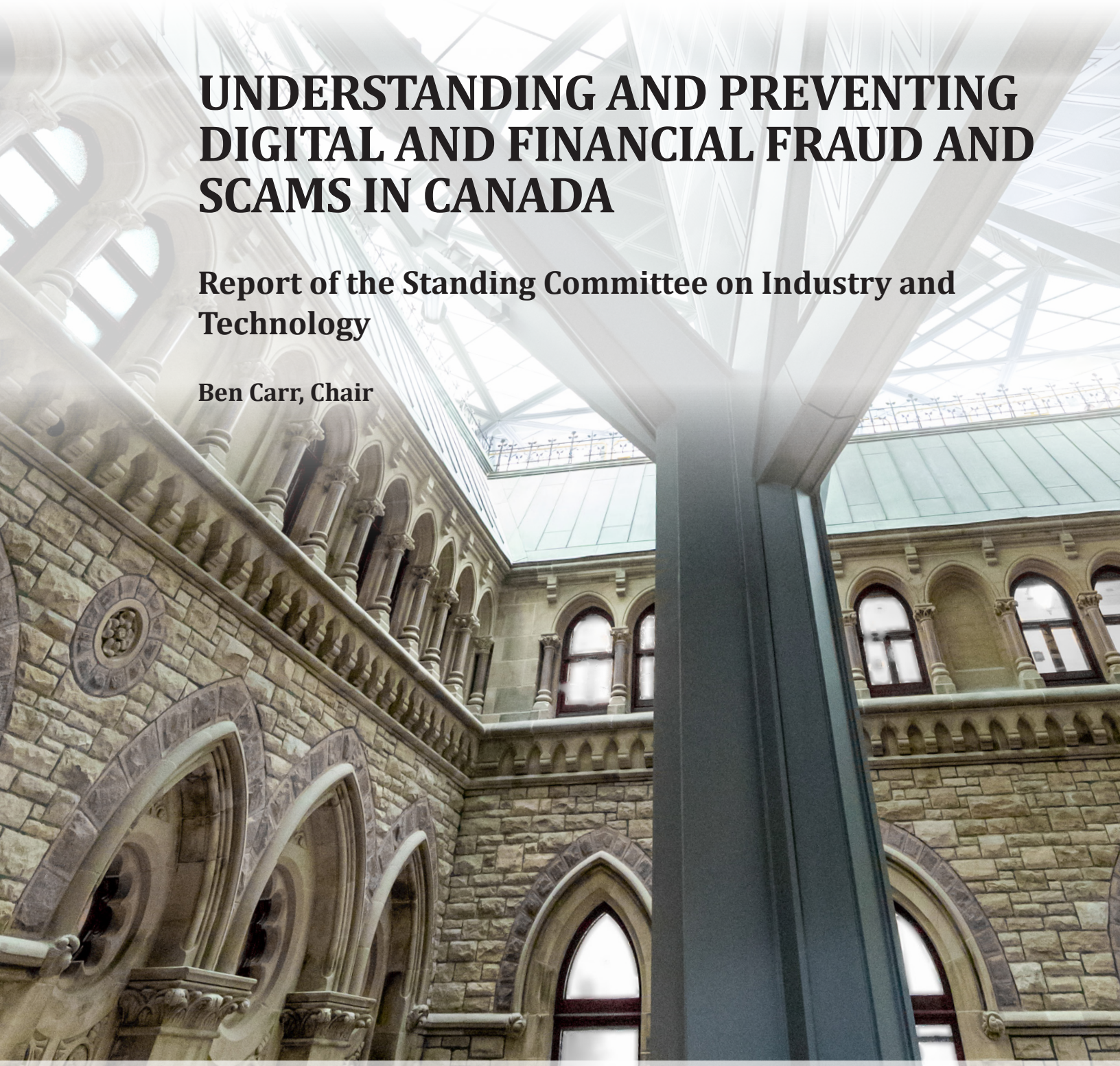
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA



UNDERSTANDING AND PREVENTING DIGITAL AND FINANCIAL FRAUD AND SCAMS IN CANADA

Report of the Standing Committee on Industry and Technology

Ben Carr, Chair

NOVEMBER 2026
45th PARLIAMENT, 1st SESSION

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Standing Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website
at the following address: www.ourcommons.ca

UNDERSTANDING AND PREVENTING DIGITAL AND FINANCIAL FRAUD AND SCAMS IN CANADA

Report of the Standing Committee on Industry and Technology

Ben Carr
Chair

NOVEMBER 2026

45th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY

CHAIR

Ben Carr

VICE-CHAIRS

Adam Chambers
Gabriel Ste-Marie

MEMBERS

Parm Bains
Karim Bardeesy
Doly Begum
Harb Gill
Jason Groleau
Leslyn Lewis
Michael Ma
Bienvenu-Olivier Ntumba
Dominique O'Rourke

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Xavier Barsalou-Duval
Bardish Chagger
Guillaume Deschênes-Thériault
Bruce Fanjoy
Claude Guay
Will Greaves
Lisa Hepfner
Randy Hoback
Anthony Housefather
Natilien Joseph
Tamara Kronis

Viviane Lapointe
Andrew Lawton
Chris Lewis
Chi Nguyen
William Stevenson
Tim Watchorn

CLERK OF THE COMMITTEE

Ariane Calvert

LIBRARY OF PARLIAMENT

Marie Dumont, Analyst
Dana Fan, Analyst
Jesse Good, Analyst
Sarah Lemelin-Bellerose, Analyst

THE STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY

has the honour to present its

SEVENTH REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied financial fraud and scams in Canada and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS 1

UNDERSTANDING AND PREVENTING DIGITAL AND FINANCIAL FRAUD AND SCAMS IN CANADA 5

- Introduction 5
- The Role of Stakeholders: Banks, Telecommunications Companies and Social Media Platforms 7
  - Banks, Financial Institutions and Payments Canada 10
  - Telecommunications Companies 12
  - Social Media Platforms and Technology Companies 13
- Canada's Approach to Managing Financial Fraud 16
  - Prevention and Education 18
  - Cross-Sectoral Data Sharing 19
  - Liability for Fraud in Canada 21
  - Enforcement 22
- Best Practices: Lessons From Australia 24
- Conclusion 25

APPENDIX A: LIST OF WITNESSES 27

APPENDIX B: LIST OF BRIEFS 29

REQUEST FOR GOVERNMENT RESPONSE 31

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

That the Government of Canada remove unnecessary legal and regulatory barriers that prevent the timely sharing of meaningful information among financial institutions, telecommunications service providers, digital platforms, public agencies, law enforcement and international partners; reduce delays affecting the sharing of information necessary for fund recovery; and introduce safe-harbour provisions protecting organizations that share information in good faith for fraud detection, prevention, investigation, and recovery from liability under applicable privacy and competition laws.

Recommendation 2

That the Government of Canada develop standardized data-sharing protocols among stakeholders involved in cybercrime prevention and financial fraud reduction while protecting individual privacy and improving the quality of information available concerning scam types and victim demographics.

Recommendation 3

That the Government of Canada accelerate implementation of the National Anti-Fraud Strategy announced in Budget 2025 and the establishment of Canada's Financial Crimes Agency, and use this framework to establish a coordinated, multi sector scam-prevention regime – bringing together financial institutions, telecommunications service providers, digital platforms, regulators, law enforcement and other relevant stakeholders to share information – and to track and respond to the rapidly changing financial fraud landscape – with the goal of providing feedback to federal, provincial and territorial governments – while drawing lessons from Australia's coordinated cross-sectoral approach.

Recommendation 4

That the Government of Canada require social media companies to verify that every advertiser of financial services is a legitimate, regulated entity prior to accepting and posting advertisements.

