Protecting Seniors from Financial Harm

Rob Paddick & Grace McSorley

June 5, 2025

OBSI OMBUDSMAN FOR BANKING SERVICES AND INVESTMENTS
OSBI OMBUDSMAN DES SERVICES BANCAIRES ET D'INVESTISSEMENT

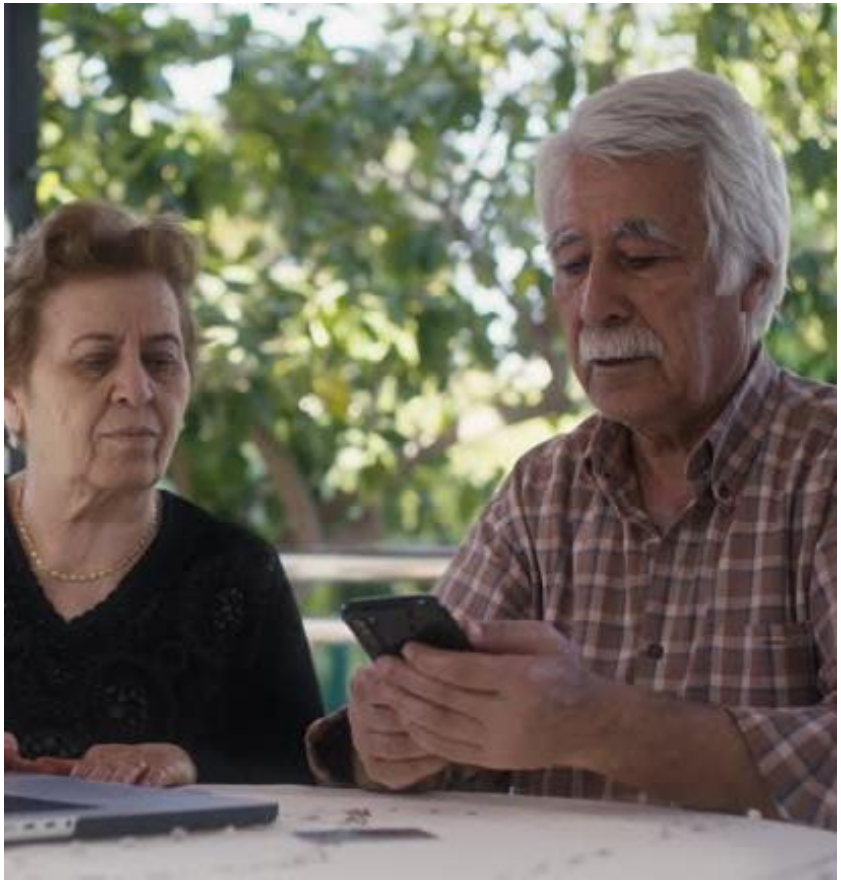
Agenda

- OBSI Overview
- Cases involving seniors
  - E-transfer Fraud
  - Credit Card Fraud
  - Debit Card Fraud
  - Crypto Fraud
- How to protect yourself
  - Powers of Attorney
  - Trusted Contact Person
  - Office of the Public Guardian and Trustee
- Q & A

OBSI Overview

- OBSI is Canada's national, independent, not for profit dispute-resolution service for consumers and small businesses with a complaint they can't resolve with their banking services or investment firm.
- OBSI is overseen by an independent Board of Directors. A majority of the directors are from the community, having not been part of industry or government for at least two years. OBSI's board also has dedicated positions for three industry-affiliated directors and three Consumer Interest Directors.

