Financial Exploitation and Artificial Intelligence: Confronting the Realities

DISCLAIMER

Not speaking on behalf of CIRO

CIRO · OCRI

Canadian Investment Regulatory Organization

Organisme canadien de réglementation des investissements

Advancing the rights
and well being of
all Canadians as
we age

CanAge: Canada's National Advocacy Organization

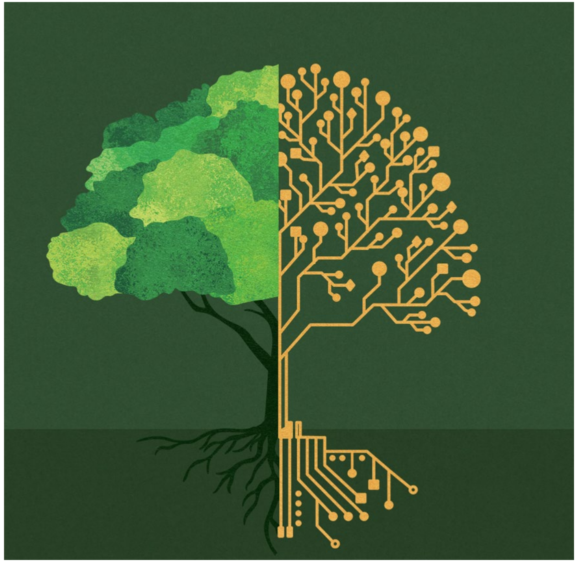
Laura Tamblyn Watts
CanAge

CanAge


"Hi Grandma, it's me! I'm in trouble and need money right away. Can you help me out?"


MacBook Pro

AI Shaping the Future



AI in Healthcare

Revolutionizing medical diagnosis and treatment

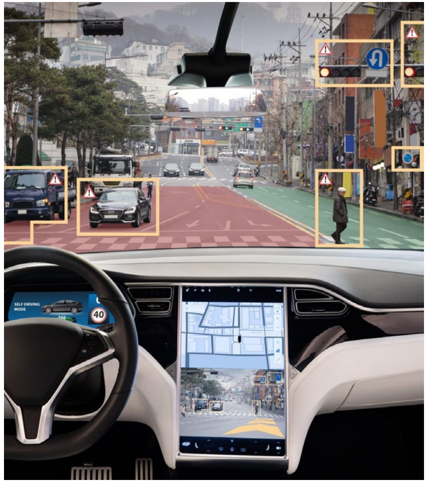
AI-Powered Autonomous Vehicles

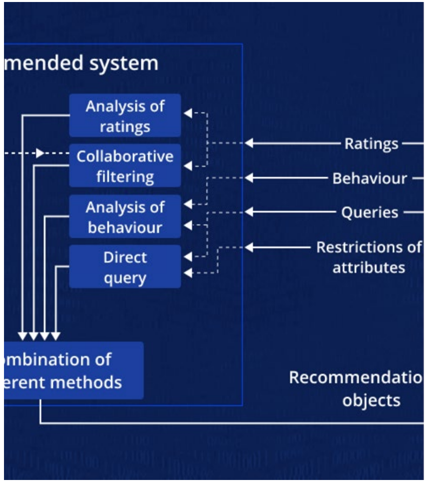
Transforming transportation and mobility