Recommendation 5

That the Government of Canada require platforms to immediately remove fraudulent advertisements and repeat fraudulent advertisers when notified by financial institutions or legitimate organizations that are being impersonated and allow bulk removal rather than requiring fintech and financial institutions to flag each ad individually.

Recommendation 6

That the Government of Canada ensure that financial sanctions imposed by Canadian securities regulators for the most serious forms of market misconduct are not extinguished through bankruptcy proceedings by amending section 178(1) of the *Bankruptcy and Insolvency Act* to add fraud, market manipulation, and misrepresentation to the list of debts that are not released through bankruptcy.

Recommendation 7

That the Government of Canada maintain support for the Anti-Scam Coalition and the Canadian Anti-Fraud Centre.

Recommendation 8

That the Government of Canada require digital platforms that manage online advertising channels, regardless of transaction volume, to publicly disclose their budgets for fraud prevention, itemized broadly between public education campaigns and internal tooling development.

Recommendation 9

That the Government of Canada mandate that financial institutions, telecommunications service providers, and digital platforms implement documented measures – including, but not limited to, explicit modal confirmation dialogues that require clickthrough before proceeding to enact a transaction or continuing on to a different website – to warn and educate their

customers and users about fraudulent scams in a timely manner; and consider mechanisms to hold organizations accountable for scams conducted through their channels including financial disincentives that place the burden of proportionate victim repayment upon scam-permitting channels.

Recommendation 10

That the Government of Canada support increased public education and awareness tailored to different types of scams and demographics, including how and where to report frauds and scams.

Recommendation 11

That the Government of Canada establish a national, cross-sector anti-fraud framework that assigns clear responsibilities to financial institutions, telecommunications providers, digital platforms, regulators, and law enforcement; uses existing regulators and agencies wherever practical; and requests reports from entities in the fraud chain annually on measurable outcomes, including fraud losses, funds recovered, scam content removed, fraudulent calls and texts blocked, and enforcement results.

Recommendation 12

That the Government of Canada clarify and, where necessary, strengthen legal safe-harbour protections to allow financial institutions, telecommunications providers, digital platforms and relevant public agencies to share actionable fraud indicators quickly and in good faith, subject to privacy safeguards, use limitations, and a process to correct false positives.

Recommendation 13

That the Government of Canada work through existing sector regulators to develop proportionate, risk-based expectations for high-risk scam activity, and consider including advertiser verification for financial and investment products, prompt action on verified scam content, stronger blocking and traceback of spoofed calls and texts, and targeted warnings or optional safeguards for unusual transfers, while preserving legitimate communications, consumer choice, and workable appeal processes.

Recommendation 14

That the Government of Canada strengthen the capacity of the Canadian Anti-Fraud Centre using existing federal structures, including by maintaining accessible telephone and online reporting options, providing victim-centred triage and referrals, standardizing the information collected, and adding the findings of fraud investigation reports in their publications.

Recommendation 15

That the Government of Canada work with existing financial regulators, Payments Canada, financial institutions, and the Canadian Anti-Fraud Centre to establish clear, rapid protocols for notifying receiving institutions, recalling or freezing suspected fraudulent transfers where legally permitted, and measuring the proportion and value of victim funds recovered.

Recommendation 16

That the Government of Canada direct existing sector regulators to develop a limited set of standardized, Canadian-specific fraud-prevention metrics for major financial institutions, telecommunications providers, and digital platforms, including verified scam content and accounts removed, response times, fraudulent calls and texts blocked, funds recovered, false positives and appeals; and publish results regularly.

Recommendation 17

That the Government of Canada prioritize organized, high-loss and cross-border fraud within existing RCMP and Canadian Anti-Fraud Centre resources; improve specialized training and access to lawful investigative tools for police; strengthen operational cooperation with provincial, territorial and international partners; and report on investigations, charges, convictions, disruptions and funds recovered.

Recommendation 18

That the Government of Canada, when designing regulations that affect banks and financial institutions, preserve the ability of financial institutions to apply reasonable time holds and threshold limits on cheques and other paper-based instruments that may be altered, counterfeited or used fraudulently.

UNDERSTANDING AND PREVENTING DIGITAL AND FINANCIAL FRAUD AND SCAMS IN CANADA

INTRODUCTION

Imagine a grandfather receiving a phone call from his grandson, who explains that he is in trouble due to a car accident and needs money. The grandfather drives to the bank to collect money and meets a stranger who collects it, or sends an e-transfer to a seemingly familiar email address. Only after the money is exchanged, when the grandfather speaks to his family, does he realize that it was not his grandson who phoned him, but someone with the deepfake ability to emulate the voice. The money is gone, and the whole incident was a fraud. This example – provided by Ian Paterson, Chief Executive Officer of Plurilock Security – is but one illustration of the growing problem of financial fraud in Canada.

Section 380(1) of the *Criminal Code* defines fraud as using "deceit, falsehood or other fraudulent means" to unlawfully deprive the public or a person "of any property, money or valuable security or any service." In 2025, as reported by the Canadian Anti-Fraud Centre, Canadians lost more than $704 million to fraud, the worst year on record. As well, between 2022 and 2026, the reported amount that Canadians have lost due to fraud exceeds $2.4 billion. However, the true amount lost to fraud is likely much higher, because the centre estimates that only 5% to 10% of fraud cases are reported. David Shipley, Chief Executive Officer, Beauceron Security, shared his estimate that in 2025, the true losses in Canada due to fraud likely ranged between $7 billion and $14 billion, due to this underreporting. He also said that since 2020, fraud losses have increased in Canada by 326%.

Witnesses outlined the global and transnational scope of fraud and scams. Jeanette Patell, Director, Government Affairs and Public Policy, Google Canada, explained that

> Financial fraud and scams exploit people and undermine the trust that is essential to the digital ecosystem. This society-wide challenge has grown in scale and complexity, with global fraud losses estimated at nearly $580 billion for 2025, according to Nasdaq's "Global Financial Crime Report". This is driven by sophisticated transnational criminal operations that combine online and offline methods.

Likewise, Ian Paterson noted that "[s]ome of the biggest operations originate outside the country. In the Indo-Pacific, scam compounds run at industrial scale, often staffed by trafficked workers targeting Canadians." Furthermore, Jeanette Patell pointed out that

"this is a fight without a finish line. We are dealing with sophisticated criminal organizations that constantly adapt and are looking for new opportunities to exploit vulnerabilities and identify new vulnerabilities." Ian Paterson contended that "Canada should invest more in international assistance, to help dismantle these networks at the source, before they reach Canadians."

The top three reported cases of fraud in Canada in 2025 were identity fraud, investment fraud and service fraud, and the frauds with the highest financial impacts were investment fraud, romance fraud and job fraud. As Jennifer Quaid, Executive Director, Canadian Cyberthreat Exchange, put it, the "threat we face is not coming from opportunistic amateurs. These are organized criminal networks using sophisticated technology and professional operational models." The Canadian Anti-Monopoly Project outlined that "[i]n cases of authorized fraud, [such as with the example provided above] the victim of a scam is likely out of luck."

In this context of increasing financial fraud in Canada, on 22 September 2025, the House of Commons Standing Committee on Industry and Technology (the committee) agreed to the following motion:

> That, pursuant to Standing Order 108(2), the Standing Committee on Industry and Technology undertake a study on financial fraud and scams in Canada, recognizing this is a significant and growing threat to consumers and the economy, to identify best practices for prevention to strengthen Canada's anti-fraud framework;
>
> That the study examine:
>
> - the role of banks, telecommunications companies, and digital platforms in preventing scams and protecting consumers;
> - the responsibilities of Innovation, Science and Economic Development Canada, the Canadian Radio-television and Telecommunications Commission, and the Canadian Anti-Fraud Centre, as well as other federal departments and agencies in enforcement, regulation, and public awareness;
> - the adequacy of consumer protection laws, law enforcement capacity, and inter-agency coordination;
> - the impact of emerging technologies, including artificial intelligence [AI], in enabling and combating fraud;

- best practices from other jurisdictions, such as Australia, for improving prevention and enforcement measures; and

- the broader economic and social consequences for Canadians.