Seniors & OBSI

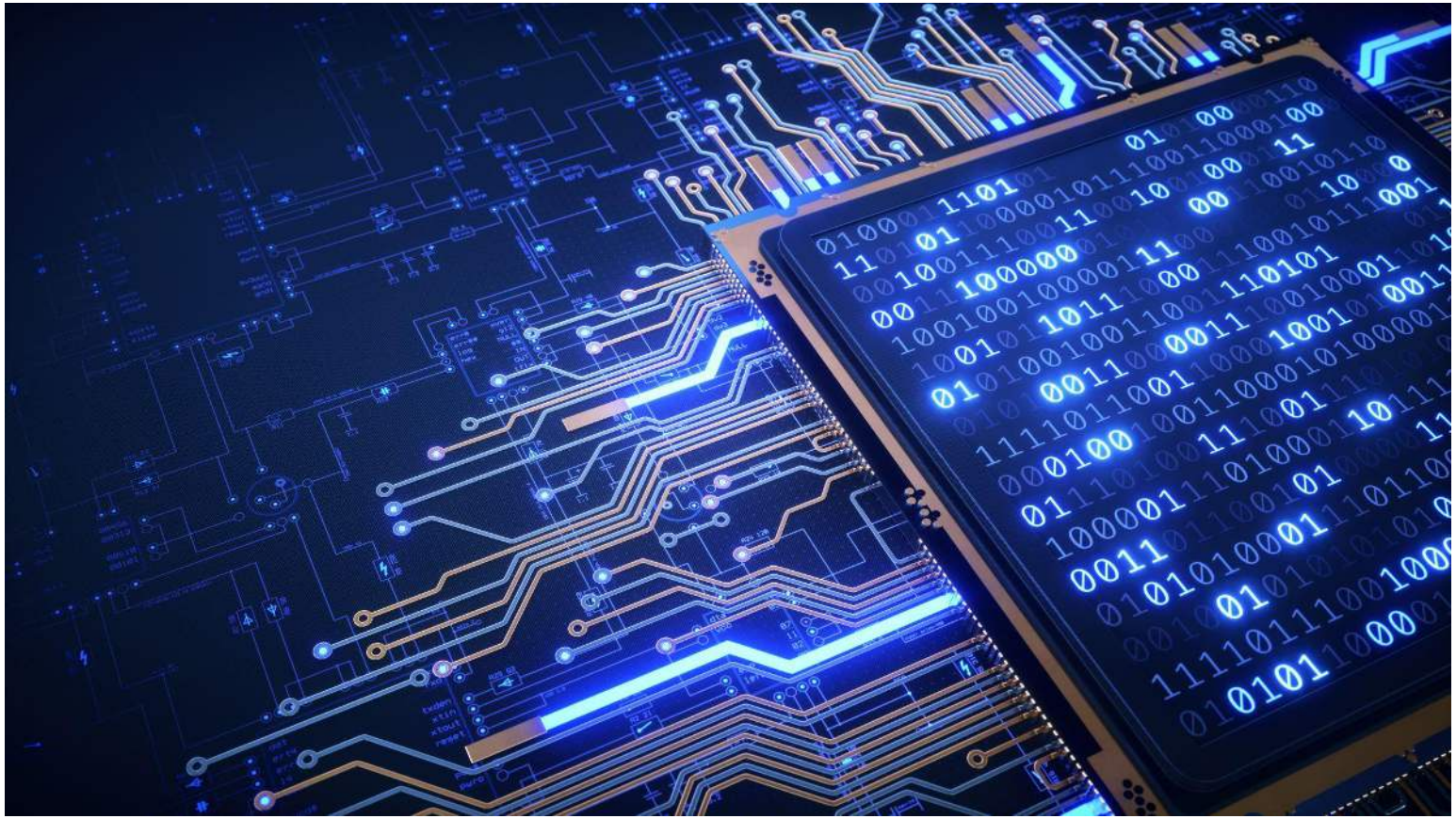


- Seniors are a core group of users of OBSI's services who have unique issues
- 32% of banking complaints and 40% of investment complaints were from consumers 60+ in 2024
- This is higher than the proportion of Canadians who are seniors (30%)
- Some seniors are vulnerable – may have reduced capacity, disabilities

OBSI staff are well-positioned to work with seniors

- Are trained on working with seniors
- Respond to calls in a timely manner
- Are alert to identifying vulnerabilities
- Help seniors articulate their complaints
- Consumer can have an authorized representative assist them

Fraud case examples



Text Message Scam

- Ms. V got a text message
- It was her “phone company”
- It said they were giving her a refund
- She clicked on the link and followed instructions to select her bank and log on
- Later, she was notified that a $3,000 e-transfer was accepted by an unknown recipient

Text Message Scam

- Ms. V contacted the bank and complained
- The bank did not compensate Ms. V because the transaction was completed using her confidential banking information

