your life — family, employer, support workers — so they are aware of the situation
- If you believe you face immediate risk, contact local police and document your concerns in writing, including dates and specific details

Monitoring window

The risk from this breach does not resolve in the coming weeks. Contact and location data remains usable over time, particularly when combined with information from other sources.

Check your credit reports again at three months, six months, and twelve months.

Review your account login histories periodically.

Remain alert to phishing attempts for at least the next 12 to 24 months.

Quick reference checklist

- ☐ Verification discipline applied to all unsolicited contact
- ☐ Port protection and account PIN added with your phone carrier
- ☐ Email account secured with strong, unique password and authenticator-app two-factor authentication
- ☐ Active login sessions reviewed on key accounts
- ☐ Unique passwords set on all important accounts
- ☐ Fraud alert placed with Equifax Canada — call 1-800-465-7166
- ☐ Fraud alert placed with TransUnion Canada — call 1-800-663-9980 or transunion.ca
- ☐ Credit reports pulled and reviewed from both bureaus
- ☐ Suspicious activity reported to the Canadian Anti-Fraud Centre: 1-888-495-8501
- ☐ Additional safety steps taken if personal safety is at risk

Check out the Factsmtr Civic Action Learning Series. Skills and Strategies for Real-World Change. Available to ***paid subscribers.***

Sources

Elections Alberta — official statements on the breach

- Initial statement
- Updated statement
- Chief Electoral Officer message to Albertans

Office of the Information and Privacy Commissioner of Alberta

- Statement on jurisdiction and risk to Albertans — CBC News, May 1, 2026

Government of Canada — credit reports and fraud alerts

- Credit reports and fraud alerts — Canada.ca

Steps to Justice — fraud alert process in Canada

- How to place a fraud alert with a consumer reporting agency

Canadian Anti-Fraud Centre

- Canadian Anti-Fraud Centre
- SIM swap fraud guidance

Edmonton Police Service — SIM swap fraud guidance

- SIM Swap Fraud — Edmonton Police Service