That the Committee invite the Minister of Industry to appear for no less than one hour on this study, as well as witnesses from the relevant departments and agencies, industry representatives, and experts;

That the Committee hold no fewer than four meetings on this study; and

That the Committee report its findings and recommendations to the House.[1]

Over five meetings from 4 June 2026 to 18 June 2026, the committee heard from 22 witnesses, including representatives from banks and payment organizations, technology and social media companies, cybersecurity organizations, telecommunications providers, law enforcement, financial regulators, consumer advocacy groups, and Canadian and international industry associations. In addition, more than 15 written briefs were submitted to the committee for this study. This report summarizes witness testimony, providing the perspectives from stakeholders in industry, government and the public. It provides a landscape of Canada's agencies, organizations initiatives and legislation to address fraud. It also shares insights that the committee learned from the Australian experience in addressing fraud. It includes recommendations for the Government of Canada to address the persistent and growing issue of financial fraud.

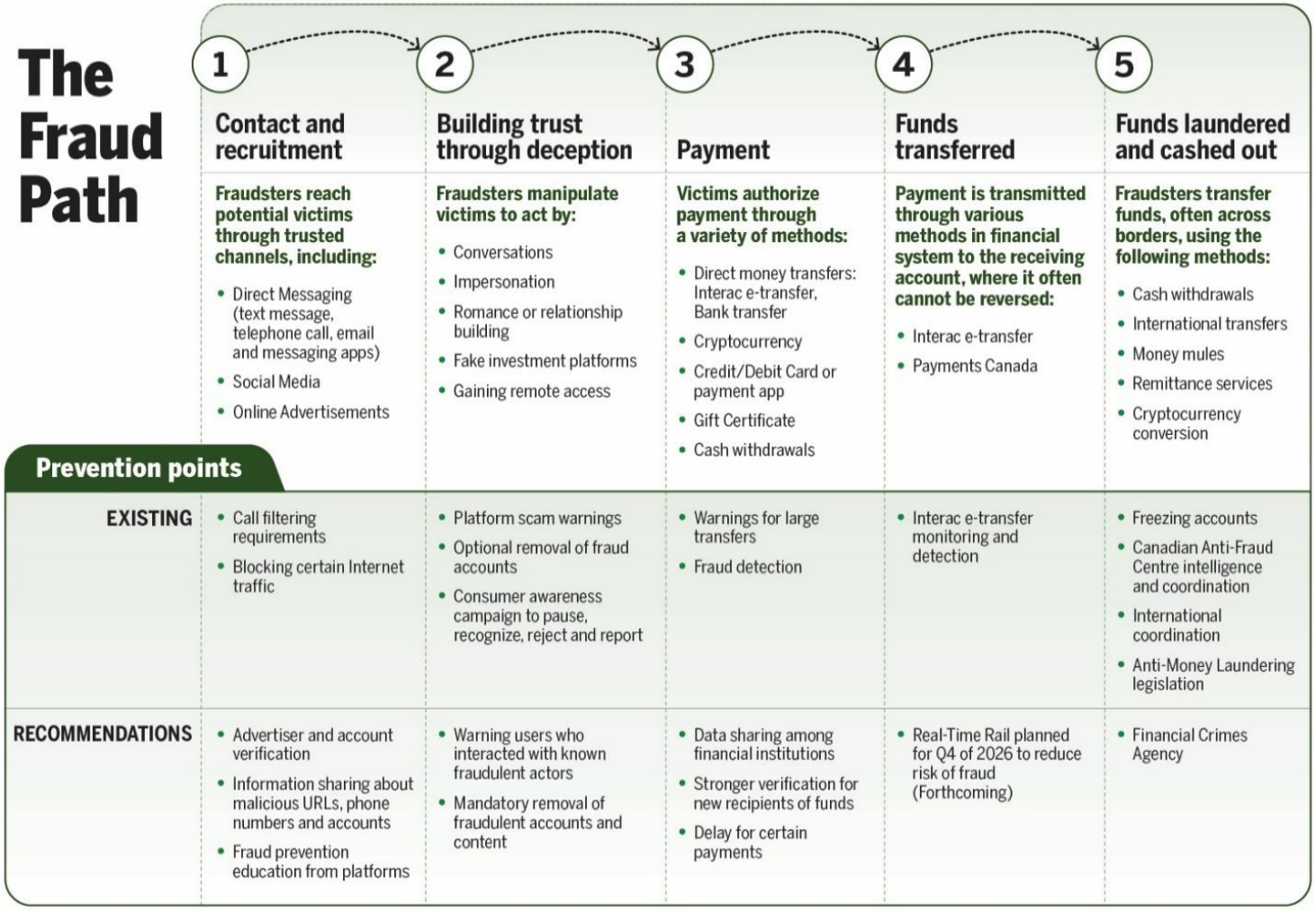
THE ROLE OF STAKEHOLDERS: BANKS, TELECOMMUNICATIONS COMPANIES AND SOCIAL MEDIA PLATFORMS

Various stakeholders, including banks and financial institutions, telecommunications companies, and social media and digital platforms have the potential to facilitate fraudulent transactions and scams, while at the same time are at the forefront of prevention efforts. Eric Smith, Senior Vice-President, Canadian Telecommunications Association, identified that "[f]raud prevention is most effective when telecommunications providers, financial institutions, digital platforms, government agencies and law enforcement work together and share information." Mark Hines, Head of Fraud Product, Interac Corp., likewise said that the "single most effective step Canada can take is enabling better data sharing across sectors, including financial institutions, telecommunications

1 INDU, *Minutes of Proceedings*, 22 September 2025.

providers, digital platforms and law enforcement." At the same time, David Pegley, Managing Director, Australian Financial Crimes Exchange Ltd., pointed out that while the banking sector is familiar with collaboration to share intelligence to identify bad actors, digital platforms and telecommunications companies are "strong competitors," and therefore the "idea that they would collaborate together is a foreign concept." This section examines the role of these multiple sectors regarding fraud and scams in Canada. Figure 1, below, provides an example of the steps involved during a financial fraud.

Figure 1—The Financial Fraud Path



Source: Prepared by the Library of Parliament using data from the Government of Canada.

Banks, Financial Institutions and Payments Canada

Anthony Ostler, President and Chief Executive Officer, Canadian Bankers Association, highlighted that Canada's banks "invest heavily in fraud prevention, cybersecurity training and client awareness," noting that "no single organization or sector can successfully stem this tide." Likewise, Mark Hines noted that Interac's perspective that the problem of fraud "cuts across multiple industries and sectors" and that "[n]o single company or sector can solve this alone." In recognition of this reality for banks, Tru Cooperative Bank's written submission explained that it "works closely with payment providers, industry partners, regulators, law enforcement agencies, and organizations such as the Canadian Anti-Fraud Centre and [Financial Transactions and Reports Analysis Centre of Canada] FINTRAC to share information and support coordinated responses to emerging threats."

For their part, banks, financial institutions and Payments Canda are making efforts to address the issue of fraud. Colin Smith, Vice-President, Risk and Decision Science, Wealthsimple, highlighted that Wealthsimple uses pass-key, trusted places, and real time warnings as tools to combat fraud. For example, Colin Smith outlined that "[i]f someone is moving money in [the Wealthsimple] app while on a phone call, [Wealthsimple] show[s] a warning that the call is not from [it]." He continued in explaining that "[w]hen a client appears to be a victim of a scam, a specially trained team… call[ed]… spell breakers group reaches out to talk to them before the money is gone." Anthony Ostler noted that one of the "biggest accomplishments" of the Canadian Bankers Association was the launch of the education awareness campaign called "Stand Against Scams," which includes the call to action to "Stop. Check. Talk." David Shipley recommended that banks "provide and track fraud education with their customers."

