ASC
Alberta Securities Commission

# Senior Financial Exploitation

## Understanding risks and prevention strategies for older clients

**Hilary McMeekin**
Director, Communications & Investor Education,
Alberta Securities Commission

# Senior Financial Exploitation Overview

## Growing Risk Among Seniors

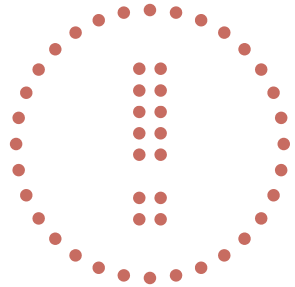
Seniors face increased exposure to sophisticated financial scams targeting their vulnerabilities.

## Evolving Fraud Schemes

Investment fraud schemes have evolved to exploit trust, social connections, and emotional vulnerabilities unique to older investors.

## Prevention and Protection

Sharing case studies, behavioral insights, and actionable steps enhances early fraud detection and client protection.



# Prevalence of Investment Scams Among Seniors

## Targeting Seniors' Vulnerabilities

Seniors face increased risk due to accumulated wealth and limited familiarity with modern financial technologies.

## Underreporting and Challenges

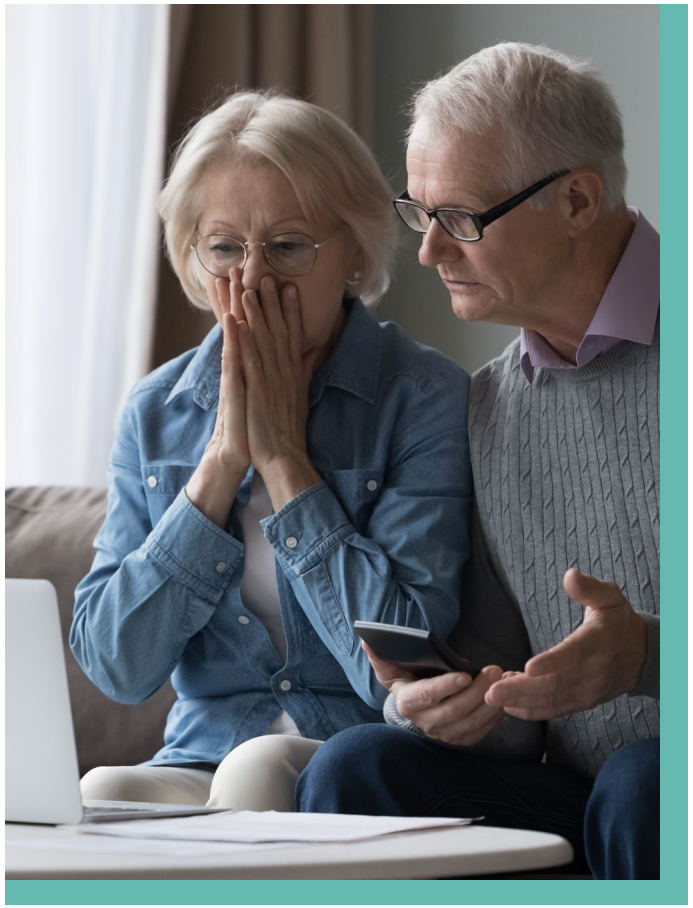
Victims often underreport scams due to embarrassment or unawareness, complicating enforcement efforts.

## Types of Scams Affecting Seniors

Long-haul scams, affinity fraud, and romance scams build trust over time to deceive seniors effectively.

## Playing a Role in Prevention

Professionals can identify subtle behavior changes to detect scams early and reduce financial harm.



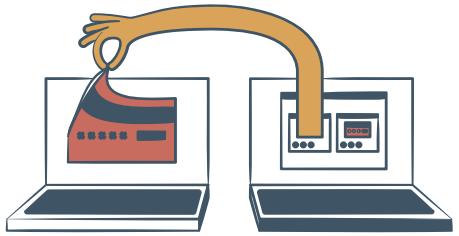
# Technology-Driven Fraud Risks

## Cryptocurrency Scams Targeting Seniors

Fraudsters use Bitcoin ATMs and crypto platforms to exploit seniors unfamiliar with digital currencies.

