HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

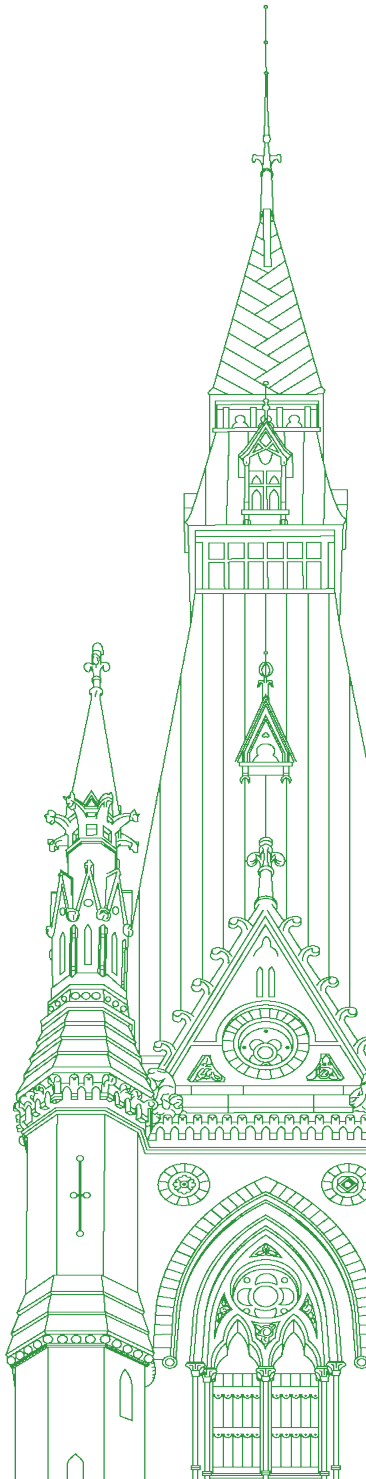
45th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 044

Thursday, June 11, 2026



Chair: Ben Carr

Standing Committee on Industry and Technology

Thursday, June 11, 2026

● (1100)

[*English*]

The Chair (Ben Carr (Winnipeg South Centre, Lib.)): Good morning, colleagues. We're going to get going here. I'm asking staff and others who are engaged in conversations to keep the noise level down, please.

Colleagues, we're continuing our study on fraud. This is now the third meeting that we have had on this topic here at the industry committee.

Witnesses in the room, I will remind you that if your earpiece is plugged in but not on your ear, to please ensure that it's on the sticker in front of you to protect the health and well-being of our interpreters.

[*Translation*]

I can also confirm that we've completed all the visual and audio tests.

[*English*]

We have two witnesses joining us virtually today in addition to one in the room. From the British Columbia Securities Commission, we have Sarah Corrigall-Brown, general counsel.

I do understand, Ms. Corrigall-Brown, that in the wee hours of the British Columbia morning, you were very accommodating of the necessity for us to get all of our tests done, so we want to thank you off the top for your co-operation in that regard.

From Payments Canada, we have Jude Pinto, chief delivery officer, who is here in the room with us today, and from Plurilock Security, we have Ian Paterson, chief executive officer.

Witnesses, you'll each have up to five minutes for introductory remarks, at which point we will turn to colleagues around the table for questions and answers.

With that, Ms. Corrigall-Brown, I will turn the floor over to you for up to five minutes for your introductory remarks.

Sarah Corrigall-Brown (General Counsel, British Columbia Securities Commission): Dear Chair and members of the committee, thank you very much for the invitation to be with you and to contribute to your important study regarding financial fraud and scams in Canada.

My name is Sarah Corrigall-Brown. I'm the general counsel of the B.C. Securities Commission. I'm joining you virtually today from Vancouver.

The scourge of financial fraud has been around for a long time, but in the past decade and especially since the pandemic, it has spread and intensified like a mutated virus that is many times more contagious and virulent than ever before. We are very pleased to see the actions the federal government is taking to address fraud, including the government's intention to launch a new financial crimes agency.

The B.C. Securities Commission and Canada's securities regulators, which keep watch over the country's investment markets and contribute to the integrity of Canada's financial system, have been on the front lines of this battle. Securities regulators have a mandate to protect investors from fraudulent, manipulative and misleading practices. We see the exponential growth of financial fraud as one of the greatest threats to investors today.

Prevention and detection of fraud is essential, but combatting fraud also requires strong and effective enforcement. Today, I want to talk to you about one aspect of Canadian law that is undermining our enforcement efforts.

When fraudsters are located in Canada, securities regulators like the BCSC take formal action through administrative tribunal proceedings. These tribunals, which are composed of recognized experts in securities law and bound by rules of procedural fairness, have the power to exclude lawbreakers from the investment market and to impose financial penalties on them. Those penalties sometimes reach into the millions. They are key to deterring further misconduct by the lawbreakers themselves, but they also deter misconduct by others who might be tempted to defraud unsuspecting investors. For those penalties to have deterrent power, however, it is not enough for our tribunals to hand down legal orders. We need to be able to collect sanctions; otherwise, they are penalties in name only.

There are many obstacles that lawbreakers can exploit to block our collection efforts. One of them is a federal law, which is the Bankruptcy and Insolvency Act, or the BIA. The BIA is designed to enable the financial rehabilitation of honest but unfortunate debtors and give them a fresh start by releasing them from their debts upon discharge from bankruptcy. The BIA does this well, and Canada's securities regulators wholeheartedly support that objective.

However, the BIA 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. These are people whose debts result from their own predatory behaviour toward other Canadians and who are seeking to avoid paying those debts. When they do this, it undermines Canadian securities regulators' efforts to enforce the law and protect investors from fraud.

To pick one example from Alberta, Saileshwar Narayan admitted to committing fraud in mortgage financial schemes in which investors lost $4 million. One month after the Alberta Securities Commission ordered him to pay a $300,000 administrative penalty, he entered bankruptcy and was discharged from bankruptcy 10 months later. The penalty was erased, and the ASC collected only $6,300 toward Narayan's debt.

We believe examples like this undermine confidence in the ability of the Canadian regulatory regime to hold fraudsters accountable for their actions. This undermines the foundation of honesty and fairness that we all expect of Canada's markets. We also believe they fly in the face of the federal government's laudable crackdown on financial crime. There is, however, a fix.

The BIA has a list of debts that Parliament has decided should not be extinguished in a bankruptcy. We and all other Canadian securities regulators ask that Parliament add to this list the financial sanctions imposed by Canadian securities regulators for the most egregious types of market misconduct: fraud, market manipulation and misrepresentation.

We have spoken about this request with ISED officials and have made submissions to the House finance committee and the Department of Finance. The Government of B.C. and all securities regulators across Canada support this request. It is also supported by a range of organizations, including the investor advocacy group FAIR Canada, the Consumers Council of Canada, CFA Societies Canada and the Canadian Association of Retired Persons.

Making this change to the BIA would have no impact on the honest but unfortunate debtors that the BIA aims to serve, and it would impose no additional burden on the bankruptcy courts that ably carry out the BIA's crucial mission. It would reconcile provincial securities law and federal bankruptcy law that, in this particular respect, are working at cross-purposes.

It would also serve a more practical imperative. As Canada seeks to become as economically competitive and resilient as possible, we must ensure that our market is seen as honest and fair, and therefore a safe place to invest. A crucial component of that effort is strong and effective enforcement to hold individuals accountable when they harm our market through fraud, market manipulation and misrepresentation.

I ask that you consider our proposed amendment to the BIA as a meaningful way to support strong enforcement and enhance the fight against financial fraud in Canada.

Thank you again for your time today. I welcome any questions.

● (1105)

The Chair: Thank you very much.

I'm going to turn the floor now to you, Mr. Paterson. You have up to five minutes for your introductory remarks, sir.

Ian Paterson (Chief Executive Officer, Plurilock Security Inc.): Thank you, Chair and members of the committee, for the invitation.

My name is Ian L. Paterson. I'm the CEO of Plurilock, a Canadian cybersecurity company. For 10 years, I've built and patented systems that verify who people are and delivered cybersecurity for government agencies and businesses. I'm here as an operator with a practical view of why fraud works and what would slow it down.

I'll offer three recommendations to combat the fraud that's hurting everyday Canadians, but first I'll start with a story.

A grandfather gets a phone call. He hears his grandson's voice: He's been in a car accident and needs money right now. The grandfather drives to the bank, gets the funds and hands a money order to a stranger who showed up in person to collect it. Only later, when the family compared notes, did the truth come out. The grandson was fine. The voice was a deepfake. It was a fraud.

That's one story. I have many, as I think most Canadians do.

Canadians reported $704 million in losses to the anti-fraud centre in 2025, which was the worst year on record. The RCMP estimates that only 5% to 10% of fraud ever gets reported, which means the real cost to the Canadian economy runs into the billions.

What do we do? In cybersecurity, we talk about prevention as “left of boom” and response as “right of boom”.

First, on left of boom, prevention comes down to identity.

Fraud works because we still verify people with things that are easy to fake: phone numbers, text messages, passwords and, now, voices. Back in 2019, I wrote in The Globe and Mail that my video game provider had better security than my bank. Seven years later, not much has changed, and deepfakes and voice cloning are letting bad guys automate and scale their attacks.

The fix is stronger identity that everyday Canadians can trust. When your telco, your bank or your government reaches out, it should come over a channel that can't easily be spoofed, like a push notification from a smart phone app. When you sign into a service, it should be with credentials that can't easily be phished, like passkeys, which no one could read over the phone to a criminal. When it's human to human, the answer is resilience. Criminals can fake a phone number and a familiar voice, so hang up, call back a number you know and ask about shared context like, “What did Aunt Bertha bring to Christmas dinner last year?”