In its written brief to the committee, Payments Canada noted that its

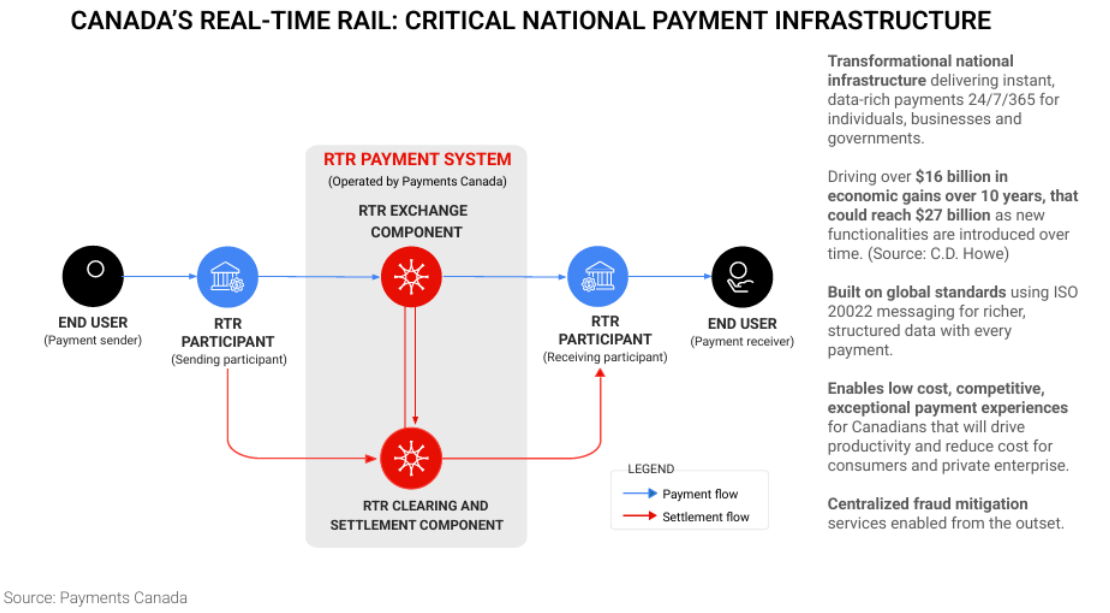
> biggest contribution to the fight against fraud, and a centrepiece of Canada's payment infrastructure innovation, is Canada's Real-Time Rail (RTR)[2], which is launching in Q4 of this year, with centralized fraud services. Combined with broader access to our membership and systems, the RTR will enable competition, innovation, economic growth and financial inclusion by delivering: instant, irrevocable payments with 24/7 availability [and] data-rich, ISO 20022[3] messaging.

2 The Real-Time Rail is Payments Canada's upcoming digital payment system that will clear and settle transactions of up to $100,000 in seconds. Payments will be final and immediate upon settlement.

3 International Organization for Standardization (ISO) 20022 is a single global standard for electronic data exchange between financial institutions.

Figure 2, below, illustrates the payment process of Canada's forthcoming RTR.

Figure 2—Payments Canada's Real-Time Rail



Source: Payments Canada.

Colin Smith noted that "[f]inancial institutions and clients can work together to fight fraud, but most fraud originates outside of the financial system." Illustrating this point, several financial institutions including Interac raised the issue of fraudulent advertising representing their companies on social media platforms, with Meta's Facebook and Instagram as common platforms for this fraudulent advertising. As an example, Colin Smith stated that Wealthsimple reported more than 10,000 fraudulent ads to Meta that were using the name and logo of the company for scams. He said that "it took an average of four days for these ads to be removed after [Wealthsimple] reported them to Meta." These examples raise questions about Meta's willingness to rapidly remove cases of fraudulent advertising on its platforms.

Witnesses from the banking and financial sectors commented on the Government of Canada's approaches and direction towards combatting financial fraud, with Frédéric Lapalme, Senior Director and Deputy Head, Fraud and Financial Crime Management and Supervision Unit, Desjardins Group, expressed Desjardins' support for the Government of Canada's commitments, noting that it "must avoid subjecting fraud to an overly rigid regulatory framework." He noted that the bank processes billions of transactions

annually and suggested that it "must be able to share this information with Interac and our colleagues at the banks to ensure that we use this data wisely to combat fraud."

David Shipley recommended against building a bank-only liability model. He suggested that this would lead fraud costs to grow for consumers because "the banks never pay these costs in the end. The costs will be passed on to your constituents in service charges and interest." Providing another view, Anthony Quinn, President, Canadian Association of Retired Persons, shared his opinion that banks "should take a higher level of responsibility" for losses from fraud. Fintechs Canada agreed that "tackling these risks requires a broader, ecosystem-wide response, not just point solutions," and suggested that "[o]nly by aligning incentives, clarifying roles, and enabling secure data-sharing across this wider ecosystem can Canada close the gaps that scammers exploit."

Telecommunications Companies

Eric Smith explained the role of that telecommunications companies as the providers who "deliver the envelope" but "do not read the mail." He noted that companies take measures including

> blocking certain types of calls; caller ID spoofing prevention tools, like do-not-originate programs and the implementation of STIR/SHAKEN technology;[4] call trace-back capabilities to help identify the origins of scam calls; network-level analytics to identify and flag suspicious communications; spam reporting systems; identity and account protections; and ongoing collaboration with law enforcement and government agencies.

Despite these efforts, Carey Frey, Chief Security Officer, Telus, pointed out, "[t]he unfortunate reality is that telephone calls and SMS messages can be impersonated." He noted that even though Canada's telecommunications industry has developed secure protocols to prevent impersonation, all countries would need to adopt them to be effective. Eric Smith agreed with this assessment, noting that if "technology is not adopted in the jurisdiction where a call has originated, for example, it doesn't provide that function." Anthony Quinn, speaking on behalf of retired persons, suggested that "telecoms providers must do more to authenticate calls, prevent spoofing and block fraudulent texts before they reach Canadians." He requested that "institutions, particularly banks and telecoms, be held to a higher degree of accountability in this and

4 Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted Information using toKENs (SHAKEN) is set of telecom protocols designed to stop illegal caller identification spoofing on Internet Protocol networks.

that they be part of the solution to preventing the frauds. I believe that if they were on the hook for some of these losses, they would be more likely to take action."

Carey Frey outlined certain limitations in stating that "telecommunications companies could block more fraudulent traffic on our networks, but today liability risk constrains what we can do." He noted that "[s]afe harbour laws protecting good-faith anti-fraud actions would help protect Canadians at no additional cost to taxpayers." In this context, a safe harbour law is a statutory or regulatory provision that would protect telecommunications service providers from liability if they accidentally block legitimate communications. Specifically, as Eric Smith identified,

> Section 36 of the *Telecommunications Act* prohibits telecoms providers from independently blocking communications without specific authority provided by the CRTC. This restriction is a fundamental element of Canada's net neutrality framework and exists to ensure that anti-fraud measures do not inadvertently block lawful traffic or interfere with critical communications.

According to Steven Harroun, Vice-President, Compliance and Enforcement, Canadian Radio-television and Telecommunications Commission (CRTC), "[i]n 2021, the CRTC approved an application by a Canadian telecommunications service provider to implement an [artificial intelligence] AI-based solution that can stop suspicious calls in the provider's network before they ever reach Canadians. Billions of these calls have already been blocked to date."

Social Media Platforms and Technology Companies

Social media companies are platforms where many fraud experiences begin. For example, as reported in The Sunday Times on 6 June 2026, the United Kingdom's Lloyds Bank found that more than two thirds – 68% – of fraud reports from its customers began on a Meta platform. The committee heard from social media platforms and technology companies, including Meta and Google, who shared their efforts to combat fraud and scams, and responded to questions about their companies' profits from fraudulent advertising. According to the Canadian Anti-Monopoly Project, "the liability of social media platforms is currently a legal gray area." Witnesses offered suggestions about regulating social media companies regarding fraud.