AI in Sustainability

Optimizing energy usage and environmental protection

AI in Action





Autonomous Driving

AI-powered self-driving cars revolutionize transportation

Medical Imaging Analysis

AI algorithms accurately detect and diagnose medical conditions

Personalized Recommendations

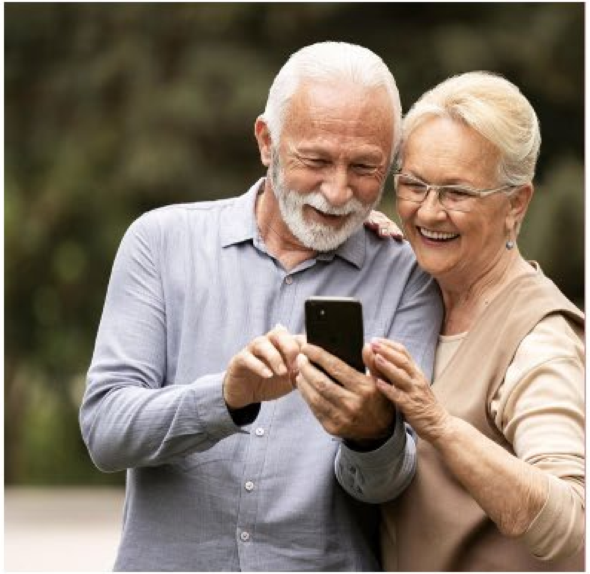
AI-driven recommendation systems enhance user experiences

Predictive Maintenance

AI predicts equipment failures to optimize maintenance schedules


ChatGPT: Optimizing Language Models for Dialogue
We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests. ChatGPT is a sibling model to InstructGPT, which is trained to follow an instruction in a prompt and provide a detailed response.
TRY CHATGPT ↗
MacBook Pro

Seniors Adapting to the Tech Landscape



Navigating Unfamiliar Tech

Seniors learning to use new digital devices and applications

Adapting to Digital Communication

Seniors embracing online communication tools like video calls

Overcoming Tech Anxiety

Seniors building confidence in using technology through training

Financial exploitation is the fastest-growing form of elder abuse.

Older Americans reported nearly $4.9B in losses to online fraud in 2024 (43% year-over-year increase)

Every country in the world is affected

A borderless crime

BILLIONS OF SCAMS ARE ENCOUNTERED IN CANADA EVERY SINGLE DAY.

The money stolen through scams is often used to fund more serious crimes, including human trafficking, organized crime, terrorism, and the drug trade. But Canadians can take back control.

Wildly Underestimated.

SCAMS IN CANADA IN 2024:

SOURCE

Reported dollars lost

$647M

SOURCE

Reports processed by Canadian Anti-Fraud Centre

51.6K

SOURCE

Percentage of all scams reported

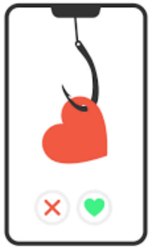
5-10%

Adjusting for underreporting, the FTC estimates that the overall cost of fraud to older consumers in 2023 may have been as high as

$61.5 billion

That's **$117,000** per minute

AI Enabled Scam Typologies



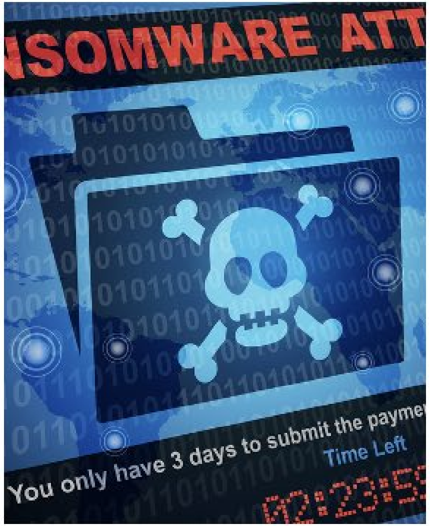
- INVESTMENT LURING / ROMANCE-BAITED INVESTMENT SCAMS

- TECH-SUPPORT & BANK-IMPERSONATION FRAUD

CRYPTO APPROVALS & WALLET-DRAINING

RECOVERY SCAMS IMPERSONATING REGULATORS/BANKS

Cybercrime Threats



Ransomware attack

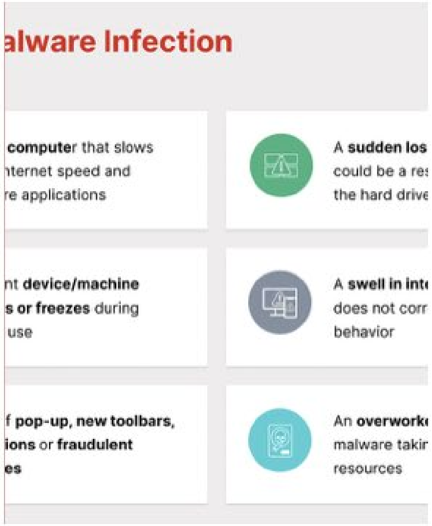
Showcasing a devastating ransomware attack locking down a computer system