Cheap habits beat expensive technology. That grandfather in the story wasn't careless. He did what all of us were taught to do: trust the voice on the line. That's what has to change, and it's fixable.

Government should go first. Every Canadian knows about the fake CRA calls. If the CRA and agencies like it used channels that can't easily be spoofed, they'd end one of the most common scams in the country and set the standard for everyone else.

Second, on right of boom, response comes down to coordination.

When the victim, the bank, the phone company and the criminal sit in different jurisdictions, the first question is always, who owns the file? Our police officers are some of the most mission-driven people I know, but too often the local police agency that ends up with the file doesn't have the training, tools or mandate to chase this kind of crime, and that police detachment has to weigh a $5,000 scam against an armed robbery down the street. The criminals count on that weakness and exploit it.

We have a start with the national cybercrime coordination centre, but its role is to support. The investigating still falls to individual officers. Canada needs a national response that leads these cases, not just supports them: one that cuts across jurisdictional boundaries and brings banks and telecoms to the table with privacy built in and a mandate to chase these crimes whatever the dollar amount.

Third, Canada cannot tackle these issues on its own. Some 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. We need to invest more in international assistance to help dismantle these networks at the source, before they reach Canadians.

Fraud is an identity problem, a coordination problem and a test of our resilience. Every day, Canadians are being electronically mugged by criminals who've turned this into an industry, one that runs on the seams in our system. Those seams are ours to close.

Thank you. I look forward to your questions.

● (1110)

The Chair: Thank you, Mr. Paterson.

Mr. Pinto, I'll turn the floor over to you now, sir, for up to five minutes.

Jude Pinto (Chief Delivery Officer, Payments Canada): Thank you, Mr. Chair, and thank you all for the invitation to appear today.

As Payments Canada's chief delivery officer, I lead large-scale delivery programs, including Canada's real-time rail and its central fraud services. I have over 35 years of experience in transforming financial technology and operations.

Payments Canada owns and operates the critical national payments infrastructure—the systems, rules and standards that help keep Canada's economy moving. Established by the Canadian Payments Act, we are a national public-purpose organization that operates on a non-profit basis. Our board of directors is majority-independent, and the Minister of Finance is responsible for our enabling legislation.

Our systems, which are overseen by the Bank of Canada, include Lynx, Canada's high-value payment system, used by participants to clear and settle primarily wire payments and large-value payments; the automated clearing settlement system, ACSS, which clears and settles retail batch payments, like direct deposits and debits; and Canada's forthcoming real-time rail, which I will speak to in a moment.

In 2025, our system safely cleared and settled $103 trillion among institutions. Our vision is to enable prosperity, productivity and safety for Canada through trusted, world-class payments. Our legislated public policy objectives are to promote the efficiency, safety and soundness of our systems.

Our perspective on fraud requires a clarification on the unique role we play. Payments Canada's systems, rules and standards allow our system participants, including financial institutions, payment service providers and credit unions, to move funds safely between one another. We do not hold, have visibility to or manage any individual customer bank accounts, nor do we see any private data. However, as fraud threats evolve, we all have a role.

Our own research reinforces the rate at which fraud threats are growing. These threats are not evenly distributed across Canada's demographics, often targeting Canada's most vulnerable.

Fraud arises through multiple channels, sectors and parties. There's no single solution nor institution that can solve it in isolation. This is why Payments Canada strongly supports the Government of Canada's establishment of the financial crimes agency and its commitment to develop a national anti-fraud strategy.

Our consultation submission on that strategy emphasizes the need for purpose-driven data sharing across sectors; coordinated regulation and oversight to ensure fair, predictable outcomes across industries; and strengthened, collaborative consumer education.

Payments Canada is also an active member of the Canadian anti-scam coalition.

Our biggest contribution to the fight against fraud, and a centrepiece of Canada's payment infrastructure innovation, is Canada's real-time rail, or RTR, 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, 24-7 availability and data-rich ISO 20022 messaging.

We have benefited from extensive engagement and learnings from other jurisdictions that have found that while new risks emerge, real-time transactions can be safe transactions.

No payment type is immune to fraud. That's why Canada will be the first to launch its national real-time payment system with mandatory fraud mitigation on day one.

These four requirements are, one, real-time fraud transaction scoring with network-level insights to inform fraud management and payment decisioning; two, a centralized intelligence platform that provides national reporting with aggregated fraud insights; three, a shared and centrally managed risk list to track and flag attributes of those involved in confirmed fraud; and, four, confirmation of payee capability, allowing individuals to verify the account identity of the recipient.

The RTR's use of the ISO 20022 messaging standard will unlock powerful new analytics, allowing participants to better track and disrupt complex fraud patterns. Further, the RTR is designed to facilitate compliance with anti-money laundering requirements for cross-border indicators.

Modernizing Canada's payment infrastructure is a nation-building exercise. Payments Canada is fully committed to supporting collaborative efforts to safeguard Canadians in this pivotal era for payments.

Thank you, and I look forward to your questions.

● (1115)

The Chair: Thank you very much, Mr. Pinto.

Colleagues, we will now turn to our round of questions.

Mr. Falk, the floor is yours for six minutes, sir.

Ted Falk (Provencher, CPC): Thank you very much, Mr. Chair.

Thank you to all of our witnesses for their testimony here.

Mr. Pinto, I would like to begin my questions with you. Your organization, Payments Canada, primarily deals with transactions between institutions.

Jude Pinto: That's correct.

Ted Falk: At what end of the transaction do you typically find instances of fraud?

Jude Pinto: That's a great question.

If a transaction is split between the exchange of values between end consumers and businesses, that part we don't typically get involved in. Historically, the settlement between the sender and the receiving institution or bank is the part that we clear through Bank of Canada settlement accounts. That mix of exchange, clearing and settlement through Bank of Canada accounts with RTR actually gets combined; all three of those steps start happening in a subsecond transaction.

That's why it was important.... With regard to RTR, it's the first time we have purview into some of the origin of where fraud occurs. The discussions we've been hearing so far are generally at the exchange level.

Ted Falk: You're very excited about RTR coming on later this year, and you believe that's going to assist you in minimizing and reporting real-time scams and fraud.

Jude Pinto: Yes.

Ted Falk: Is there anything that can be done between now and then to mitigate some of the fraud that's happening in the system today?

● (1120)

Jude Pinto: The answer globally is yes. From Payments Canada's purview, we currently operate Lynx and ACSS, and we're one quarter away from launching our first foray into fraud and the exchange layer of payments. That might be more the purview of the banks and institutions that are currently involved in the exchange of transactions today, versus Payments Canada, which is involved in the settlement.

Ted Falk: Are you involved in all the settlements in Canada?

Jude Pinto: Yes.

Ted Falk: Your organization participates—

Jude Pinto: In fiat currency...?

Ted Falk: Yes.

Jude Pinto: Yes.

Ted Falk: Thank you for clarifying that.

Mr. Paterson, I'd also like to ask you some questions.

In your story of the grandfather being scammed.... At a previous committee meeting, we had testimony from Meta here. One of the questions we posed to Meta was on its level of accountability as the one providing the conduit or the medium through which scamming is happening. What degree of responsibility do you think the mediums should hold?

Ian Paterson: When we're talking about fraud prevention, this is really a societal-level resiliency exercise that we have to go through. Certainly, technology platforms—be they social media platforms, banks, telcos, etc.—can all play a role. I don't think there's any one platform or any one provider that stands out to me as a bigger issue than the others.

The larger aspect to this problem is that there are certain habits, customs and practices that we, across society, have adopted, whether implicitly or explicitly. These are things like logging in with a password, trusting that a phone call that you get is coming from an authorized person and believing that the voice you hear belongs to that person. Those are actually the root causes of how some of this fraud is perpetrated. Those are the things I believe we need to address.

Ted Falk: Some of the information that we had here at committee was that two-thirds of scams happen on Meta platforms. You don't believe that Meta has a responsibility in this aspect.

Ian Paterson: All technology platforms have a responsibility, but I would also say that email and SMS messages carry a large chunk of scams as well. The reality, certainly from what I have seen over my career over the last 10 years, is that bad guys will adopt whatever is being used. If Meta is the most popular platform, that's where they're going to go, absolutely. If WhatsApp becomes the dominant communication platform, I fully believe that will become the number one platform they use.

I don't think it's any one company's responsibility. I do genuinely believe we can all play a leadership role in increasing the resiliency across society.

Ted Falk: How do you think Plurilock would fit into the equation of reducing scamming and fraud?

Ian Paterson: Plurilock is primarily a B2B company. We typically don't work directly with consumers, although, given our leadership in the cybersecurity space, I am frequently the guy people call when they get into a problem. That story I shared with you about the grandfather was about somebody in my network who approached me, simply asking for help.

As it pertains to helping organizations become cyber-resilient, certainly that is something we do. I will give the caveat that my organization historically has done significantly more business in the United States. I'm here principally as a Canadian citizen looking to share my experiences to make Canada a safer and more prosperous nation.

Ted Falk: Thank you.

Finally, to Ms. Corrigall-Brown, do you believe that we currently have adequate resources to prosecute people who are charged with crime and fraud offences?

The Chair: Answer in a tight 30 seconds, please, Ms. Corrigall-Brown.

Thank you.

Sarah Corrigall-Brown: Certainly, we, the federal government and Crown agencies make do with what we have. There's always—as we've all identified—the scope of the problem and the scope of the harmed Canadians.