Text Message Scam

- We reviewed the evidence in the case
- We interviewed Ms. V to get her story
- We looked at the account agreement
  - It says the bank is allowed to rely on instructions received from a person with the consumer's confidential banking information
- The bank gave us evidence showing:
  - The consumer's confidential banking information and a one-time password (OTP) was used to complete the e-transfer
  - The transaction was made from a known / trusted device
- We did not recommend compensation because the bank:
  - followed its agreement with the consumer which says it can act on instructions given using the consumer's confidential banking information
  - it did not miss an opportunity to warn her

“Friendly” Fraud

- Ms. G, an 82-year-old woman, gave her credit card to a trusted friend to help her pay her expenses
- The friend misused her credit card over a three-year period, accumulating around $75,000 in unauthorized charges and cash advances
- She wasn’t checking her statements so she didn’t notice the charges

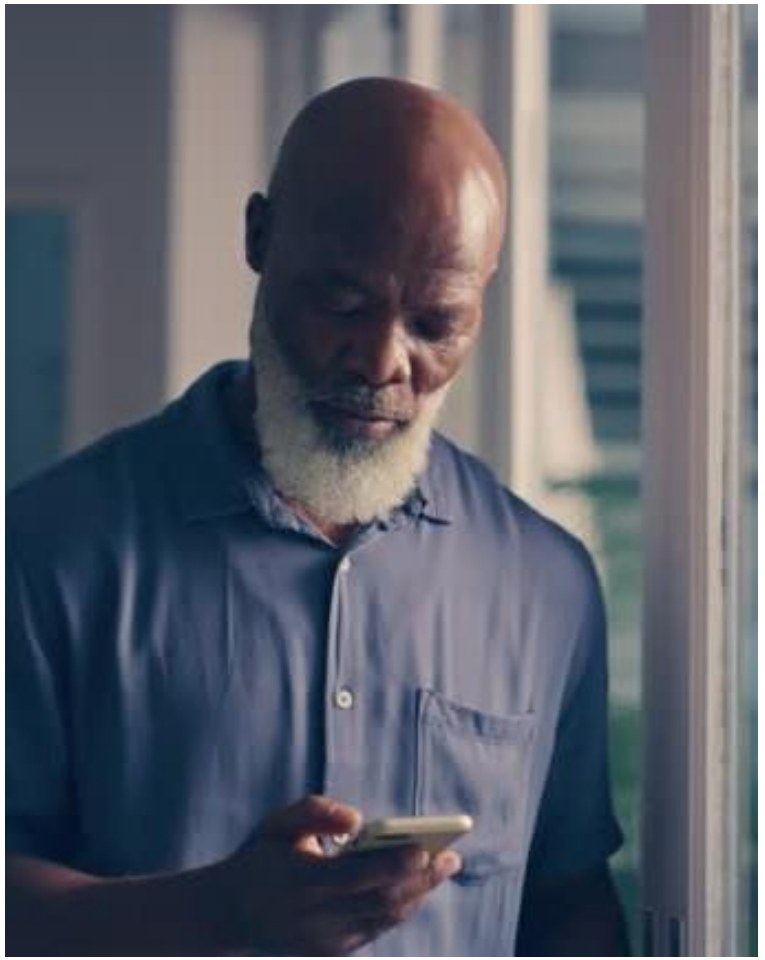
“Friendly” Fraud

- Credit card agreements say consumers must
  - protect their cards and confidential information
  - verify their transactions within a certain period of time or else they are deemed to have agreed to them*

*so review your statements each month

Fake Fraud Investigation Scam

- Mr. B got a call from his “bank”
- The phone number that appeared on his phone was his bank’s number and had the name of his bank
- The person on the phone knew a lot of information about him
- The caller told him he had been defrauded and they needed his help to protect his account