Phishing scam

Highlighting a phishing email luring an unsuspecting victim to reveal sensitive information

Data breach

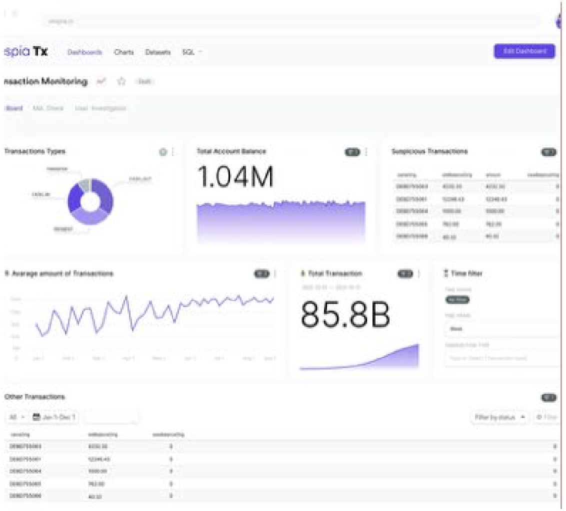
Depicting the aftermath of a data breach, with sensitive information exposed



Malware infection

Showcasing the infiltration of a computer system by malicious malware

Combating Financial Fraud



Financial Transaction Monitoring

Utilize advanced algorithms to detect and flag suspicious financial activities in real-time.

Biometric Authentication

Implement secure biometric identification methods to prevent unauthorized access to financial accounts.

Fraud Reporting Hotline

Establish a dedicated fraud reporting hotline to encourage individuals to report suspected fraudulent activities.

FinCEN Issues Analysis on Elder Financial Exploitation

Immediate Release: April 18, 2024

Financial Institutions Report $27 Billion in Elder Financial Exploitation Suspicious Activity in One-Year Period

WASHINGTON — The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis today focusing on patterns and trends identified in Bank Secrecy Act (BSA) data linked to Elder Financial Exploitation (EFE), or the illegal or improper use of an older adult's funds, property, or assets. FinCEN examined BSA reports filed between June 15, 2022 and June 15, 2023 that either used the key term referenced in FinCEN's June 2022 EFE Advisory or checked "Elder Financial Exploitation" as a suspicious activity type. This amounted to 155,415 filings over this period indicating roughly $27 billion in EFE-related suspicious activity.

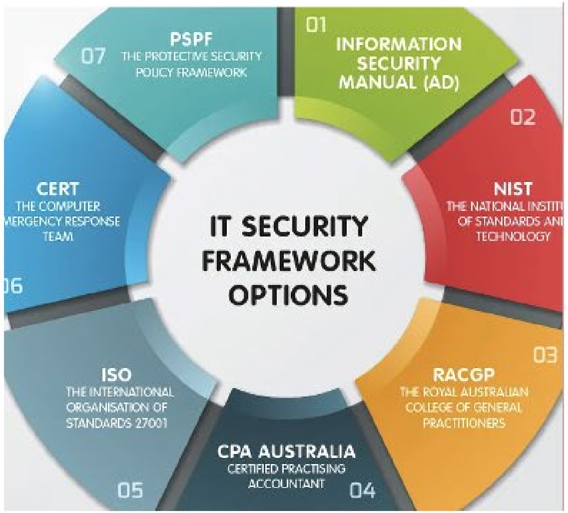
"FinCEN has long recognized the threat that Elder Financial Exploitation poses and the need to protect the older adult population from financial abuse," said FinCEN Director Andrea Gacki. "FinCEN's analysis highlights the critical role of financial institutions in helping to identify, prevent, and report suspected Elder Financial Exploitation. We are grateful for their vigilance and for the BSA information they have filed — and continue to file — in response to FinCEN's 2022 advisory."