We absolutely welcome the federal government's focus in this area and the opportunity to partner with securities regulators. I agree with what my colleagues have said. It needs to be a national, full-society response. The allocation of resources and attention to this matter is important and necessary.

The Chair: Thank you, Mr. Falk.

Mr. Bains, you're online today. The floor is yours for six minutes, sir.

● (1125)

Parm Bains (Richmond East—Steveston, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for joining us for this very important study.

Mr. Paterson, you shared a story, but there are so many that I've heard from constituents and family members. We ourselves get these calls and SMS messages. It's a rather complex problem that we're dealing with. It's a global issue. We're ultimately seeing issues around extortion. We're trying to wrap around all of these different ways that people are being attacked.

I was wondering if you can very quickly share how the cyberthreats facing different organizations and governments differ between Canada and the U.S. Is there a specific vulnerability that you can point to? What do fraudsters most commonly exploit as targets? It could be systems that each government has or the regulations that they have in overseeing some of these platforms like Meta and WhatsApp.

Can you share something on that?

Ian Paterson: Thank you for the question.

I could speak to the [*Technical difficulty—Editor*] resilience and also vulnerabilities.

I think one of the things that will come as no surprise to anybody here is that AI has really made scams [*Technical difficulty—Editor*] to author perfect English, whereas previously one of the most common ways of identifying if an email was real or fraudulent [*Technical difficulty—Editor*].

The Chair: Mr. Paterson, I'm not sure if it's on our end or your end, but unfortunately we're getting a little bit of choppiness. I'm going to let it go one more time. If it disconnects, it just makes things a little bit too difficult for the interpreters to work with. I may have to circle back to you—if we get a correction in that connection.

I'm looking now, and you appear to be frozen.

Mr. Bains, I'm going to ask you to redirect that question. I'll give you some time back.

Mr. Paterson, if you can hear me, we're just going to have to try again in a few minutes.

Mr. Bains, the floor remains yours.

Parm Bains: I'm going to move to Ms. Corrigall-Brown.

A large focus of the work that you're doing and your advocacy around reforming bankruptcy laws is on preventing bad actors from abusing laws and hiding their gains from fraud behind bankruptcy protections. How can we improve this?

Sarah Corrigall-Brown: Thank you very much for the question.

This is a very specific focus of the securities regulators. We are also involved across the board in prevention, detection, disruption and enforcement. What we find, though, is that this has been an area that has persisted for years. We have taken the efforts to detect, investigate and hold hearings, and we have held people accountable by imposing sanctions. They then made no effort to pay their sanctions and turned to our bankruptcy regime to seek to be released in bankruptcy, therefore avoiding paying those sanctions and avoiding all consequences of their actions.

There are some debts that do survive bankruptcy. A person is discharged in bankruptcy, but they remain obliged to pay some debts. We are asking that debts that have been imposed by securities regulators for the most egregious kinds of misconduct—fraud, market manipulation and misrepresentation—be added to the Bankruptcy and Insolvency Act by amending the act so that those debts would survive bankruptcy. We could continue to collect on them as the person continues, and the rest of their debts could be discharged. We think that's essential.

We recognize the absolute importance and necessity of disrupting fraud before it happens. It's the best way to ensure that investors don't lose their money, to retain their confidence in participating in our economy and to protect Canadians. Early disruption is essential, but the system also needs to have strong and effective enforcement. We need to be seen to be able to manage and to regulate our economy and to protect Canadians. Having strong enforcement and amending the Bankruptcy and Insolvency Act so that people who commit this kind of misconduct can't declare bankruptcy and, therefore, avoid all the consequences of their actions is, we think, an essential part of closing a gap at the end stage. If we have actually held someone accountable, we think they should continue to be obliged to pay those sanctions.

● (1130)

Parm Bains: Quite often we witness people moving. If they commit fraud, they'll move to a different jurisdiction. First, could you mention if the provinces and territories are aligned on this within Canada, and then, could you mention other outside jurisdictions that you're working closely with to tackle this problem and whether there are jurisdictions that can serve as a model for us to compare to?

The Chair: You have about 45 seconds for the response, Ms. Corrigall-Brown.

Sarah Corrigall-Brown: All Canadian securities regulators, provincial and territorial, support this request. It is a problem across the country, and we are all supportive. The provincial securities regulators work very closely together to have a harmonized security regulatory regime that protects investors and ensures that our markets are fair and have integrity.

The markets are global and fraud is global, so we also work very closely with counterparts in Europe, Asia and the United States. The United States bankruptcy regime is of note. Sanctions imposed by their securities regulators do not get extinguished on bankruptcy. That is a policy decision that has been made in the United States, and that's what we're recommending that we mirror here.

The Chair: Thank you very much, Mr. Bains.

[*Translation*]

Mr. Ste-Marie, you have the floor for six minutes.

Gabriel Ste-Marie (Joliette—Manawan, BQ): Thank you, Mr. Chair.

Ladies and gentlemen, thank you for your presence and your testimony. Everything you've shared with us is very insightful.

Ms. Corrigall-Brown, I'd like to follow up on your request and the discussion you just had. Does the federal government seem open to making the amendment to the Bankruptcy and Insolvency Act that you're requesting?

[*English*]

Sarah Corrigall-Brown: We've had discussions with ISED officials over the last year that have been productive, and we've met with the Department of Finance as well as the Department of Industry. We've also met with representatives of this committee, and we've been invited to present to this committee. I would say that the federal government has been very open to discussions, to hearing our request and to better understanding the challenge this is raising for securities regulators.

[*Translation*]

Gabriel Ste-Marie: All right, that's fine. We'll continue to remind them that this request is very important.

On another topic, I'd like to address the issue of cryptocurrencies. Do you consider cryptocurrency to be a form of currency or rather a security that falls under your jurisdiction?

[*English*]

Sarah Corrigall-Brown: What a great question. Cryptocurrency in itself, when it's used as a payment method, we see as a currency. We don't regulate cryptocurrency itself as a security.

[*Translation*]

Gabriel Ste-Marie: All right.

In that case, are cryptocurrency exchange platforms considered financial intermediaries that do not fall under your jurisdiction?

[*English*]

Sarah Corrigall-Brown: We do regulate crypto trading platforms if those trading platforms are trading in what we call “crypto contracts”. Essentially, they are contracts where the value is referenced on the underlying cryptocurrency. The crypto contract is a derivative. We do regulate the trade in those crypto contracts. Those crypto trading platforms are subject to our regulation.

[*Translation*]

Gabriel Ste-Marie: Okay. Very well. Thank you.

In the fight against fraud, when it comes to cryptocurrencies, is the federal government's role to intervene and regulate you, or—given all the security commissions working together, along with the exchange mechanisms and effective collaboration you mentioned—do you have everything you need to monitor cryptocurrency transactions?

[*English*]

Sarah Corrigall-Brown: In crypto, as in the capital markets and fraud as well, we think there's a necessity for the federal government and the provincial securities regulators to work together. When crypto itself, for example, is used as a payment, that's federal jurisdiction, and there are federal bodies that regulate in that space. The regulations and the protections they provide for Canadians are essential, yet crypto can also be used in the investment markets and for investment purposes, which we regulate. We have different protections and powers to address the risks that creates for Canadians.

It's really essential that we work together and partner; otherwise, there are gaps. Again, this is where the fact that the federal government is focusing on this and taking such a holistic view of how we can combat fraud and of the way that crypto is used for not only legitimate purposes but also fraud...we need to understand that, working together at the provincial and federal levels.

● (1135)

[*Translation*]

Gabriel Ste-Marie: Thank you very much.

Mr. Pinto, from Payments Canada, my first question concerns the centralized platform you mentioned. Is the participation of the various intermediaries such as banks and other stakeholders mandatory or voluntary?

[*English*]

Jude Pinto: For any of our participants who are using RTR or a third party exchange that clears through the RTR's clearing and settlement, it is mandatory. There are the four services that I described. The network-level risk score will be consumed by them. It's available to them. It needs to go into their adjudication process on whether to proceed with a payment. There is a requirement in our rules to report fraud, account-to-account fraud with a common national taxonomy. There is an obligation under specification to contribute to the risk list. There is a requirement to use the confirmation of payee to identify a valid account.

That includes all new participants coming into the RTR directly as well as the first third-party exchange, which is Interac's e-transfer. All are mandatory.

[*Translation*]

Gabriel Ste-Marie: Okay. Thank you very much.

Can you give us more details on how the scoring system works, including the assessment of fraudulent transactions, among other things? If it's too complex, you can send us a written response. However, I'd like you to give us a 30-second overview.

[*English*]

Jude Pinto: My sound cut out for a little bit. Can you repeat the first part of the question?

[*Translation*]

Gabriel Ste-Marie: Yes.

Can you give us more details on how the scoring system for assessing fraudulent transactions works?

[*English*]

Jude Pinto: We work with our members on the types of indicators they need from a score to come back into their system. They help define the requirements. We run those through algorithms that then provide, effectively, a caution to perhaps not proceed, a yellow to please investigate or a green zone for them to adjudicate. Those types of scores get ingested in our participants' prepayment initiation fraud checks.

Before they send a payment through the RTR, they have all of their internal systems. Let's say you're a bank or a fintech. They would run through that and make a decision, using algorithms, to proceed with the payment or not. It allows them to hold the payment and do further investigation or reject the payment because it's been identified as fraud.

[*Translation*]

Gabriel Ste-Marie: Thank you very much.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

Ms. Borrelli, the floor is yours for five minutes.

Kathy Borrelli (Windsor—Tecumseh—Lakeshore, CPC): My question is for Mr. Pinto.

