Identity Protection Checklist

Are your personal information, accounts, and records properly protected?

Name or household: _____ Date: _____

Next review: _____

Where to begin

An unfamiliar charge, missing statement or unexpected login alert deserves a closer look. This checklist helps you protect your information, recognize warning signs and know whom to contact.

Use it once a year, or after a lost wallet, data breach or suspicious account activity. If fraud is happening now, contact the affected institution promptly.

How to use this checklist

• Work through the sections that apply to you. Involve family members where needed.

• Tick an item once you've reviewed it and can answer it. Circle anything that's unclear or needs attention.

• Choose one priority and one question to address next. You don't have to settle everything at once.

Keep your information private

Don't record account or policy numbers, passwords, identification details or medical information here. Keep the completed checklist in a secure place.

I help people make clearer decisions today, before life forces harder ones later.

© 2026 David D. Seemungal. All rights reserved.

1 Warning signs you should not ignore

A small inconsistency may be the first sign that personal information is being misused.

☐	A credit inquiry appears that I don't recognize.
☐	A new credit, loan, phone, utility, or service account appears that I didn't open.
☐	My credit score changes suddenly and I can't explain why.
☐	I receive a bill, collection notice, approval, or rejection for something I never applied for.
☐	I receive a login alert, password reset, or one-time code that I didn't request.
☐	An address, phone number, email address, or security setting changes without my approval.
☐	Expected mail, statements, replacement cards, or government correspondence stop arriving.
☐	My bank, credit card, tax, benefits, mobile-phone, or online account shows unfamiliar activity.
☐	A financial institution or service provider contacts me about information I didn't submit.
☐	Someone tells me my information was exposed, lost, stolen, or found in a data breach.

Why this matters

Identity theft doesn't always begin with a dramatic event. The first warning sign is often small, easy to dismiss, or mixed in with legitimate activity.

What needs attention: _____

2 Everyday digital protection

☐	I use a different strong passphrase for each important account.
☐	I use a reputable password manager instead of reusing or memorizing many passwords.
☐	Multi-factor authentication is turned on for email, banking, government, cloud, and social accounts where available.
☐	My phones, computers, browsers, apps, and security software are kept up to date.
☐	I don't share passwords, PINs, or one-time security codes, even when a message sounds urgent.
☐	I verify unexpected requests using a trusted phone number, app, or website that I found independently.
☐	My recovery email addresses, phone numbers, and backup methods are current and secure.
☐	My devices lock automatically, and sensitive activity is avoided on unsecured public networks.

What needs attention: _____

© 2026 David D. Seemungal. All rights reserved.

3 Financial and credit habits

☐	I review bank and credit-card transactions regularly, not only at month-end.
☐	Transaction, login, and account-change alerts are turned on where available.
☐	I know how to obtain and review my credit information from both Equifax Canada and TransUnion Canada.
☐	My financial institutions and credit bureaus have my current contact information.
☐	I understand that credit monitoring may help detect changes, but can't prevent every problem.
☐	I contact the institution promptly when I see a transaction, inquiry, or account I don't recognize.
☐	I investigate even small unfamiliar charges because they can be used to test whether an account is active.
☐	I keep copies of important correspondence and note the date, time, name, and reference number for important calls.

What needs attention: _____

4 Protecting key accounts and documents

☐	My primary email account has a unique password and multi-factor authentication because it can reset other accounts.
☐	My mobile-phone account has a secure PIN or other protection against unauthorized changes.
☐	My tax, government, benefits, and health-related online accounts are protected and reviewed periodically.
☐	Passports, birth certificates, Social Insurance Number records, and other identification are stored securely.
☐	I shred or securely destroy personal and financial documents before disposal.
☐	I collect mail regularly and update financial institutions and service providers promptly when I move.
☐	I have a private list of the cards and identification normally kept in my wallet, without recording passwords or PINs.
☐	I ask why my Social Insurance Number or other sensitive information is needed and how it will be protected before providing it.
☐	A trusted person knows where to find emergency contact information if I need help responding.

What needs attention: _____

© 2026 David D. Seemungal. All rights reserved.

5 If information may have been exposed

A data breach or suspicious message doesn't always lead to identity theft. The response should match what may have been exposed.

☐	I've identified what information may have been exposed, such as an email address, password, card number, identification, or Social Insurance Number.
☐	I changed affected and reused passwords from a trusted device, starting with email and financial accounts.
☐	I secured my mobile-phone and email accounts before using them to recover other accounts.
☐	I contacted the affected institution through an official app, website, statement, or trusted phone number.
☐	I reviewed recent logins, transactions, forwarding rules, contact details, and account settings.
☐	I'm watching for follow-up scams that refer to the breach or pretend to offer recovery help.
☐	I've kept the breach notice, suspicious message, screenshots, dates, and reference numbers.
☐	I've considered whether additional credit alerts or monitoring are appropriate for the information involved.