Tech Support	$1,464,755,976	**Advanced Fee**	$102,074,512
Personal Data Breach	$1,453,296,303	**Phishing/Spoofing**	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	**SIM Swap**	$25,983,946
Confidence/Romance	$672,009,052	**Overpayment**	$21,452,521
Government Impersonation	$405,624,084	**Ransomware ***	$12,473,156
Data Breach	$364,855,818	**Harassment/Stalking**	$10,611,223
Other	$280,278,325	**Botnet**	$8,860,202
Employment	$264,223,271	**IPR/Copyright and Counterfeit**	$8,715,512
Credit Card/Check Fraud	$199,889,841	**Threats of Violence**	$1,842,186
Identity Theft	$174,354,745	**Malware**	$1,365,945

Australia plans to combat scams through data fusion

Future state: National Anti-Scam Centre regular data sharing

Navigating the Cyber Landscape



Cybersecurity Frameworks

Explore comprehensive cybersecurity frameworks to enhance organizational security

Zero Trust Architecture

Implement a zero trust approach to verify and secure user and device access

Security Automation

Leverage AI and machine learning to automate security processes and response

Risk Landscape

Scale & speed: digital rails amplify reach.

AI lowers cost of deception: voice cloning, deepfakes.

Push-payment fraud shifts liability to consumers.

Who's Most at Risk?

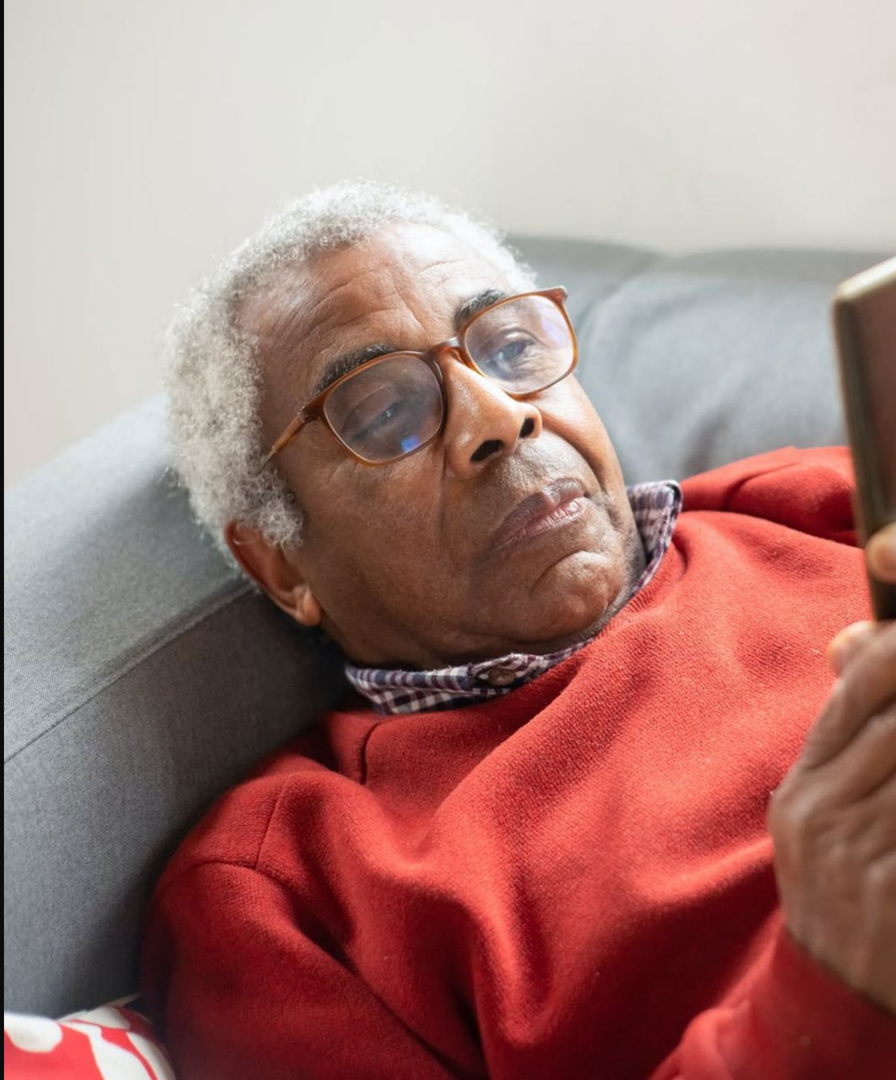
FINRA/DeLiema research:

Prior knowledge reduces losses by ~80%

Loneliness increases susceptibility

'Official' appearance of outreach heightens risk

Action: Targeted education + social connection.



Academic Research Findings

What Increases Risk?	What Decreases Risk?
➢ Financial Fragility	➢ Targeted Fraud Education
➢ Loneliness	➢ Forewarning
➢ Stress	➢ Scam-prevention messages
➢ Risky financial behaviours	➢ Psychological well-being
➢ Cognitive decline/neurological vulnerability	➢ Cognitive engagement
➢ Emotional arousal & positivity effect	➢ Advanced financial planning expertise and / or supports
➢ Repeat victimization	➢ Institutional safeguards

Dr. Marti DeLiema - U of Minnesota - Social Work, Education and Aging

Risk factors:

- ➔ Financial fragility
- ➔ Loneliness and depression
- ➔ Stressful life events
- ➔ Widowhood
- ➔ Risky behaviours
- ➔ Cognitive & decision-making vulnerabilities
- ➔ Emotional arousal

*Carstensen, L. L. & **DeLiema, M.** (2018). The positivity effect: A negativity bias in youth fades with age. Current Opinion in Behavioral Sciences, 19, 7-12.*

Protective factors:

- ➔ Education and awareness
- ➔ Scam prevention messaging
- ➔ Psychological well-being
- ➔ Advanced planning
- ➔ Institutional safeguards (eg: temporary account holds)

***DeLiema, M.,** Li, Y., & Mottola, G. (2022). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. International Journal of Consumer Studies.*

Dr. Natalie Denburg - U Iowa, Neurology

Risk Factors:

1. **Age-related changes in the ventromedial prefrontal cortex (vmPFC)**

➔ The vmPFC regulates skepticism and gut reactions, contributing to the formation of counter-arguments
➔ The vmPFC may become less effective with age in some individuals

2. Positivity effect

➔ Tendency to focus on positive information = increased susceptibility in interactions with persuasive fraudsters

Protective Factors:

1. **Forewarning interventions**

➔ Encourages the formation of counter-arguments
➔ General warnings are more effective long-term in comparison to scam-specific warnings

2. **Decision-making supports**
➔ Educational tools (ex: self-evaluation worksheets)

Denburg, N., Goetz, T., Jones, A., Garcia, N. & Cole, P. (In Press). Self-evaluation worksheets enhance elder financial decision making.