Many fraud victims, including seniors and small businesses, are manipulated into sending mass money transfers, but the payment systems treat the transaction as final.

What options exist to make high-risk payments more interruptible and recoverable, for example, temporary holds, recall mechanisms, delayed settlement for suspicious transfers and the like?

Jude Pinto: That's a great question, and it's commonly misunderstood what is recoverable versus irrevocable. Our rules basically have been written to allow for certain categories of high-risk payments or known fraud, etc., to actually be required to be returned. We set up rules that say here are the mechanisms by which the sending and receiving organization under certain mechanisms will agree to actually return funds.

The irrevocability has to do with when that doesn't kick in. If that rule wasn't an indicator of needing to return, then it's irrevocable, and even when money has to be returned, it's the second transaction that comes back. That's the way to think about that.

As far as putting holds on it are concerned, we go back to the discussion we just had around the fraud indicators and the score. Before an RTR transaction, an actual payment transaction is initiated in subsecond time, that fraud check, a check against the risk list and an ingestion of the score would go into the participants' algorithm, and they could decide to place a hold and investigate or decide what to do with it, case by case.

● (1140)

Kathy Borrelli: In your opinion, should the federal government set a clear policy expectation that payment modernization must include not only faster payments but faster fraud response?

Jude Pinto: That's a good question. Thank you for that.

To the extent that we've come to designing and launching RTR, that has been the expectation. Our membership, our future membership through new participants coming in with wider expansion, and our regulatory guidance have all required that we make this mandatory via our rules and via an initial market offer that launches simultaneously with the system.

Kathy Borrelli: Should there be a centralized hub where sectors like police can co-operate with access to the data necessary to prosecute fraudsters?

Jude Pinto: I think that's an astute question.

The centralized hub...let's separate that from the need to collaborate. On the need to collaborate...absolutely. For law enforcement and prosecution, in the channels as we talked about—social media might have data, telcos, banks, etc.—there has to be a mechanism to be able to collaborate and share data, where required, for financial crime fighting. With the national anti-fraud strategy and the financial crimes agency, we're expecting to get engaged in a lot of that type of discussion as part of those.

The notion of a centralized hub pooling data from all of those sources hasn't been a big part of the discussion. It's been more about the official mechanisms to share data in a collaborative way and build schemes to share data amongst all those involved in fraud prevention, detection and prosecution across a pretty wide network.

Kathy Borrelli: Mr. Paterson, many seniors are targeted through fake tech support scams or bank impersonation scams where the victim is convinced to install remote access software. Once that happens, the scammer may be able to guide or control the transaction.

What technical safeguards could help detect when a person is being coached or controlled remotely through a financial transaction?

Ian Paterson: Thank you for the question.

[*Technical difficulty—Editor*] is key. As well, in terms of specific technical controls that can be put in place, there's visibility, so understanding what you are installing and what it does, and, frankly, making use of existing technologies such as firewalls. These don't require additional cost [*Technical difficulty—Editor*].

[*Translation*]

Gabriel Ste-Marie: Mr. Chair, on a point of order: the interpreters are indicating that they are unable to do their job.

The Chair: Yes, I understand. Thank you.

[*English*]

Mr. Paterson, unfortunately, notwithstanding the fact that we heard bits and pieces of what you said, you're coming in continuously choppy. I'm going to move on. However, I will provide Ms. Borrelli an opportunity to ask that question again down the line if we see that the connection has improved. If not, we'll have her submit that question to you in writing, at which point you can submit your answer to the committee. We can hear you enough, but the challenge is for the interpreter. Unfortunately, I can't rely confidently on the status of the connection at the moment, so we'll try to come back to you, sir.

Ms. Borrelli, we were at the end of your time there, but—

● (1145)

Kathy Borrelli: I had about a minute left, I believe.

The Chair: No, you didn't. You had five minutes, and we were over. I'll circle back to allow you to ask that question again—or another question, if you so choose—as a result of the technical difficulties.

Kathy Borrelli: What do you mean by “circle back”?

The Chair: In a few minutes, if that connection stabilizes, I'm going to allow you the opportunity to take 45 seconds or a minute and ask that question again, or another question.

Kathy Borrelli: That's great. Thank you.

The Chair: Thank you.

Mr. Bardeesy, the floor is yours for five minutes.

Karim Bardeesy (Taiaiako'n—Parkdale—High Park, Lib.): Thank you very much.

Ms. Corrigall-Brown, you mentioned the relationship between cryptocurrencies and the issue we're studying today. The Government of Canada has announced its intention to help create a stablecoin framework, and it's standing up a financial crimes agency.

Can you speak to that? Some written advice afterwards would also be great. What is the collective security regulators' view on melding these two pieces at the same time—the introduction of the stablecoin framework and the introduction of a financial crimes agency?

Sarah Corrigall-Brown: Thank you for that question.

Our enforcement directors and the CSA enforcement committee have met with representatives in relation to the financial crimes agency. They are also consulting with and providing their views to the federal government in the development of the stablecoin legislation. It is important. There will be the need to ensure that there is respect for the respective jurisdictions and that there's a really clear ability to share information and have co-operative and partnered oversight of entities, as stablecoin is used by different market participants for different purposes. These products and businesses move through jurisdictions, so we need to partner together.

At the highest level, we are partnering. We have offered our strong support for and our view that collaboration and information sharing are absolutely essential.

Karim Bardeesy: That's great.

The Chair: Mr. Bardeesy, I'm going to pause the clock for one second.

Mr. Paterson, if you can hear me, I'm trying to correct this problem. We have some folks from the tech side at the House of Commons trying to reach out to you. If you want to take a moment to check your phone or email, we're going to try to have you sign out and sign back in. I want to prompt you to keep an eye out for that.

Mr. Bardeesy, you have three minutes remaining.

Karim Bardeesy: Thank you, Ms. Corrigall-Brown. We'd love to get some written recommendations on that with your further thoughts.

Mr. Pinto, I understand that Interac is the exchange solution provider for real-time rail. Coming into that project, what are the questions Payments Canada is asking of Interac—which also runs the e-transfer network, which is well known by Canadians—with respect to some of the potential vulnerabilities that could emerge from the partnership you have? What do you think needs to be attended to?

Jude Pinto: Are you referring to technical vulnerabilities or something wider?

Karim Bardeesy: Take it where you will.

Jude Pinto: Payments Canada is the owner and operator of the total RTR solution. It's made up of several components. It's made up of a clearing and settlement component. It's made up of a brand new exchange. That exchange has leveraged Interac's expertise in e-transfer for the last 22 years by putting a modern architecture to it and having Interac as a provider in that regard. Interac's e-transfer will convert to use the new clearing and settlement engine that has been built.

It's not so much a vulnerability as it is an opportunity we have here. The protection against fraud covers even the in-market solution that's been there for 24 years, including building on what we've learned from e-transfer and giving it an uplift with the types of extra features we're adding to it. Our rules allow for a wide scope of those mandatory fraud controls.

● (1150)

Karim Bardeesy: I'll just pick up Mr. Falk's question from earlier. E-transfer is, unfortunately, one of those vectors that social media.... Social media, as a vector to e-transfer, is the mechanism by which social media-enabled frauds are executed. Are there any specific questions you're asking of Interac with respect to this project, given that reality?

Jude Pinto: Our participants in RTR, in both cases, are the banks, financial institutions, credit unions and PSPs. The social media interaction happens at that layer. Again, the direct participants are where that intersection with their customers and social media and telcos, etc., will happen.

What we've put in place with Interac, where we can help as things flow through exchange, clearing and settlement, is a greater degree of mandatory reporting against a common taxonomy. That helps trends and sees movement to that, and that can feed back to Interac participants and ours, as required.

The risk list will help everybody. If one institution identifies a confirmed scam, seven others can prevent that from happening and use it to actually stop a payment. We're a bit at the middle to the back end of the thing, but we're adding tools that will help the participants at the front end, where scams and fraud are occurring.

Karim Bardeesy: Thank you.

The Chair: Thank you, Mr. Bardeesy.

[*Translation*]

Mr. Ste-Marie, you have two and a half minutes.

Gabriel Ste-Marie: Thank you, Mr. Chair.

Mr. Pinto, I'd like to continue with you. Could a bank or financial institution decide not to use the real-time payment system at all, or does it have no right to opt out of using it?

[*English*]

Jude Pinto: It's a great question. You're talking about using the four fraud controls.

It's mandatory that they consume it, but once they consume it, their internal risk policies are what guide their individual thresholds on what to pass and what to fail. All of them have supplementary tools. For example, they might be absorbing four different scores, including the one we're providing, which has some network-level efficacy to add to what they're using today. For that part of it, they'll choose which score and threshold to use, from amongst the number of tools, to decide to let the payments through or to stop them, and that's because they bear the liability as the sender. They do the checks before and, generally, they have to deal with the fraud that arises between their own fraud losses and customer fraud losses, so that's where it leads to.

The parts of the solution that are mandatory, via our rules, are the contribution to the risk list and the contribution to the standard reporting nationally.

[*Translation*]

Gabriel Ste-Marie: Okay. Thank you very much.

Let me make sure I've understood this correctly. Your real-time payment system aims to implement the process with the anti-fraud services we discussed. It is not intended to further speed up payment systems that are already very fast, but rather to improve security. That is why you say that, with this, Canada would be among the first to launch a system with these security features. Is that correct?

[*English*]

Jude Pinto: It's a great question.

We saw that other countries launched their instant payment rails without direct attention to the types of new and different frauds that can accompany real-time payments. We have seen the types of solutions they've put in place, and then we worked with our members. I think there were a couple of dozen different things that could be done at the national level. They ended up picking these four and said, “Well, let's make sure that goes out on day one as part of the solution.”