Jon Camfield, Defense Lead, Security Policy, Meta Platforms Inc., outlined that Meta "invests heavily in cross-sector information sharing," and listed Meta's fraud intelligence reciprocal exchange, or FIRE, a bidirectional signals exchange with financial institutions, and the Global Signal Exchange, which is a collaboration between Oxford Information Labs, Google and the Global Anti-Scam Alliance. In April 2026, the Canadian Cyber

Threat Exchange joined the Global Signal Exchange. Jeanette Patell outlined that Google has "invested for over two decades in advanced technologies, robust policies, legal action and expert teams dedicated to protecting the users of our products and services." She noted that in 2025, Google's artificial intelligence tool, Gemini, contributed to "catch[ing] over 99% of policy-violating ads before they ever served."

At the same time, a *Reuters* article from November 2025, reported that Meta projected that 10% of its 2024 revenue would be from ads for scams and banned goods. Jon Camfield clarified that the 10% figure was a "misinterpretation" and that 3% to 4% was the more likely figure for 2024. According to Meta Investor Relations, in 2024, Meta's total revenue was US$164.5 billion. Jon Camfield stated that in 2025, Meta achieved a reduction in the number of reported scam ads by more than 50%. Still, witnesses, including Wealthsimple and Interac, drew attention to the problematic use of their companies in fraudulent advertisements on Meta platforms. Wealthsimple stated that between October 2025 and January 2026, it reported 10,000 such ads on Meta platforms, and more recently, reported as many as 1,500 fraudulent ads in a day. When asked if Meta knowingly allows scammers on its site and keeps fraudulent advertisements on its site as part of a cost-benefit analysis, Rachel Curran, Director, Public Policy, Meta Canada, responded, "I'm going to disagree wholeheartedly with that. That's bullshit."

In its written submission to the committee, Meta further explained that over the past decade, globally, it has invested more than US$30 billion in safety and security, noting that it is difficult to define the investments in one specific country due to the transnational nature of fraud and scams. As outlined by Meta Investor Relations, in 2025, Meta's revenue was nearly US$201 billion. Since the company went public in 2012, cumulative revenue has exceeded US$1 trillion, and profits have exceeded US$328.5 billion.

Colin Smith stressed that reporting individual ads – which is the current approach for Wealthsimple regarding Meta ads – is a "losing game" and identified that Meta has not provided a platform level solution to address the issue in Canada. He noted that the "lasting solution is to require social media companies to verify that every advertiser of financial services is a legitimate, regulated entity, as the U.S., U.K., Australia, Hong Kong and six other countries already do today." In acknowledging that this verification is a "good solution" and "another tool" Frédéric Lapalme said, "[i]t won't solve everything, but the principle stands that the greater the anonymity, the higher the incidence of fraud. Clearly, a transparency requirement to help us understand the players involved, the payers and the funders behind the advertisements or other activities on different platforms remains a valid option." For Meta's part, Jon Camfield explained it is "expanding advertiser verification, with a goal of 90% of its ads revenue coming from verified advertisers by the end of 2026, up from 70% at the end of 2025."

When members of the committee asked if Meta was willing to use its platform to share news articles that provide actionable information about how to fight fraud, it refused, with Rachel Curran asserting that "[t]he Online News Act does not allow us to share even a single article on Facebook or Instagram unless we are subject to the entire framework that is set out in the Online News Act." Regarding the technical ability of Meta to remove links from its sites, be it fraudulent information or news, Rachel Curran claimed that Meta is complying with Canada's *Online News Act* by removing news content from its platforms. In speaking about the CRTC's interactions with Meta regarding the social media company's technical ability to remove news articles from being shared, Scott Hutton, Vice-President, Consumer, Analytics and Strategy, CRTC, stated that Meta had been taking a "light-handed approach" in blocking bona fide news sites. He noted that there are a limited number of such news sites, whereas in contrast, there are hundreds of thousands of fraudsters.

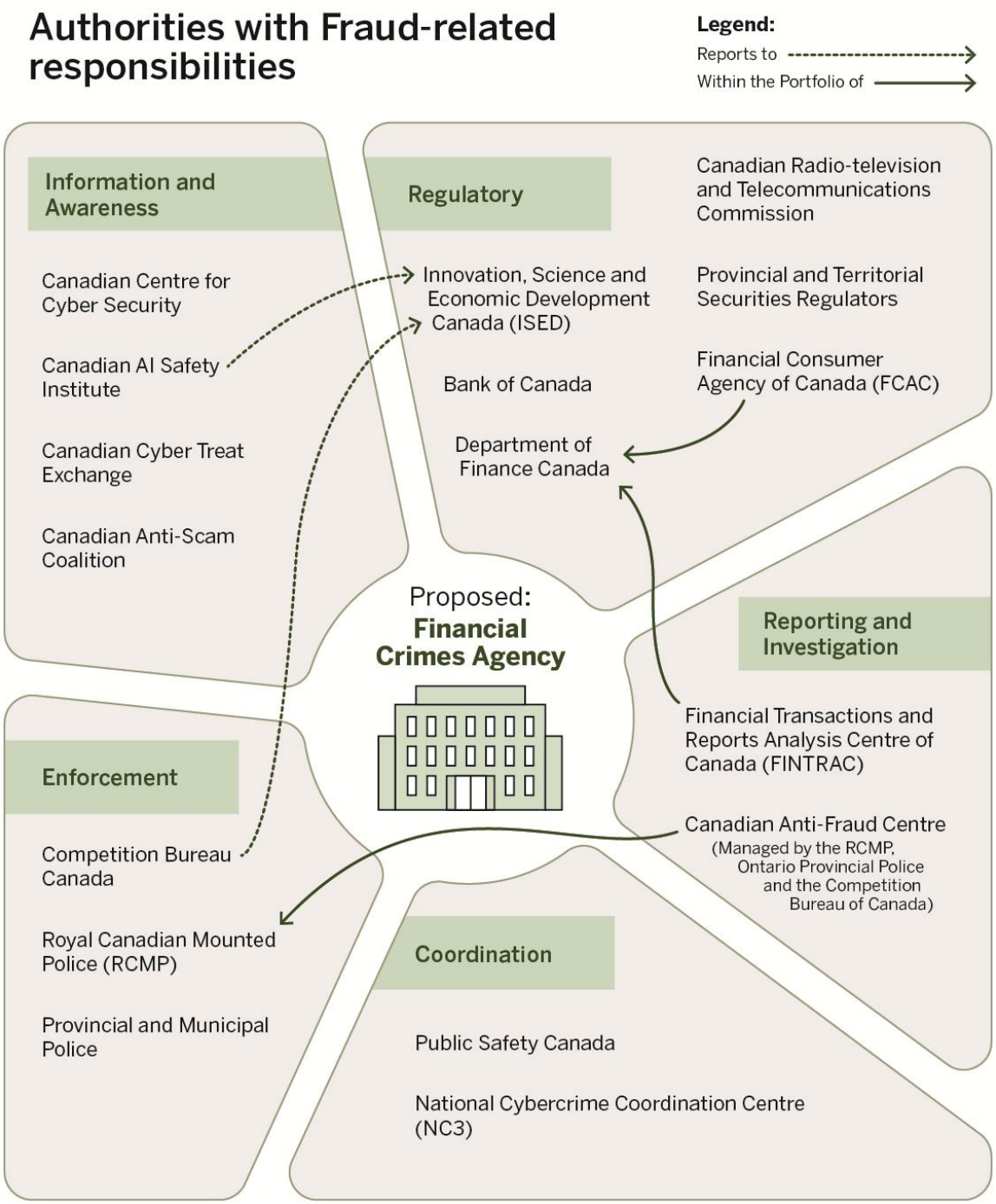
For Google, Jeanette Patell contended that Google "built [its] business model and our enforcement mechanisms so that we are not making profit from this. We are able to block these ads before they're ever seen by users, so that they don't enter our ecosystem." At the same time, in response to a question about whether Google would have collected revenue from a fraudulent YouTube advertisement during the duration that it was visible to Canadians, Jeanette Patell responded, "[i]t really depends; I don't have a good answer for you on what the revenue model would have been for a specific ad." Jeanette Patell noted that Google platforms such as YouTube have advertiser verification, with enhanced verifications for sensitive and higher-risk sectors such as financial services. Furthermore, Google does not allow most cryptocurrency advertisements and requires registration with FINTRAC for those it does allow.