Does Getting Old Make People Vulnerable to Financial Exploitation? A Neuropsychological Perspective

Natalie Denburg, PhD

Professor of Neurology

University of Iowa Carver College of Medicine

Dr. Patricia Boyle - Rush U, Chicago

Risk Factors:

1. **Cognitive decline**

➔ Associated with declining financial literacy

2. **Dementia & Low Scam Awareness**

➔ Low scam awareness associated with later dementia and Alzheimer's disease pathology

Rita Rubin, MA JAMA. Published online June 12, 2019. Low Awareness of Scammers' Tactics Linked to Dementia Risk in Cognitively Normal People

Protective Factors:

1. **Psychological well-being**

➔ A strong sense of purpose in life linked with slower cognitive decline

2. **Cognitive engagement**

➔ Ongoing mental stimulation (ex: from reading, learning, playing games, etc) helps preserve cognitive functioning

Rita Rubin, MA JAMA. Published online June 12, 2019. doi:10.1001/jama.2019.5765Low Awareness of Scammers' Tactics Linked to Dementia Risk in Cognitively Normal People

Journal of Elder Abuse & Neglect ›

Volume 28, 2016 - Issue 2

Articles

Five-year all-cause mortality rates across five categories of substantiated elder abuse occurring in the community

Jason Burnett PhD, Shelly L. Jackson PhD, Arup K. Sinha MS, Andrew R. Aschenbrenner BS, MS, Kathleen Pace Murphy PhD, Rui Xia PhD & ...show all

Pages 59-75 | Accepted author version posted online: 21 Jan 2016, Published online: 25 Feb 2016

Cite this article https://doi.org/10.1080/08946566.2016.1142920

Australian Government

National Anti-Scam Centre

Focus: Stopping scams at the source through data fusion and acting on it

FY23/24	FY24/25	FY25/26
✓ Establishment & governance	National Anti-Scam Centre website	Whole of ecosystem near real time data sharing
✓ Public/private Advisory board	Scam website takedown service	Proactive intelligence
✓ People & workforce capability	Website and scam ads report service	Fusion cells 3 and 4
✓ Partners & engagement	Data partner onboarding: police; banks; digital platforms; cryptocurrency exchanges; telcos; regulators	Ongoing awareness
✓ Collaborative disruption projects	Data integration and reporting	Technology enhancements
✓ Industry forums & working groups	Disruption strategy	Coordinated response to emerging scams
✓ Technology foundations	Awareness campaign	
✓ Scamwatch website uplift	Second fusion cell	
✓ Investment scam fusion cell	Actionable intelligence service	
✓ Auto referrals for victim support	AFCX Intel Loop partnership	
✓ URL sharing to ASIC	Scam email forwarding service	
✓ Data standards		

Financial Transactions and Reports Analysis Centre of Canada

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor. Its mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.

Fraud alert

Many scams and fraudulent activities attempt to imitate government services in order to gain access to your personal and financial information. FINTRAC and FINTRAC personnel have occasionally been misrepresented in scams and fraud attempts.

5 Ways AI Can Protect Seniors from Fraud & Scams

1. Real-Time Fraud Detection	AI scans millions of transactions instantly, flagging unusual patterns and stopping fraud before money is lost. Example: Mastercard and JPMorgan use AI to detect anomalies at scale.
2. Just-in-Time Warnings	AI delivers tailored alerts at the moment of risk. Script-specific warnings ('This looks like a romance scam') are highly effective. UK's Confirmation of Payee model shows the power of timely intervention.
3. Client-Side AI Copilots	AI assistants can simplify investment offers, flag risks, and check opportunities against regulator alerts. Research by Ioannis Spyridopoulos highlights how this empowers older adults.
4. Voice & Deepfake Detection	AI tools identify cloned voices or fake videos, preventing grandparent scams and deepfake investment frauds. Germany's Hawk AI already supports banks in real-time detection.
5. Shared Fraud Intelligence	AI enables real-time sharing across banks, regulators, and telecoms to disrupt scams early. Australia's National Anti-Scam Centre leads with AI-driven scam disruption squads.