It is available for all of the incumbent banks using e-transfer or all of the new participants that will use either e-transfer or RTR direct. It is available to all. Whether you've had 20 years of history in banking or you're a two-year-old fintech, it is available to you, with a network level of protection and insight.

● (1155)

[*Translation*]

Gabriel Ste-Marie: Thank you.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

Mr. Lawton, the floor is yours for five minutes.

Andrew Lawton (Elgin—St. Thomas—London South, CPC): Thank you very much, Mr. Chair. It's great to be here at this committee for the first time.

I'd like to start with you, Mr. Paterson. Hopefully, we've had the technical issues worked out here. One thing I understand about safeguarding against frauds and scams is that it's very much a multi-layered effort. There are individual decisions people can make to protect themselves. Then, at the system level, we also have protections that are needed.

I'm just wondering, given the security work you do, what caution could be given to the government, in the context of Bill C-22, the lawful access act, which actually requires the insertion of back doors into what are, right now, secure.... I'm just thinking of how that would affect people's vulnerability to bad actors, instead of just law enforcement, using those same back doors.

Ian Paterson: I apologize for the Internet connectivity issue.

I'm very concerned about proposed back doors. We have seen in the industry, for decades now, well-intended efforts to create vulnerabilities inside systems, which, inevitably, are used by bad guys to get access to that data. We saw this, most recently, in the United States, when a nation-state was able to compromise the lawful access in the telephony system in the United States.

I would focus the government's attention more toward how to build stronger systems across the board. There are definitely technologies. I mentioned pass-keys as well as phishing-resistant or spoofing-resistant communication channels. There are, absolutely, newer technologies that can make a material impact on reducing fraud. I think that we should start there as opposed to trying to weaken systems.

Andrew Lawton: If I extrapolate from what you're saying or, perhaps, try to tighten it up in a way that other people could draw from this, any vulnerability that might exist for the good guys is also there for the bad guys. Is that an accurate summation of what you're saying there?

Ian Paterson: It's very accurate, sir.

Andrew Lawton: In terms of the way that we navigate these and other related issues, I'm just a bit confused. We have done so much, I think, to try to prevent people from being targeted by this. One of the things that strike me as so interesting is that we have, basically, this game of whack-a-mole, in which the technology is evolving more quickly than the education. What role do you think literacy plays in safeguarding against fraud?

Ian Paterson: I think that literacy is crucially important. I would also say 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.

I don't believe that fraud can be legislated away. It has to be a team effort, with public agencies as well as private corporations and individual citizens all taking responsibility for their respective areas to address these issues. That sounds like a hard thing to do, but I am [*Technical difficulty—Editor*] renewed focus on this issue, we can have a material impact on reducing fraud for Canadians.

Andrew Lawton: Thank you very much, Mr. Paterson.

I'm going to take that glitch as my cue to move on to my other questions for Ms. Corrigall-Brown.

Ms. Corrigall-Brown, you're obviously representing the B.C. Securities Commission. I know that the overall structure of the securities system in Canada is outside of the scope of this study. From a fraud and scam prevention perspective, and with just looking at things that fall under securities regulators, I wonder whether there is a problem we're facing in Canada, in that we have a patchwork of regulators and regulations when so many of these frauds and scams are national in nature, or global even.

Sarah Corrigall-Brown: I think we absolutely recognize it. Because they're national and global is why Canadian securities regulators work so closely together in our enforcement efforts. There can be circumstances in which there are victims in multiple jurisdictions, and in such cases our enforcement teams work closely together.

As you said, the fact that it is national and the fact that the federal government, under the federal Criminal Code, has a role to play are also why—as I've said here, representing the BCSC but also the CSA—we are very excited about and strongly committed to working with the federal government in terms of the focused role that the federal government will play.

● (1200)

Andrew Lawton: Is it your view that there is no inefficiency or nothing falling through the cracks by having multiple securities regulators in Canada?

Sarah Corrigall-Brown: I think that, in Canada, we work very well together in terms of the areas that are regulated by the provincial regulators. We're mostly harmonized in our rules. We enforce together, and we work regularly on almost all activities together.

There are always gaps. There are always possibilities for improvement. However, in terms of providing a strong regulatory regime for the Canadian capital markets, I think the provincial regulators work very well and strive to serve the Canadian markets well.

The Chair: Thank you, Mr. Lawton.

Mr. Paterson, I'm going to try to take advantage of what was a stable connection so that I can honour my commitment to provide Ms. Borrelli with those 60 seconds. We're going to try this again.

Ms. Borrelli, I'll give you an opportunity to ask a question and get a response from Mr. Paterson. Then I'll go to Mr. Joseph.

Kathy Borrelli: Thanks.

Mr. Paterson, I've heard from seniors who've been convinced to install remote access software, and, once that happened, they ended up losing quite a lot of money. What technical safeguards could help detect that this kind of thing is happening? Should banks or payment platforms be required to add extra verifications in that regard?

Ian Paterson: Education is key. Beyond education, technical safeguards, such as using built-in firewalls, can certainly play a role to identify, specifically, remote access types of tools. Those can be identified and stopped at the operating system level. Beyond that, coordination with payments companies will certainly help in this regard.

Kathy Borrelli: Do you have any idea of any programs that can help teach seniors how to do this?

Ian Paterson: Unfortunately, this is only one of several scams that exist. Romance scams, unfortunately, are another one that will often target seniors. As some of the members mentioned, it is a whack-a-mole game. Holistically, education on scams that can occur is something that should happen, and it is the first line of defence.

The Chair: Thank you, Ms. Borrelli.

[*Translation*]

Mr. Joseph, you have the floor for five minutes.

Natilien Joseph (Longueuil—Saint-Hubert, Lib.): Thank you, Mr. Chair.

I will first address Mr. Jude Pinto, but I would like to take this opportunity to thank all the witnesses for their presence.

Mr. Pinto, we know that most fraudsters or organizations that defraud people living in Canada do not themselves live in Canada, but in other countries. I don't know if you have any data on this. Can you tell us which country tops the list?

[*English*]

Jude Pinto: I don't have that data in front of me. We do have an active research department that uncovers these. If I could bring back information and share it, through the chair, that would be ideal.

[*Translation*]

Natilien Joseph: Thank you, Mr. Pinto.

I'll continue along the same lines as my colleague, but I'll go a little further when it comes to deepfakes, which can now very convincingly mimic a person's voice or image. They are increasingly being used in fraud and scams.

In your opinion, what threat does this phenomenon pose to Canadians, and what measures should be prioritized to address it?

[*English*]

Jude Pinto: If I could play back the question, it's about things like deepfakes being technologically adept and, increasingly, creating victims in Canada.

From a Payments Canada perspective, the best contribution that we think we need to grow, from the infrastructure out, is that centralized reporting on the types of fraud and looking for the trends that are happening so that the entire payments ecosystem can benefit. Then, secondly, as we successfully identify and/or prosecute any one of these actors who are committing these frauds, we'd make that knowledge available to everybody through our risk list.

I'm not in a position to comment on the best ways to protect it at the front end, where the exchange is happening. It would probably be better for that to come from my colleagues.

● (1205)

[*Translation*]

Natilien Joseph: Thank you.

Ms. Corrigal-Brown, we know that fraudsters targeting Canadians are increasingly operating from abroad. What would be your key recommendations to the federal government to effectively reduce this type of cross-border crime?

[*English*]

Sarah Corrigall-Brown: That's a great question.

It is challenging for us to take action against foreign people who are accessing Canadians from abroad. That's one of the reasons we work very closely and have memorandums of understanding with European and American regulators and regulators in Asia and Australia. We work closely with them in order to share information and to try to identify people who are outside our country, and then they can be prosecuted in their country.

I would say that the reality is that, as we've heard from other people, in some ways detection, prevention and disruption at the front end by working through.... The way that fraudsters are accessing Canadians is through the Internet. It's through technology providers. This kind of thinking around what the federal government can do in terms of legislation, in terms of thinking about interventions at that level and being able to access actors in this country—

[*Translation*]

Natilien Joseph: Forgive me for interrupting.

How many minutes do I have left, Mr. Chair?

The Chair: You have 45 seconds left.

Natilien Joseph: So I'm going to ask you one last question, Ms. Corrigall-Brown, since you mentioned prevention.

The 2025 budget announced the creation of the Canadian Financial Crimes Agency, while the spring economic update launched an anti-fraud strategy. In your opinion, what impact will these initiatives have on the prevention, detection, and prosecution of financial crimes in Canada?

[*English*]

Sarah Corrigall-Brown: I think it should be holistic. We strongly support both of these initiatives. Taking action at the front end in order to have an anti-fraud strategy where you are empowering investors, informing them and educating them, and where you are disrupting the activity at the level that it's happening, is essential. The fact is that the fraud will happen, and we need to demonstrate that we are watching and that there's integrity in our markets. That's why we very strongly support the financial crimes agency at the federal level to show that we are taking enforcement action and that there will be consequences. I think that creates an atmosphere where we may be a less attractive place for people to come in and target.

[*Translation*]

The Chair: Thank you, Mr. Joseph.

I would like to thank all the witnesses.

[*English*]

Thank you very much to all of the witnesses for availing yourselves to us today. We appreciate the insight and the guidance that you have given us as we continue this important conversation.

Colleagues, I'm going to suspend briefly in order for us to get prepared for the next hour. In about five minutes time, we will resume.

Thank you very much.