A written brief from Reset Tech entitled *Clickbait Cures: Unmasking the Deceptive Health Ad Infrastructure on Meta and Google* investigated fraudulent medical advertising on Meta and Google platforms in the European Union, and found that the platforms were hosting fraudulent advertising that went against their own corporate policies. Reset Tech identifies that "[n]either Facebook nor Google systematically deplatforms problematic advertisers; instead, they focus mostly on removing individual ads. Unless addressed at a network level with stricter rules on health-related advertising, these campaigns will continue." Regarding the ability of Google to remove fraudulent advertisements, Jeanette Patell clarified that Google's role "is to assess content, including ads, for whether they are policy-violative. We cannot make a finding on whether they are fraudulent. That is the role of law enforcement."

CANADA'S APPROACH TO MANAGING FINANCIAL FRAUD

Regarding Canada's current legal framework, Carey Frey contended that "Canada already has much of what it needs to fight fraud more effectively. The Canadian anti-fraud centre, sector regulators, law enforcement agencies and the private sector coalitions are there. What is missing is a central coordinating force that ensures that the best tools and intelligence reach the people who need them." In a written brief, Kevin Cosgrove, a digital safety educator who submitted the brief in his personal capacity, suggested that "[t]he problem is that the current public-facing model remains too fragmented, too reactive, and too often focused on delivering information rather than ensuring that the public learns, remembers, and applies the message under pressure." Simlarly, Jennifer Quaid said, "If our response remains fragmented, we will continue to be outmanoeuvred." This section examines the legal framework in Canada, including consumer protection laws, law enforcement capacity and inter-agency coordination with regards to prevention, information sharing, liability and enforcement. Figure 3, below, provides a depiction of authorities with fraud-related responsibilities in Canada.

Figure 3—Authorities with Financial Fraud-related Responsibilities in Canada



Source: Prepared by the Library of Parliament using data from the Government of Canada.

Prevention and Education

Witnesses identified the role of Government of Canada agencies and initiatives to prevent fraud and to educate the public about fraud. Chris Lynam, Director General, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police (RCMP), outlined that the Canadian Anti-Fraud Centre, Canada's central agency for collecting information and intelligence on fraud, jointly managed by the RCMP, the Ontario Provincial Police and the Competition Bureau of Canada, "uses targeted messaging to promote public awareness of fraud threats on its website, via social media and through in-person engagements." Chris Lynam acknowledged, "[t]here is absolutely more work to be done to prevent [certain] solicitation scams from getting to Canadians."

Steven Harroun outlined the role of the CRTC as an administrator of the civil regulatory regime. He noted that the CRTC's prevention efforts include administering the do not call list, requiring service providers to block calls from numbers that are not normal, requiring service providers to implement STIR/SHAKEN, a technology to verify Caller Identification (ID), and working with the Competition Bureau and the Privacy Commissioner of Canada to monitor compliance within Canada's anti-spam legislation. He informed the committee about the *Compliance and Enforcement and Telecom Decision CRTC 2026-140*, released on 18 June 2026, which expands the ability of telecommunications companies to block botnets, which are networks of computers, cell phones, or other devices infected with malware, from reaching devices in Canada. At the same time, because of the CRTC's civil legislative jurisdiction, Steven Harroun acknowledged that "[t]here's not much that [the CRTC] can do about true fraud, true crime or true criminal behaviour." He noted that "as a regulator of a civil regime, education is critical, because the more Canadians are aware of scams, the less likely they are to become victims."

Witnesses commented on the role of education for the Government of Canada's anticipated National Anti-Fraud Strategy, announced in Budget 2025. Jude Pinto, Chief Delivery Officer, Payments Canada, outlined that Payments Canada's submission to the Government of Canada's consultation regarding the national anti-fraud strategy included the need for "strengthened, collaborative consumer education." Likewise, Jeanette Patell noted that Google agreed that "investing in public education" should be one of the three core principles of this national anti-fraud strategy. In a written brief, Questrade shared that part of the role of the forthcoming Financial Crimes Agency – announced in Bill C-29 – should be to provide prevention guidance and education for Canadians.

Regarding prevention and education as a means to combat fraud, Ian Paterson characterized it as "the first line of defence." Eric Smith suggested that "[h]elping Canadians recognize scams remains one of the most effective tools available." Jennifer

Quaid stated that "[p]revention must be [the Canadian Cyber Threat Exchange's] primary objective." David Shipley highlighted the role of teaching about emotional intelligence, noting that fraudsters often prey on the "loneliness epidemic in this country."

Still, Jon Camfield acknowledged, "[e]ducation is only one part of it. It really takes a lot of just-in-time messaging to get in front of people and prevent that engagement. It is a challenge." David Shipley cautioned that "[w]ithout a feedback loop, fraud awareness programs are just noise. With one—and we've proven this in our work in employee education—it guides people to less risky behaviours …That's shared responsibility." Concerning older adults, Mark Hines stated that "[e]ducation is vital, but we also have a role to play to make sure that we're building a wall around [older adults] a bit to protect them as well."

Providing another perspective, Anthony Quinn contended that for an older Canadian who might have lost a lifetime of savings, "educational programs, corporate platitudes, public relations campaigns and reminders to be careful are not enough." He reiterated that "education is only a small part of the problem. It has proven not to be effective." He opined that "awareness and education are important and likely the easiest to accomplish. That's why Canada has relied primarily on education over the last decade, but frauds and scams have been continuing to increase even as education has increased." He outlined that

> fraud prevention must become a system responsibility, not merely an individual responsibility... Digital platforms must also take greater responsibility for fraudulent advertisements, impersonation accounts, fake investment promotions and other scams distributed through their systems. Perhaps most importantly, financial institutions must strengthen their fraud detection and intervention before the money leaves the customer's account.

Regarding fraud literacy, Ian Paterson suggested "that not only is it a whack-a-mole game from a technology perspective, but it's also a whack-a-mole game from a legislation perspective."

Cross-Sectoral Data Sharing

Witnesses spoke about the importance of cross-sector and international data sharing, and the role of existing legislation and Government of Canada agencies to facilitate data sharing. According to Jennifer Quaid, "a bank, a telecommunications provider and a digital platform may each identify the same scam activity, yet there is no effective mechanism to share that intelligence in real time. As a result, each organization sees only part of the picture, while fraudsters share information instantly and exploit the gaps

created by siloed systems and outdated regulations." Accordingly, several witnesses, including Anthony Ostler, Mark Hines and Jon Camfield, emphasized the importance of "cross-sector" approach to sharing. Bernard Brun, Vice-President, Government Relations, Desjardins Group, identified that one of the key structural challenges was "fragmentation of data and information-sharing mechanisms." Likewise, from Australia, Nicholas Giurietto, Head of Future Policy, Australian Banking Association Inc., said "we remain more convinced than ever that the only way to minimize the devastating harm that scams cause to everyday Australians is a coordinated cross-sectoral ecosystem approach with each industry sector doing their bit.