100


SAMSUNG
Username
username
Password
****
Remember Me
Login
Register


fortunat y,
we longer eed
r servic


A
I


VISA
VISA
I
O
K

Minister Champagne highlights Spring Economic Update measures to fight financial crimes

From: Department of Finance Canada

News release

May 6, 2026 - Toronto, Ontario - Department of Finance Canada

Quotes

> "Too many Canadians—especially seniors and vulnerable people—are being targeted by scams and financial crime. The Spring Economic Update takes bold steps to protect people, crack down on criminals, and promote safer futures, financial security, and independence for Canadians."
>
> *- The Honourable François-Philippe Champagne, Minister of Finance and National Revenue*

Quick facts

- To stand up the new Financial Crimes Agency, the Spring Economic Update 2026 proposed to provide:
    - $352.7 million over five years starting in 2026-27, with $57.8 million in remaining amortization, and $82.1 million ongoing to the Financial Crimes Agency;
    - $46.2 million over five years and $11.5 million ongoing to the Public Prosecution Service of Canada; and
    - $19.6 million over five years and $1.5 million ongoing to the Department of Finance Canada.
- As part of the National Anti-Fraud Strategy, in addition to general prevention requirements, organizations could be required to take fraud prevention measures specific to their industry, for example:
    - providing specific warnings about the risk of fraud when individuals initiate large-scale transfer payments (e.g., wire transfers, international money transfers);
    - blocking or flagging calls that "spoof" legitimate enterprises, government institutions, and law enforcement; and
    - implementing screening for fraudulent profiles and pages, and blocking malicious ads.

- Bill C-15, which recently received Royal Assent, makes amendments to the *Bank Act* that require banks to:
    - have policies and procedures in place to detect and prevent consumer-targeted fraud and mitigate its harms;
    - obtain the express consent of personal deposit account holders before enabling prescribed account capabilities which fraudsters can use to steal consumers' money, including transfer and payment capabilities, and to permit account holders to disable prescribed capabilities they do not want;
    - allow personal deposit account holders to adjust their transaction limits to protect themselves; and
    - collect fraud-related data and report it to the Financial Consumer Agency of Canada.
- On February 19, 2026, the Minister of Finance and National Revenue directed FINTRAC to help combat extortion and support law enforcement investigations by:
    - prioritizing financial intelligence resources to tackle extortion;
    - launching the Countering Extortion Partnership with financial institutions, government, and law enforcement;
    - assigning financial intelligence experts to support police;
    - providing financial institutions with clear guidance on how to detect extortion transactions; and
    - publishing intelligence on how criminals move and hide extortion money.
- Crypto ATMs have become a primary method for scammers to extract cash from victims and for criminals to place their cash proceeds of crime in Canada. Studies have found that between 85 and 98 per cent of crypto ATM transactions are linked to illicit activity. The Canadian Anti-Fraud Centre conservatively estimates that between 5 and 10 per cent of fraud is reported, meaning that Canadians are estimated to have lost between $142 million and $284 million due to fraud facilitated by crypto ATMs in 2024. The details of the ban on crypto ATMs will be provided in legislation expected to be tabled shortly.
- Budget 2025 announced $1.7 billion in funding to strengthen the RCMP's response to a wide range of threats related to transnational organized crime, financial crimes, and money laundering, while enhancing its intelligence and national security capacity, fulfilling the government's commitment to hire 1,000 RCMP personnel.
- Since 2019, the government has invested close to $379 million in combatting financial crimes. These investments have strengthened supervision and financial intelligence functions at FINTRAC, increased resources and tools to support financial crime investigations, and enhanced Canada's ability to combat trade-based financial crime.

Selected References

- Key sources:
- - FBI IC3 Elder Fraud Reports
- - FINRA Foundation (DeLiema)
- - CSA/OSC Trusted Contact Person & Holds
- - FCA & PSR (UK) on APP reimbursement & CoP
- - ACCC/NASC scam reports
- - Spyridopoulos: AI & Financial Independence

If you have any questions, please contact

647-969-6793

www.CanAge.ca

laura@canage.ca | info@canage.ca | partnerships@canage.ca