● (1205)

(Pause)

● (1215)

The Chair: Colleagues, welcome. We are going to continue into the second hour. Thank you very much to Mr. Lynam, who has joined us from the RCMP as the director general for the Canadian anti-fraud centre. I think your testimony today is going to be quite crucial to our understanding of the role that the federal government plays in addressing this challenge.

Mr. Lynam, you'll have up to five minutes. You are the only witness that we have on this panel, which will allow us to get into the depths of your expertise.

Colleagues, I did mention to a few of you just before gavelling in here that we are slightly behind. We are sitting for three hours today, which will butt up against the beginning of question period, so there may be a slight reduction in this hour and in the next in the amount of allocated time, but we will ensure that everybody has their opportunity to speak.

With that, Mr. Lynam, again, thank you for joining us. The floor is yours, sir.

Chris Lynam (Director General, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police): Good afternoon, Mr. Chair and honourable members of the committee. Thank you for the invitation to appear today. I would like to acknowledge that we are gathered on the traditional unceded territory of the Anishinabe nation and recognize the enduring presence of first nations, Inuit and Métis peoples.

My name is Chris Lynam. I am the director general of the national cybercrime coordination centre and the Canadian anti-fraud centre at the Royal Canadian Mounted Police.

Financial fraud and scams represent a significant, evolving and increasingly complex threat to Canadians and to our economy, with major impacts felt across the country. In 2025 alone, the Canadian anti-fraud centre received reports of fraud and cybercrime losses totalling over $700 million. This marks eight consecutive years of record losses, and we assess that this represents only a fraction of the actual losses that are being felt.

Fraud has become highly organized, industrialized and automated. Canadians are targeted by industrial-scale scam compounds that employ thousands of individuals and operate from various parts of the world. They also face individual fraudsters who leverage easy-to-use, low-cost, fraud-as-a-service platforms. These schemes often rely on digital platforms and leverage emerging technologies, allowing threat actors with minimal technical expertise to defraud Canadians at scale.

To provide an example, one recent phishing-as-a-service platform was used by thousands of Canada-based suspects, with almost one million Canadians falling victim to this platform alone. The threat environment continues to evolve rapidly, driven in large part by advances in technology and automation, particularly artificial intelligence. Criminal actors are using AI to generate convincing phishing messages, to draft and translate luring emails and texts, to produce deepfake impersonation and scamming videos and calls, to mine stolen data, to identify new victims and to exploit vulnerabilities in networks.

Faced with these threats, the Canadian anti-fraud centre plays a central role in combatting fraud in Canada along four lines of effort—prevention, victim support, disruption and pursuing the criminals behind these scams.

To facilitate prevention, the CAFC uses targeted messaging to promote public awareness of fraud threats on its website, via social media and through in-person engagements. The goal is to help Canadians recognize and avoid fraud and to encourage at-risk Canadians, particularly young people, not to engage in fraud and cybercrime activities.

In terms of support for victims, we assist fraud victims by providing guidance to limit further losses and, in some cases, by coordinating rapid action with partners to freeze or recover funds. We also provide tips to help victims avoid being victimized again in the future. The CAFC often receives information or intelligence about victims who do not know they are being scammed, for example, through romance or what we now call relationship fraud. In those cases, CAFC employees will reach out and warn those victims.

In terms of disruption, we work with financial institutions, telecommunications providers and digital platforms to disrupt the fraud ecosystem by identifying and disrupting the entities, tools and services—the so-called enablers—that facilitate fraud.

Then there is pursuing those responsible. Finally, we enable investigations and help partners pursue those who are responsible by providing actual intelligence and investigative leads, coordinating across multiple agencies and linking Canadian efforts with multinational criminal investigations and operations.

Reports received from members of the public and businesses that have been targeted or victimized are a key component of the CAFC's efforts. Through our modernized reporting platform, reportcyberandfraud.canada.ca, Canadians can more easily report incidents of fraud and cybercrime. Additionally, the CAFC has built extensive partnerships in Canada and around the world to combat fraud. These partnerships are vital to tackling fraud in an investigative environment that is often complex, cross-border and resource-intensive.

Finally, the CAFC continues to pursue innovative and holistic approaches to reduce the impact of fraud on Canadians. We believe that our four lines of effort approach is sound and produces tangible operational results, but we must work with more partners and do it at a broader scale to reduce the levels of fraud victimization in Canada. Rest assured that we are fully committed to this mission.

Thank you. I look forward to your questions.

● (1220)

The Chair: Thank you very much, Mr. Lynam.

Mr. Lawton, the floor is yours for six minutes, sir.

Andrew Lawton: Thank you very much, Mr. Chair.

Thank you very much, Mr. Lynam, for being here today.

Just as a bit of context, I've had rather a rude awakening on this issue in the last few months with a number of constituents I've spoken to who have been defrauded—in some cases, out of small amounts, and in others, out of obscenely large ones.

One case that is burned into my mind is that of a man who was in tears at a town hall I was hosting on fraud prevention alongside the St. Thomas Police Service. He had been hoodwinked for a small amount by a crypto scam. Then he was scammed again by a person purporting to be part of an agency that would help him recoup his losses. In the end, he and his wife were drained of everything they had: $80,000. When he shared his story, everyone else put up their hands because they had their own stories.

These are happening with more and more frequency. I know and truly believe that you are committed to trying to stop this as much as possible. How often can you succeed in getting money back? How often is something being recovered in these scams?

● (1225)

Chris Lynam: Thank you for the question.

Unfortunately we do hear, just as you heard from your constituents, these tragic stories of people losing their life savings. It is happening across Canada.

Unfortunately, the percentage of the incidents where we can help try to get people their money back, or at least frozen, is relatively small. Part of the challenge is that there's a lot of shame associated with reporting, and people don't report it. There is a window in some cases. If an e-transfer was made and if the victim doesn't report, that window might be over. It is a small percentage of what we see, but we do encourage people to be reporting. As we've talked about, and as we're going to talk about, prevention is really key to avoid being victimized from the start.

Andrew Lawton: I'm obviously more attuned to stories that are happening locally. There was a gift card scam recently in St. Thomas, and a $20,000 cryptocurrency app fraud. Someone else put money into a platform they really didn't understand that much, and in the end had $10,000 taken from them. You have these fake investment schemes. In another one that came to us, someone was out $3,000 or so.

I know that all scams are different and whatnot, but if you can generalize even somewhat, how many of these would you say are coming from inside Canada versus from outside of Canada?

Chris Lynam: It is often very challenging, at the front end, to determine where the scam happens because they're scammers; they don't tell you where they're operating from. A large percentage of the various types of scams is coming from abroad.

I talked a little bit about the scam compounds. Those are often themed in things like investment scams or job scams. However, there is fraud happening that starts in this country. I talked about these fraud-as-a-service platforms, where people with very minimal technical skills can use these platforms to defraud Canadians. It is a mix of both, but the majority comes from overseas.

Andrew Lawton: I mentioned earlier the man who was taken for over $80,000. The company, the fake law firm, that was responsible for this has a website that, even now, even after police have been investigating it, is still up.

If someone goes to that website, they'll see the same information he did, pictures of people who look like they're lawyers, talking about how they succeed in recouping money. Just to use that as an example—and others like it—why do these websites stay up? What is needed from a policy perspective for things that are known to be frauds, known to be scams, to be taken off-line?

Chris Lynam: It is, as you can imagine, a horrible situation of someone who's lost their money and thinks there's an opportunity to get it back by going to what seems like a reputable institution.

There are a couple of pieces to this. First, it's somewhat the nature of the Internet, of registered domains and of how web hosts work that almost anybody can put up a website. There's not a huge amount of front-end looking at how that works.

Having said that, when we get that information, from a disruption perspective, we will often go to that web host or domain registrar and say, “Look, we think this site violates your terms of service.” Ideally, there's an investigation going on in parallel, but part of the idea is to get that website taken down so that others can't be victimized. This is what this committee is doing—looking at this and asking how we make recommendations to have this holistic approach to reduce the victimization across the country.

Andrew Lawton: Are you having success there? If not, on things that we can identify as frauds, where we know the website is serving as the gateway to that, what policy mechanism would you recommend that would help towards taking that off-line?

Chris Lynam: I'll speak to what we're doing operationally.

Part of this is a little bit of a theme. Really, the way forward, from an operational collaboration perspective, is to bring many partners together who have data of enablers of fraud and then also have organizations lined up that can do something about that.

We hosted an operation called “Maple Disruption” last December, where we did that. We brought a whole bunch of partners together from the private and public sectors. At speed, we were able to have information come in and get it to the right entities who could take that action. We are going to be hosting Maple Disruption 2026 and do that on a much bigger scale. That just gives you a sense that we have to be able to do this almost in real time if we're going to make a difference operationally.

● (1230)

The Chair: Thank you very much, Mr. Lawton.

Ms. O'Rourke, the floor is yours for six minutes.

Dominique O'Rourke (Guelph, Lib.): Thank you so much, Chair Carr.

To the DG, thanks for being with us. I want to ask a question that's a bit broader because you're the director of the national cybercrime coordination centre and the Canadian anti-fraud centre within the RCMP. It's a very broad mandate.

We have a bill before the House of Commons right now, Bill C-22, and it proposes lawful access to give RCMP and police officers across this country more up-to-date digital tools to intercept crime. I'm wondering if you could tell this committee why Bill C-22 would be helpful in the case of disrupting and investigating all cybercrime, but also specifically frauds and scams.

Chris Lynam: One of the real challenges with technologies that target what we call cybercrime or cyber-enabled fraud is that the perpetrators are often in another jurisdiction, the victims are in a whole bunch of different jurisdictions across Canada and then the data might be in yet another jurisdiction. To investigate that in an efficient and rapid way, police across the country need the right tools.