Chris Lynam highlighted that the Canadian Anti-Fraud Centre and the RCMP's National Cybercrime Coordination Centre hosted Maple Disruption in 2025, which brought together partners together from the private and public sectors. During the exercise, information was shared and provided to the proper entities to take action. He assessed that this exercise "created some real efficiencies" in how to address real time information sharing. Meta and Google noted their participation in this exercise, which will again take place in 2026.

Concerning legislation around data sharing, Hartland Elcock, Assistant General Counsel and Vice-President, Canadian Bankers Association, outlined that the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which is Canada's federal private-sector privacy law, provides the privacy breach reporting obligations for private companies. Mark Hines noted that financial technology companies – including Interac – focus on the importance of consent and having the legal grounds to share data. He noted that within PIPEDA, there is a "a clear basis to process data for fraud." Providing a different perspective, the written brief from Fintechs Canada stated,

> Laws such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the *Bank Act* create uncertainty around the sharing of fraud-related information in ways that do not reflect how modern fraud operates. For example, PIPEDA's lack of a clear fraud definition can restrict the sharing of critical victim-related information.

Witnesses Carey Frey, Jon Camfield, Jennifer Quaid, Mark Hines, Fintechs Canada and the Future of Financial Intelligence Sharing, drew attention to the importance of safe harbour provisions for intelligence sharing, which exist in other jurisdictions including Australia. With Mark Hines, stating that the "safe harbour provision encourages the type of intelligence sharing that we think is key if we're going to stop the problem at the outset." Nicholas Giurietto suggested, "[t]he key role of government is to provide the policy framework that enables secure and privacy-compliant data exchange with appropriate safe harbour protections."

Concerning Canada's legal framework surrounding information sharing, Carey Frey pointed out that certain existing policies in Canada may unintentionally assist fraud, highlighting "the CRTC's customer confidentiality regulations restrict cross-industry information-sharing. Another example is the CRTC's device unlocking rules, which currently make it easier for criminals to defraud Canadians of their smartphones, leaving them with significant debt and damaged credit scores."

Within this current framework, Jennifer Quaid contended that Canada needs "a framework that breaks down silos, enables real collaboration, provides meaningful resources where they are needed and puts prevention at its centre." She highlighted that the Canadian Anti-Scam Coalition and the Canadian Cyber Threat Exchange, which are both voluntary groups that bring together the private sector and governments, "stand ready to help build that framework."

Liability for Fraud in Canada

As outlined in a brief submitted by the Canadian Anti-Monopoly Project, "[i]n Canada, the legal frameworks for the liability of online scams are not comprehensive, and there is limited recourse available for individuals." The brief distinguished between unauthorized and authorized fraud, noting that financial institutions may be liable in some unauthorized cases. Accordingly, "banks have developed more sophisticated techniques for preventing unauthorized fraud." As a result, "scammers have adapted" to focus on pig butchery[5] or romance scams, where the scammer earns the trust of the victim, who transfers them money voluntarily, known as an authorized scam. In an authorized scam, "the victim of a scam is likely out of luck." The brief pointed out the added complications with the rise of cryptocurrency, where "there may be even less recourse for victims, as cryptocurrency transactions are irreversible, and are often done without involvement of any regulated financial institution."

As outlined in a written brief submitted by Peter Squire, who, according to *CBC News*, lost nearly $650,000 due to an example of such authorized fraud, Canada should shift from a principle of "consumer beware" to one of "system responsibility." He advocated for a mandatory reimbursement model that would "[r]equire financial institutions to compensate victims where fraud prevention systems fail or warning signs were missed." Similarly, in agreeing that a platform hosting a fraudulent advertisement should share liability, Anthony Quinn shared his view that "[w]e have arrived at a situation in Canada

5 A pig butchery scam is a long-term online fraud that includes romance based on a metaphor that the victim is a pig who is fattened up with trust, friendship or love before being slaughtered for financial gain.

of blaming the victims for not educating themselves or not being aware enough. I believe we have to turn the tables to protect Canadians."

Witnesses commented on the role of liability and shared views about which actors are or should be liable in cases of fraud. Mark Hines pointed out that, "as the network in the middle, [Interac does not] take a direct role in compensating victims of scams. That's managed by our participants, usually a financial institution." He noted Interac's proposal that "each actor in that chain—the platform, us, the bank and the individual—has specific obligations. If we don't meet them, then we should hold some level of responsibility for it." Frédéric Lapalme outlined that in certain cases, "the financial institution would bear much of the responsibility for whether the victim is compensated. However, as we have shown today, a whole chain of stakeholders all share responsibility. As a result, the Canadian Anti-Scam Coalition and other initiatives designed to bring all stakeholders together are all the more important."

When asked if Google reimburses victims of fraud for losses incurred, Jeanette Patell stressed the complexity and stated that Google "recognize[s] the human cost here, and we also recognize that we need to have criminals held accountable for their actions. The written submission from Google shared the corporation's view that it

> believe[s] that a balanced approach, emphasising both user education and technological solutions as well as law enforcement that directly target fraudsters and associated organised crime, as well as cooperation among stakeholders such as industry and government agencies, will be more effective than introducing financial penalties for platforms.

From the perspective of the Canadian Anti-Fraud Centre, Chris Lyman shared that

> [he was] not sure [he was] well placed to give an analysis of where liability lies. I would say that all the digital platforms have a key responsibility in addressing the fraud and cybercrime challenges facing this country. We've had some great relationships for figuring out how we can send them information and how they can send us information, but there's more to be done. There absolutely is more to be done across the spectrum for the role of digital platforms in this.

Enforcement

Witnesses discussed the different aspects of enforcing Canada's legal framework surrounding fraud and scams. As Mark Hines stated, however, "[e]nforcement matters, but enforcement acts after harm is done."

Concerning the repayment of money collected from fraudsters who are found liable, Sarah Corrigall-Brown, General Counsel, British Columbia Securities Commission, raised

an issue concerning the *Bankruptcy and Insolvency Act*, that prevents the British Columbia Securities Commission from collecting money to repay the victims of fraud because the act "treats the penalties imposed by securities regulators for egregious misconduct the same as consumer debt. This means people who have been penalized for significant market misconduct can have their penalties erased through the bankruptcy process." She recommended that the *Bankruptcy and Insolvency Act* be amended to include fraud, market manipulation and misrepresentation as types of debt that would be obliged to be paid even in bankruptcy.

Hartland Elcock explained the money laundering, terrorist financing and sanctions evasion role of FINTRAC, in that it is "not the predicate offences of fraud; it's the treatment of the money after those initial incidents, and what FINTRAC does is package that information to send it on to law enforcement." He clarified that FINTRAC is "an intelligence agency rather than an enforcement agency. Our members are the largest reporters to FINTRAC of suspicious transactions, which is where an institution has seen suspicious activity that leads to reasonable grounds to suspect money laundering, and it sends that information to FINTRAC." Regarding the effectiveness of the roles of FINTRAC and the Canadian Anti-Fraud Centre Frédéric Lapalme stated that

> Desjardins interacts with both on a daily basis. Law enforcement agencies can send us requests to carry out investigations. Depending on the reporting thresholds, we provide FINTRAC with information on hundreds of thousands of transactions each year. Unfortunately, we often send information—reports—to FINTRAC, only to receive a direct request from a law enforcement agency investigating the same case. This means that organizations on both sides of the information-sharing process stand to benefit.
>
> Regarding the agency, we would like to see the investigations lead to arrests. This aligns with the Financial Action Task Force's recommendations, published five years ago, and likely with the next report scheduled for release. We want to ensure that the system effectively combats both fraud and financial crime—these areas may overlap—in order to achieve the concrete result of an arrest and a conviction. Prevention is useful. However, certain situations reach a point of no return that requires investigations and, unfortunately, formal charges.
>
> This is where we would potentially like to see the agency or another organization step in. Investigations into financial crimes require a level of expertise that not every law enforcement agency in Canada possesses.