Fake Fraud Investigation Scam

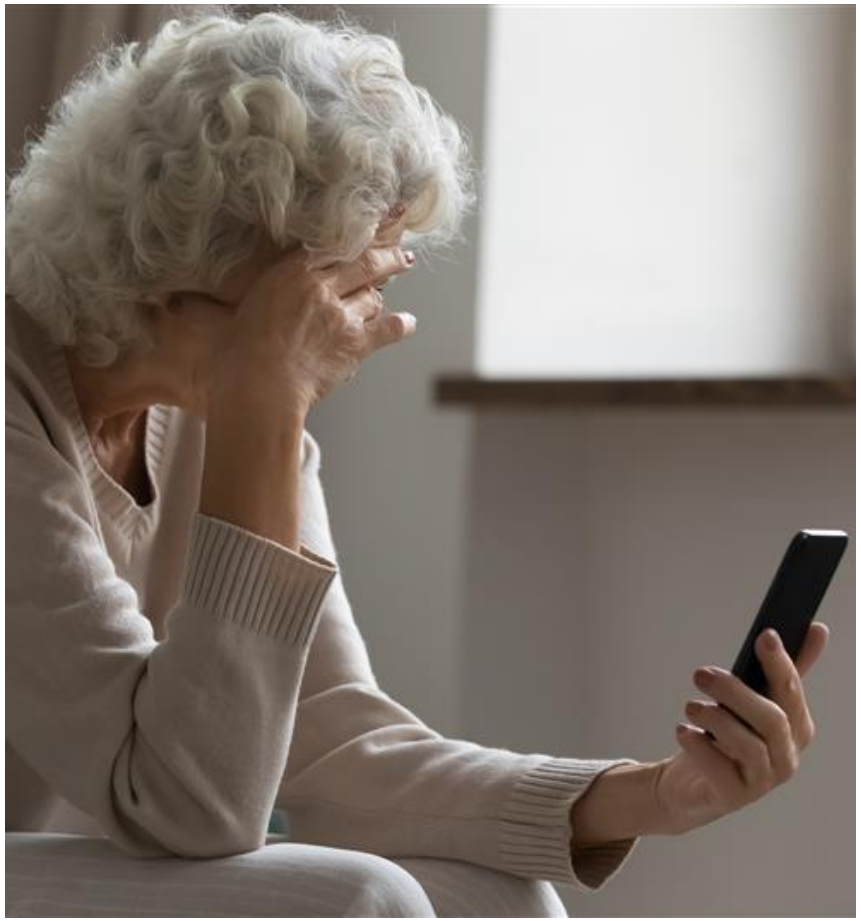
- The caller told Mr. B to:
  - log onto his online banking
  - share certain information about his account
  - provide them with information from a one-time password they were sending him
- Shortly thereafter Mr. B noticed an e-transfer was deposited to another account

Fake Fraud Investigation Scam

- When we investigated the complaint, we found the consumer had shared confidential information with the fraudster including a one-time verification password that said “do not share this with anyone”
- We didn’t recommend compensation because there was no evidence the bank made a mistake that caused the loss

Grandparent Scam

- Ms. W received a phone call from someone pretending to be her grandson
- He said he needed money because he had been wrongly arrested while traveling and he needed money for bail and a lawyer
- Wanting to help, she wired a total of $30,000 in multiple transactions to the scammer
- Later, when her real grandson visited, she discovered he had never requested money, revealing she had been scammed



Grandparent Scam

- The bank didn’t compensate the consumer because they were following her instructions
- We investigated and learned
  - The bank representatives asked her why she was making a large wire transfer that was unusual for her
  - The fraudster had told her to lie about the purpose of her wire transfers saying if the bank found out what it was for, they may not allow the transfer, and it was urgent that he get the money
  - She told the bank representatives she was sending money to a contractor doing work on her vacation home

Grandparent Scam

- We didn’t recommend compensation because:
  - The bank made reasonable inquiries, and the consumer lied to the bank
  - So, it appeared the bank acted reasonably in following the consumer’s instructions

Misconceptions about fraud protection

Consumers often incorrectly believe that they are protected from fraud and that their bank will return any money they have lost to fraud.

This is not always the case.

In most cases, consumers breached their account agreements by sharing confidential banking information, intentionally or unintentionally.

As a result, consumers are often held liable for their losses in many fraud cases.