Secure the accounts that unlock other accounts first

Secure the accounts that can unlock other accounts first. For most people, that means email, mobile phone, banking, and government access.

What needs attention: _____

6 If identity theft or fraud is confirmed

☐	I contacted the affected bank, creditor, payment provider, or service provider immediately.
☐	Affected cards, credentials, or accounts were blocked, replaced, or secured as appropriate.
☐	I contacted both Equifax Canada and TransUnion Canada, reviewed my files, and asked about fraud alerts or warnings.
☐	I disputed inaccurate accounts, inquiries, addresses, or other information through the appropriate organization.
☐	I reported the incident to local police and kept the file number for future reference.
☐	I reported the fraud or cybercrime through the Canadian national reporting system.
☐	I notified the relevant government department if tax, benefits, Social Insurance Number, passport, or other government information was involved.
☐	I kept a written record of every report, conversation, letter, deadline, and follow-up step.
☐	I didn't agree to pay or acknowledge an unfamiliar debt until I verified it and requested supporting information.

What needs attention: _____

© 2026 David D. Seemungal. All rights reserved.

7 Household and family readiness

☐	We've discussed common impersonation, account, investment, romance, grandparent, and emergency-message scams.
☐	Family members know to pause and verify urgent requests for money, passwords, codes, or personal information.
☐	We have a trusted way to confirm unusual family requests, such as calling back on a known number or asking a private question.
☐	Older relatives, teenagers, and anyone who may need support know whom to contact before acting on a suspicious request.
☐	We don't send identification, account details, or private documents through unsecured messages unless necessary and verified.
☐	We understand that a caller ID, email address, logo, voice, photograph, or video can be copied or manipulated.
☐	We know where to find reliable legal, financial, credit, and identity-restoration help if a problem occurs.
☐	No family member is expected to manage a serious identity problem alone.

What needs attention: _____

8 Build a simple recovery record

Good records can make disputes and follow-up easier. Keep the details in a secure place, not on this public-facing checklist.

☐	A list of affected institutions, accounts, documents, or services.
☐	Dates and approximate times when suspicious activity was first noticed.
☐	Copies of letters, emails, texts, screenshots, statements, and breach notices.
☐	Names or employee numbers for people contacted, plus case or reference numbers.
☐	Police and national fraud-reporting reference numbers, where applicable.
☐	Dispute deadlines, replacement dates, promised follow-up dates, and unresolved items.
☐	A brief record of losses, fees, missed time, and other consequences.
☐	A reminder to review credit files and affected accounts again after the immediate problem appears resolved.

Don't make the recovery file a new risk

Store it securely. Avoid keeping full passwords, PINs, one-time codes, or unnecessary copies of sensitive identification in the same place.

What needs attention: _____

© 2026 David D. Seemungal. All rights reserved.

Questions worth discussing

1. Which account or document would create the most disruption if it were compromised?
2. Which email address or mobile number can be used to reset our other important accounts?
3. Would we recognize the warning signs early, or are we relying on someone else to notice them?
4. Do we know exactly whom to contact and what to record if fraud is discovered?
5. Who in our family or business may need help understanding or responding to a suspicious request?

Choose one next step

Start with the issue you most need to clarify.

The issue I want to review

_____

One question I need answered

_____

Who needs to be involved

_____

My next action and target date

_____

Official starting points

Canadian Anti-Fraud Centre: centreantifraude.ca

Report Cybercrime and Fraud: reportcyberandfraud.canada.ca

Equifax Canada: equifax.ca/personal

TransUnion Canada: transunion.ca

Get Cyber Safe: getcybersafe.gc.ca

How I can help

Send me the one question this checklist raised. I can help you identify protection resources and the questions to take to the affected institution, a lawyer or a credit or technical specialist.

David D. Seemungal, EPC | Senior Insurance and Investment Advisor

Elder Planning Counselor | VFG Financial Group

416-716-4675 | david@davidseemungal.ca | davidseemungal.ca

I help people make clearer decisions today, before life forces harder ones later.

For education and discussion. This checklist does not replace legal, financial, credit, cybersecurity or identity-restoration advice. Contact the affected institutions and the appropriate professionals for guidance. Procedures and contact details can change.

© 2026 David D. Seemungal. All rights reserved.