Carey Frey recommended that law enforcement be provided "with the explicit mandate and necessary resources to effectively apprehend fraud perpetrators and dismantle their technical apparatus."

BEST PRACTICES: LESSONS FROM AUSTRALIA

Australia is moving from voluntary anti-scam cooperation toward a mandatory, multi-sector scam prevention regime through Australia's *Scams Prevention Framework Act 2025* (SPFA) received Royal Assent on 20 February 2025 and amends the *Competition and Consumer Act 2010*. The SPFA makes scam prevention a shared legal responsibility across designated sectors. It requires regulated entities to put measures in place to prevent, detect, report, disrupt and respond to scams. The Government of Australia is initially focusing on banking, telecommunications and certain digital platform services because these sectors are major pathways through which scams are perpetuated. Nicholas Giurietto noted that while the SPFA legislation passed, "it is still in the process of implementation." He suggested that "the most effective component of the legislation is the fact that it frames the responsibilities of each sector as equivalent but different."

As stated by Nicholas Giurietto, "[t]he Australia scam prevention framework has attracted a lot of attention around the world as the first example of an anti-scams regulatory regime based on the principle that all industry sectors must do their share to tackle scams." He noted that other sectors involved in scams would need to be part of a coordinated response, including "crypto exchanges, non-bank money remitters, remote access software providers, online marketplaces, gift card providers and many more." Anthony Ostler highlighted that Australia is responding to fraud through a "cross-sector public-private approach," which he deemed as "essential." He stated that while Australia had reduced scams by 30% since 2022, scams had increased in Canada by 32%.

Anthony Ostler and Hartland Elcock provided an example of the regulatory burden on Canadian institutions compared with Australia's, noting that while Canada's FINTRAC has 400 fields for suspicious transaction reporting, Australia's equivalent reporting has 30 to 50 fields. These witnesses contended that by reducing the number of fields, it would be easier to obtain useful information that would empower law enforcement. With too many fields, there are diminishing returns to the increase in disaggregated data.

Anthony Ostler contended that fraudulent advertisements are not removed as quickly in Canada as they are in Australia. Nicholas Giurietto highlighted that "for the platforms, if someone wants to advertise a financial product, check that they actually hold an Australian financial services licence, which is the licence that's required to offer investment products in Australia, before you allow them to advertise their product."

Concerning obligations to counter fraud, Australia differs from Canada in that all sectors, including banks, social media platforms, telecommunications companies and futures sectors are equally responsible for their share. Nicholas Giurietto said that if banks alone are responsible, "you end up trying to stop the fire when it's already ranging." He

suggested that if telecommunications companies and platforms take action earlier, it is possible to intervene in scams at an earlier time, and information can be shared to prevent future victims.

Concerning lawful access – which for Canada, lawfully allows police and intelligence agencies to intercept communications and search and seize information under the *Criminal Code,* the *Canadian Security Intelligence Service Act,* and other Acts including the *Competition Act* – as Nicholas Giurietto said, "Australia has a federal system with overlapping police responsibilities that can sometimes make things a bit complicated to navigate, but being able to do the intelligence sharing and take action—either sharing the intel or, in some cases, supporting law enforcement in taking action—is very important." He also stressed the importance of "private-to-private data sharing [which] is at least equally important, in that sometimes the private sector can use so-called scam signals that fall short of the legal standard that law enforcement might need to meet before they can initiate a prosecution or some other action." In highlighting the intelligence sharing among private sector participants, state and federal law enforcement agencies, David Pegley pointed out that unfortunately, most of the bad actors affecting Australia are from offshore.

Witnesses also drew attention to Australia's different institutions to address fraud. David Pegley described the functions of the Australian Financial Crimes Exchange, an independent non-profit which provides intelligence sharing between approximately 100 members across eight different industries, including digital media, telecommunications companies, insurance companies, banks and digital currency exchanges. Jennifer Quaid highlighted that Australia created the National Anti-Scam Centre. With regards to Australia's efforts to address fraud, Nicholas Giurietto noted that, "[o]ver time, it makes it a more expensive proposition for the scammers to target Australia, as opposed to another country, so they might put their efforts elsewhere."

CONCLUSION

The committee's study on fraud and scams in Canada is timely. According to the Canadian Anti-Fraud Centre, between 1 January 2026 and 30 June 2026, there have been 9,935 victims of fraud in Canada, with $351 million in reported losses. This study revealed that there remain areas for Canada to improve its fraud prevention, detection, reporting, and liability enforcement mechanisms. The committee remains concerned with the apparent lack of accountability and responsibility on the part of the social media platforms in relation to the gravity of the issue of financial fraud on their platforms. Social media platforms, banks and telecommunications companies all have a role in addressing the growing issue of fraud in Canada. Witnesses advocated for a

central coordinating body and greater mechanisms for cross-sectoral information sharing. Australia, as one of the only countries that has seen a reduction in fraud in recent years, offers policy options for Canada, including a cross-sector private-public approach to tackling fraud, and cross-sectoral responsibility for fraud. Through 18 targeted recommendations, the committee urges the Government of Canada to take action to address this important issue that affects so many Canadians.

APPENDIX A:
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Canadian Bankers Association	2026/06/04	42
Hartland Elcock, Assistant General Counsel and Vice-President		
Anthony Ostler, President and Chief Executive Officer		
Canadian Telecommunications Association	2026/06/04	42
Eric Smith, Senior Vice-President		
TELUS	2026/06/04	42
Carey Frey, Chief Security Officer		
Australian Banking Association Inc.	2026/06/08	43
Nicholas Giurietto, Head of Future Policy		
Australian Financial Crimes Exchange Ltd.	2026/06/08	43
David Pegley, Managing Director		
Beauceron Security	2026/06/08	43
David Shipley, Chief Executive Officer		
Canadian Cyber Threat Exchange	2026/06/08	43
Jennifer Quaid, Executive Director		
Meta Platforms Inc.	2026/06/08	43
Jon Camfield, Defense Lead, Security Policy		
Rachel Curran, Director, Public Policy, Meta Canada		
British Columbia Securities Commission	2026/06/11	44
Sarah Corrigall-Brown, General Counsel		
Canadian Association of Retired Persons	2026/06/11	44
Anthony Quinn, President		

Organizations and Individuals	Date	Meeting
Payments Canada	2026/06/11	44
Jude Pinto, Chief Delivery Officer		
Plurilock Security Inc.	2026/06/11	44
Ian Paterson, Chief Executive Officer		
Royal Canadian Mounted Police	2026/06/11	44
Chris Lynam, Director General, Canadian Anti-Fraud Centre		
Wealthsimple	2026/06/11	44
Colin Smith, Vice-President, Risk and Decision Science		
Canadian Radio-television and Telecommunications Commission	2026/06/16	46
Steven Harroun, Vice-President, Compliance and Enforcement		
Scott Hutton, Vice-President, Consumer, Analytics and Strategy		
Desjardins Group	2026/06/16	46
Bernard Brun, Vice-President, Government Relations		
Frédéric Lapalme, Senior Director and Deputy Head, Fraud and Financial Crime Management and Supervision Unit		
Interac Corp.	2026/06/16	46
Mark Hines, Head of Fraud Product		
Google Canada	2026/06/18	47
Jeanette Patell, Director, Government Affairs and Public Policy, Canada		

APPENDIX B:
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Canadian Gaming Association

Cosgrove, Kevin

Democracy Watch

Equifax Canada Co.

Fintechs Canada

Foster, Pamela

Google Canada

Questrade Inc.

Shakepay Inc.

Squire, Peter

Tru Cooperative Bank

Visa Canada Corporation

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 42, 43, 44, 46, 47, 48 and 51) is tabled.

Respectfully submitted,

Ben Carr
Chair