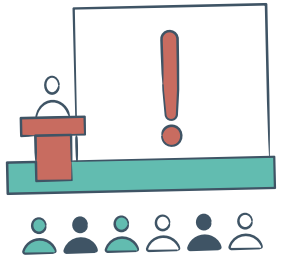
## AI-Enabled Deception

Deepfakes and avatars are used to impersonate trusted individuals for fraudulent purposes.



## Remote Desktop Access Risks

Scammers gain direct device access through remote desktop applications to steal sensitive data.



## In-Person Scam Workshops

Fraudsters conduct fake educational sessions to build trust and facilitate scams against seniors.

# A Few Enforcement Cases

| Case | Status | Nature of Misconduct | Senior Victims |
|---|---|---|---|
| Base Finance | Concluded; criminal convictions (10 years and 3 years) | Fraud (Ponzi scheme) | Many seniors lost entire retirement savings |
| Fowler | Concluded; conditional sentence; prior jail sentence | Unregistered dealing and fraud | Senior targeting other seniors |
| HW | Merits decision issued; sanctions pending | Unregistered trading (day trading) | $14M from Hutterite communities including elderly victims |
| GIC | Hearing underway | Fraud allegations ($5M+) | Targeted via religious/charity messaging |
| Black Box | Proceedings concluded; ongoing criminal investigation | Ponzi scheme, unregistered dealing | Seniors in small communities via word of mouth |

# Case Insights

## Ponzi Scheme Impact

The Base Finance case reveals devastating financial losses from one of Alberta's largest Ponzi schemes targeting seniors.

## Spread Through Word-of-Mouth

The Black Box case demonstrates how word-of-mouth spreads fraud quickly within small communities.

## Unregistered Trading Risks

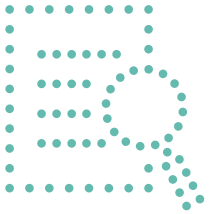
The HW case highlights risks within close communities where unregistered trading exploits trust among members.

## Repeat Offenders Targeting Seniors

The Fowler case warns of repeat offenders who specifically target seniors, emphasizing the need for ongoing vigilance.

## Exploitation via Charitable Narratives

The GIC case shows fraudsters use religious and charitable stories to gain credibility and attract investments.



# Prevention and Detection Strategies

# Client Engagement and Red Flags

## Suggested “Screening” Questions

Asking clients about new financial relationships, Bitcoin ATM usage, unrequested calls and device remote access requests can uncover early fraud risks.

## Identifying Red Flags

Talking through red flags with clients: Promises of guaranteed returns and no risk; pressure to get involved; watching for sudden withdrawals, unexplained asset depletion, and unregistered investment platform involvement.

## Monitoring Crypto Transactions

Crypto transactions are irreversible and hard to trace, making them critical and challenging.

## Fraud Detection

Combining questions with behavioral observations helps identify vulnerabilities early.

# Red flags to note

- Has the client answered “yes” to any of your awareness-building questions?
- A client makes unexpected or urgent withdrawal requests to fund a self-directed investment.
- There is unexpected depletion of cash assets held outside managed accounts.
- A client says they bought crypto assets through an online platform or a Bitcoin ATM. Note: Where crypto is involved, it's important to verify what was purchased, whether the platform was registered, and who has custody of the assets.

# What to do if you suspect?

FINTRAC CANAFE
Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

File a suspicious transaction report (STR) with FINTRAC.

CSA ACVM
Canadian Securities Administrators
Autorités canadiennes en valeurs mobilières

Report concerns directly to enforcement at one of the securities regulators.

# Key Takeaways

1 Scams targeting seniors are increasingly relationship-based, technology-enabled, and now, often tied to crypto-related payment or investment channels.

2 Having conversation and talking through what's been happening for them can help uncover vulnerabilities before losses escalate.

3 A short set of consistent questions can help professionals and firms identify warning signs and act quickly when red flags exist.

# Contact us

asc.ca
checkfirst.ca

inquiries@asc.ca

403-355-4151
Toll-free: 1-877-355-4488