Legislation like Bill C-22 and some of the powers it provides, regardless of the crime type—particularly those that have a significant digital element—will help us to have the additional tools to go after fraudsters and cybercriminals.

Dominique O'Rourke: Is it the RCMP's position that Bill C-22, lawful access, is important in combatting fraud and a whole range of cybercrime?

Chris Lynam: As I mentioned, digital tools or legislation that enables us to enforce crimes that have a major digital element.... It is really important to have those modern tools. Bill C-22 is one of those that will assist police officers, if passed, to have further tools to complete their job.

Dominique O'Rourke: Do you have the tools that you need, or do the bad guys have better tools and constantly evolving ones?

Chris Lynam: One of the challenges with law enforcement is that we set a high bar for the types of technologies and tools that we adopt. They have to be legal. We have to make sure that they respect the privacy of Canadians. The process of how you actually vet those and then operationalize them can often take a long time. Cybercriminals and other criminals don't operate by those rules. The first bad AI that can be accessed, they're going to jump on and figure out ways to do that.

There's always this sort of cat and mouse game of what new technologies the criminals are going to adopt. Part of what my centre does is work with as many police services across the country as possible to share information and come up with coordinated approaches to go after them, either before they can use these new tools or at the early onset.

Dominique O'Rourke: I just want to switch gears a little bit.

A special report published in Reuters cited internal Meta documents that indicated that they had internally projected that approximately 10% of their overall annual revenue in 2024, or $16 billion, was derived from fraudulent ads.

I have an insurance background and a municipal background. I'm familiar with joint and several liability. In that light, does this mean that Meta is a party to a fraud? What more should platforms be doing to interfere with the fraudsters on their platforms?

Chris Lynam: To the first part of your question, I'm not sure I'm 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.

Dominique O'Rourke: I have one last question.

You mentioned that young people need to be more aware of fraud. We have all received these calls in our constituency offices from seniors who have been defrauded. It's quite possible that they're the bravest in reporting.

Tell us a little more about what the landscape looks like. I'm thinking of some of the romance crimes. They are not necessarily seniors. How do we tackle scams for each target audience?

● (1235)

Chris Lynam: It's a great question. It's how we approach it. How you encourage prevention for a demographic that's a senior audience is different from how you need to approach young people. Often they can be a “click now and think later” group of people. We try to use different approaches. A social media or online public awareness campaign might work better with a younger audience, whereas in-person engagements or printed material.... We do a lot of that work.

Finally, the technical sophistication needed to become a fraudster or cybercriminal now is very low. We spend some time doing outreach to young people who may want to go onto these platforms or on a forum. They hear about how easy it is and police are challenged to track them down. We engage them and say, “Look, you do not want to go down this pathway. This will ruin your life.” There's more work to do on that front.

The Chair: Thanks very much, Ms. O'Rourke.

[*Translation*]

Mr. Ste-Marie, you have the floor for six minutes.

Gabriel Ste-Marie: Thank you, Mr. Chair.

Mr. Lynam, thank you for appearing before the committee today.

As you mentioned, there are several types of fraud. I'll start with one that's already been discussed: fraudulent ads posted on platforms like Facebook. A few weeks ago, the Journal de Montréal ran a feature revealing that, due to technological advances, there are now fake videos that look real—videos in which we see, for example, Prime Minister Carney, former Quebec premier François Legault, businesspeople like Luc Poirier or Kevin O'Leary, or even international actors like Keanu Reeves, telling people to invest in something because it's profitable.

A retiree tries investing a few dollars. They withdraw their money and make a profit. After that, they invest a few thousand dollars, withdraw their money, and make a staggering profit. Often, the person eventually decides to invest their entire retirement fund in it, but poof—the money disappears.

In the article from the Journal de Montréal, there were, among others, two people who had lost more than $100,000 because of this scam. Enquête, a public affairs program on Radio-Canada, even reported on a case where someone lost more than $400,000, if memory serves me correctly; life savings are vanishing overnight.

According to the various stakeholders, what needs to be done to ensure that this type of fraud never happens here again?

[*English*]

Chris Lynam: That is a very complex type of scam or fraud that happens. It leverages people's need to make money or there's an opportunity. It then involves deepfake technology and what have you. One of the challenges is having a holistic approach to this. On one hand is prevention and awareness—trying to make sure people understand that these types of scams are out there and how to protect themselves. Then it's trying to disrupt these types of opportunities. There are ads out there. There are websites that advertise this. At the CAFC and working with our police partners, we try to disrupt those and get them taken down.

Then there is the investigative side. The role of our centre is often having that reporting coming to us from different victims. We can then connect the different linkages and work with different police partners to pursue the people behind it. Often it has international involvement because those behind it are operating in another country.

We have to have a holistic approach across a bunch of different avenues to tackle that.

[*Translation*]

Gabriel Ste-Marie: Thank you.

Often, as you said, the fraudsters are abroad. Public affairs programs reveal that this often takes place in very poor countries. Often, even the people who are forced to commit these frauds are under threat from organized groups, who hold them captive or blackmail them by telling them they work for them and must bring in money. How does the RCMP collaborate internationally to dismantle these networks?

● (1240)

Chris Lynam: This is a major challenge for victims, and it is also a major challenge for the RCMP to combat fraud overseas. First, we use our network of liaison officers in other countries. In addition, there are certain regional organizations, such as Europol, where the RCMP has several officers serving on what is called the Joint Cybercrime Action Task Force. Through these organizations, international police agencies can exchange information in real time. This is one approach—one example—of how the RCMP combats overseas fraud.

Gabriel Ste-Marie: Thank you very much.

There is another type of fraud. With all the data breaches that have occurred at various institutions, it often happens that fraudsters show up at the home of the person they're targeting to defraud them by telling them that their account has been compromised, that they should follow them and hand over their debit card. These people may show up wearing clothes that look like police uniforms. What can be done about this? Is there anything that can be done to better combat all the data breaches at various companies?

[*English*]

Chris Lynam: I'll start with your first example of the fraud, where it's usually some emergency type of scam. They say, “I need to come to your house and pick up money,” or something like that. It is absolutely happening. It often targets senior citizens.

There have been lots of great investigations into this. This is an area where prevention and awareness are absolutely key. We have found that when young people or family members talk to their seniors and say, “I am never going to call you out of the blue and say I'm in jail somewhere and I need $5,000,” and have that conversation, it is highly effective for them to understand and avoid that kind of scam. That's, again, an example of how that in-person, person-to-person engagement is important.

Your second question was about data leaks and what have you. Unfortunately, a lot of the fraud that is perpetrated is from data that's stolen and then mined for people's identities or for ways the fraudsters can use that to then change and launch fraud attacks against them. That goes to the second half of my overall responsibilities of dealing with cybercrime, in trying to go after the cybercriminals who are hacking into systems to steal that data and leverage it in other ways.

We use the same approach. We do prevention. We work with as many partners as we can, and we do disruption to go after the cybercrime ecosystem that is trying to steal that data.

[*Translation*]

Gabriel Ste-Marie: Thank you.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

Mr. Falk, the floor is yours for five minutes.

Ted Falk: Thank you, Mr. Chair.

Thank you, Mr. Lynam, for your testimony here today.

I just want to follow up a little bit on Ms. O'Rourke's questions about Bill C-22.

What specific tools in Bill C-22 would you think would better assist you in doing the job of preventing crime or scams?

Chris Lynam: In terms of how judicial authorizations work, obviously when police services need to legally obtain data to help them investigate and prove who's behind it, they have to seek data either from financial institutions, telecommunications providers or what have you. Given how fast cyber-fraud moves, the quicker that law enforcement can get that data back helps them to advance those investigations faster.

I'll use an example of tools that allow police services to submit for judicial authorization through the courts and then get that data back. It helps to—what we call—move at the speed of cyber. I'll use that. I'll give you that. That's the example I'll use as to how those tools or legislation of the Bill C-22 type can help law enforcement.

Ted Falk: Okay, and you don't think you have those tools today.

Chris Lynam: It's just—

Ted Falk: It's just slower in requiring judicial authorization.

Chris Lynam: There has been legislation that's changed in terms of turnaround times when production orders have been submitted in the financial information sphere. I just use that as an example. Cyber-fraud is a type of crime that moves very quickly. For police to go after the cybercriminals and the fraudsters, we need to receive that legally obtained data quickly so we can analyze it, find the patterns and do the attribution and what have you. I'll just use that example of how timely response to judicial authorizations is an important tool that police need.

● (1245)

Ted Falk: It's said that only 5% to 10% of actual scams or frauds are reported to the police. I'm sure you do a cost-benefit when someone reports being scammed or defrauded. Do you think it's worth your while to pursue a lot of these scams?

Chris Lynam: When you say “cost-benefit”, are you talking—

Ted Falk: It's the amount of effort that you as the RCMP have to put into it, the investigative effort.

Chris Lynam: Right. We take that approach, in that there are...and it's based on a few factors, including whether there are solid investigative leads or intelligence that can be followed up on. If there are and there are partners that want to work together—domestic and international—that may become a full criminal investigation. If those sorts of leads aren't readily available, then it may be a disruptive type of activity that's undertaken.

At the same time, we're always doing prevention on the side in terms of learning from what happened and then going back and warning people about the latest scam reported to us.

Ted Falk: Okay. Somebody reports a fraud to you. You look at it and say that you're going to put all this effort into it, all these man-hours, all the resources, and you're actually trying to get a conviction there. Then you go to the courts, and it's basically a slap on the wrist.