Some protection for consumers and seniors

- The Canadian Code of Practice for Consumer Debit Card Services (the Debit Card Code)
- Provincial Consumer Protection Laws
- The Code of Conduct for the Delivery of Banking Services to Seniors (the Seniors' Code)
- Banks' public representations about fraud detection and prevention

Tips to protect yourself from banking fraud

- Be careful when clicking on links in texts and email
- Strengthen your online security practices
- Regularly check account statements and notifications
- Only use secure Wi-Fi Connections
- Never give your confidential information to someone who calls you
- Safeguard your personal information
- Enable two-factor authentication (2FA)
- Enable auto alerts
- Enable auto deposit for e-transfers
- Never return money to someone who has sent it to you
- Speak to your family and friends to help them be fraud aware

Crypto Fraud

- Ms. P, a senior looking to grow her retirement savings, found a company on-line promising to help investors make money investing in crypto
- Unfortunately, the company was just a fraudster with a slick website
- The fraudster convinced Ms. P that if she invested in crypto with him, she would earn high returns on her savings
- With the fraudster's help, Ms. P opened an account at a licensed crypto dealer, transferred $60,000 into the account, purchased Bitcoin, and transferred the Bitcoin to the fraudster so that he could invest it for her

Crypto Fraud (continued)

- Once the crypto was transferred to the fraudster, it was gone - crypto transfers are irreversible and can't be traced
- Ms. P complained to the licensed crypto dealer, where she deposited her money and purchased the crypto, that it should have warned her about potential fraud and stopped the transfer to the fraudster
- The crypto dealer did not compensate Ms. P
- When we investigated the case, we did not recommend compensation
- We found the crypto dealer had warned Ms. P about potential fraud
- When Ms. P was opening her account, the crypto dealer had asked Ms. P several questions related to the transactions, but Ms. P had lied to the firm because the fraudster told her to

Tips to protect yourself from crypto fraud

Only deal with licensed professionals—verify investment professionals through the National Registration Database.

Fraudsters hide behind fake identities—once the scam is discovered, they're often untraceable.

Never send money or crypto to strangers or people you've never met in person.

Be careful about doing your own research— fraudsters create fake positive reviews.

Heed fraud warnings—they're based on real scam patterns and are meant to protect you.

Pause and reflect—legitimate investments don't require rushed decisions – if you are being rushed it is a red flag!

Talk to someone you trust—a friend, family member, or professional can help spot red flags.

Be skeptical of promises of high returns—no one can guarantee consistent investment growth.

Resources and tools to protect your financial well-being

Powers of Attorney

Trusted contact person

Office of the Public Guardian and Trustee

Powers of Attorney (POA)

- A power of attorney is a legal concept in which you sign a document to give one or more people, the authority to manage your money and or your property for you.
- In most of Canada, the person you appoint is called an "attorney." That person does not need to be a lawyer.

What can your attorney do:

- Banking
- Sign cheques
- Buy or sell real estate in your name
- Buy consumer goods

Your attorney cannot:

- Make/change a will for you
- Change a beneficiary on a life insurance plan
- Give the power of attorney to someone else

Regular POA vs. Banking POA

- Regular POA
  - **Focus**: a more comprehensive delegation of authority for a wider range of financial and legal matters
  - **Scope**: can cover a wide range of financial and legal decisions, including managing investments, real estate, and personal affairs
- Banking POA
  - **Focus**: specifically for managing bank accounts
  - **Scope**: limited to the powers granted in the document, which include making deposits, withdrawals, transferring funds, or paying bills from specific accounts

Trusted contact person

- Your investment advisor may ask your trusted contact person questions about you and your wellbeing in specific circumstances, including:
- If your advisor cannot get in touch with you after repeated attempts
- If financial exploitation is suspected
- If there are concerns about your ability to make financial decisions
- To confirm your legal representative(s)

A Trusted Contact Person (TCP) is a person you authorize your investment advisor or firm to contact in limited circumstances

A TCP can help your investment advisor or firm to respond to possible situations of financial abuse or fraud affecting you and your investments

Office of the Public Guardian and Trustee

- The Office of the Public Guardian and Trustee:
  - acts as Substitute Decision Maker of last resort
  - can make financial decisions for adults who have been found mentally incapable
  - can make substitute treatment or long-term care admission decisions for incapable individuals
  - administers estates when no one else is available to do so
  - provides other services to protect the financial, legal and personal care of mentally incapable Ontarians

Summary

- Take proactive steps to protect yourself
- Be vigilant about potential fraud
- Appointing a power of attorney and trusted contact person can be beneficial for your financial well-being
- Visit OBSI's website for more resources for seniors