I'm thinking of a woman in Montreal this past March who was defrauded of thousands of dollars. The perpetrators were sentenced to 18 months of house arrest with generous carve-outs for going to the gym and things like that. Her comment was that she felt the penalty was “a joke”.

Do you, as the RCMP, also figure that there are not proper penalties for the crimes that are being committed?

Chris Lynam: We usually focus on that return on investment type of activity—what we think we can achieve from either a criminal prosecution or disruptive action. We focus our efforts on those types of calculations to figure out how we can achieve the most reductions of fraud or cybercrime in Canada. That's always part of our calculation. We tend to put our efforts in that area, as well as prevention, rather than what the outcomes are at the other end.

Ted Falk: Do you sometimes find that your officers or your personnel are frustrated with the penalty versus the actual crime and the effort involved in achieving a conviction?

Chris Lynam: As for the role of the Canadian anti-fraud centre and the national cybercrime coordination unit, we're not the lead investigating agency. We work with all the partners and, usually, a lead agency. I can't speak to what an investigator who leads that investigation...and what happens at the end.

Our main role is to bring those entities together, enable them with intelligence and technology, and orient them in the best way possible to achieve the biggest result possible.

Ted Falk: Thank you.

The Chair: Thanks very much, Mr. Falk.

Mr. Ma, the floor will be yours for five minutes, sir.

Michael Ma (Markham—Unionville, Lib.): Thank you, Chair.

Thank you, Mr. Lynam, for being here.

First, could you describe how the Canadian anti-fraud centre coordinates with the financial institutions, the telecommunications providers, law enforcement agencies and digital platforms in identifying and disrupting emerging frauds? In particular, is this a proactive prevention approach or a post-crime solving approach?

Chris Lynam: I'd say it's both, but primarily we aim to be on the proactive side. As I mentioned in my opening remarks and on one of the questions, we will come across information of a website, an email address or a cryptocurrency wallet that is facilitating fraud. We will engage with the financial institution, the telecommunication provider or what have you to say, "Look, we think this violates your terms of service and it's over to you if you're going to do something about that."

Increasingly what we've done is try to do that at scale in almost in real time. I mentioned this Maple Disruption operation that brought all those partners together in person to do that. It created some real efficiencies in how we have to address that.

At the same time, if there is a victim or there's an investigation launched, law enforcement will work very closely with the financial institutions and with telecommunications and others as part of that investigation. The level of operational collaboration that I've seen has increased significantly in the last few years.

● (1250)

Michael Ma: Thank you.

What are the biggest operational barriers to coordinating anti-fraud efforts across sectors and jurisdictions? For example, is it data sharing that's been a problem, or is it jurisdictional fragmentation? Are these barriers international actors as well?

Chris Lynam: These barriers or challenges exist domestically and internationally to a certain extent. There are still some challenges with data sharing between public and private sectors, and what have you. A little bit is cultural as well—just asking, "Hey, am I going to take a little bit of risk to share this for the greater public good?" There's been great improvement there, though.

You mentioned cross-jurisdictional. That is absolutely a challenge. A lot of how we approach things is still very geographically based, domestically and internationally, so that's where we need really strong coordination. That's what my centres do day in, day out—they try to bring those parties together and figure out how we are going to make the best use of police resources to have the biggest reduction in terms of cybercrime and fraud.

Michael Ma: Thank you.

We briefly touched on the recovering of funds and so forth. How important is the speed of information sharing between institutions and law enforcement in preventing additional victims or recovering the funds?

Chris Lynam: Speed is absolutely crucial. I talked about there being a window—let's say an e-transfer or some kind of money transfer—before that gets completely settled. At the same time, there are times when certain transactions have already been settled, so they can't be recovered.

What I've seen in the last couple of years are discussions between banks and telecommunication companies on how to share that data to reduce further victimization, and then there was the stand-up of the Canadian anti-scam coalition, which we are a member of. It's a great initiative bringing all of these parties together to figure out holistic ways to either share information or tackle this problem.

Michael Ma: Thank you. We really appreciate your doing that.

During Fraud Prevention Month, the centre emphasized the importance of bringing hidden crime into the spotlight. Why is fraud still significantly under-reported in Canada, and how does that impact and prevent prevention efforts?

Chris Lynam: It's a great question.

I mentioned that we think only 5% to 10% of individuals report. There's a bunch of shame still associated with this. People think they've done something wrong. Particularly in the senior community, they worry because they've lost significant money. There's a shame piece, so we spend a lot of time trying to encourage people by saying, "You are a victim here." That's a lot of our message. I have highly trained folks, and when they talk to people on the phone, they take that victim-centred approach. However, there's more to be done on this. Public awareness campaigns continue to try to encourage reporting.

Just to finish off, I mentioned in my remarks that we've launched a new public reporting site. We still receive calls over the phone, but with the new site, we're now receiving two and a half times the previous online reports we were before. We're making some progress on the reporting side.

Michael Ma: I'm very glad to hear that. Thank you very much.

The Chair: Thank you, Mr. Ma.

[*Translation*]

As I mentioned in the beginning, I must reduce the time allotted for the next three questions. Mr. Ste-Marie will have one minute, Ms. Kronis will have two and a half minutes, and then, for the Liberals, Ms. Begum will have two and a half minutes.

Mr. Ste-Marie, you have the floor for one minute.

Gabriel Ste-Marie: Thank you, Mr. Chair.

Mr. Lynam, I'd like to hear your opinion regarding civil liability. In your view, should someone who is defrauded and has reasonable grounds to believe that the platform was negligent be held jointly liable, given that we are discussing a crime here? What percentage of fraudulent ads should cause an organization to be designated a criminal organization? Thank you.

[*English*]

Chris Lynam: Unfortunately, I'm not well placed to give civil legal advice on whether there is a civil liability matter between a person using a platform and what have you. As I said today, the digital platforms absolutely have a role in making sure that they receive information from us quickly, that they send us information and that they look for stuff on their platforms. I think there's still a lot to do on that front.

● (1255)

[*Translation*]

Gabriel Ste-Marie: Thank you, Mr. Chair.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

Ms. Kronis, the floor is yours for two and a half minutes.

Tamara Kronis (Nanaimo—Ladysmith, CPC): Thank you so much.

We're going to try to do this at the speed of cyber.

You talked about the need for prevention and described telecoms, banks and financial institutions as.... Is it fair to say that they're supportive and responsive but largely reactive?

Chris Lynam: Is that on the prevention side?

Tamara Kronis: No, I'm sorry. It's on the responding side when a scam is happening.

Chris Lynam: I'm not sure I fully—

Tamara Kronis: Let me ask this.

Is there anything that stops a scam or a text call from getting through?

Chris Lynam: There absolutely is, both on the telecommunication side and in finding other ways to interrupt it based on who owns that sort of chain. That is happening every day. We need to do more of that. We need to figure out the frameworks to increase that.

Tamara Kronis: Is it happening through voluntary action, or is happening through regulation?

Chris Lynam: I'm not well placed to say if it's a question on the telecommunication side of how that's being regulated or if it's voluntary. I know from the interactions we have with those sectors, they absolutely want to do more to reduce cybercrime and fraud.

Tamara Kronis: Do you know of anything that actually requires telecom companies to report how much scam traffic either is going on in real time or is moving through their networks?

Chris Lynam: None of that, but I know they have protocols like the STIR/SHAKEN protocol to verify calls and to make sure they are legitimate calls coming through there. I don't know the broader answer to the first part of your question.

Tamara Kronis: Are there gaps?

Chris Lynam: There is absolutely more work to be done to prevent that solicitation scam from getting to Canadians.

Tamara Kronis: Do you have any recommendations on what the federal government can do, using our telecommunications power, to take positive and concrete action that we're not already currently doing?

Chris Lynam: I have some decent visibility on how the telcos operate and their frameworks, but unfortunately, I'm not an expert in telecommunications regulations so as to give you an informed answer.

Tamara Kronis: In that case, could you use just the last few seconds that we have together to give some advice to the folks in my riding who are scared about this happening? What are the warning signs and what should they do first?

Chris Lynam: I will make it really easy. We use the “take five”. Take five minutes to think and reflect before doing anything. We break it down into three Rs: recognize, reject and report. It's like from my generation of stop, drop and roll. We have to have that mentality of very simple terminology to encourage people. Just take five minutes and that will avoid most of the scams.

Tamara Kronis: Thanks so much.

The Chair: Thank you, Ms. Kronis.

Ms. Begum, you have two and a half minutes.

Doly Begum (Scarborough Southwest, Lib.): Thank you very much, Chair.

Thank you so much, DG Lynam, for being here. I will also try my best to go at the speed of light or cyber light.

One of the things that we heard about over the last decade, especially from seniors, was the door-to-door scams that took place. Whether it was to inspect their water heater or something else in their house, they ended up with a $15,000 or $20,000 lien on their home. To this day, I know there are seniors who haven't really recovered from that, have had to pay or couldn't sell their properties because of that.

First, are there mechanisms or is there something we can do in terms of supporting those who have been victims of that?

I want to ask my second question, because I have little time. In reflection of that, I feel that youth are now coming across similar types of crime, which is not door-to-door but, rather, on their phones. For example, they get a message from Starbucks where they're offered a free coffee, and they click, “I agree”.

I was listening to a data scientist named Booshra Ahmed, who spoke recently at a talk about the hidden cost of clicking “I agree”. It's basically the future of AI, understanding what's happening, how your data is widely shared and what that means for you.

Could you speak to what we can do to support youth over the coming decades, and how we can avoid ending up in a similar situation?

Thank you very much.

Chris Lynam: I'll come at it from two angles. I'll come at it from the first part of your question.

Many seniors sometimes fall victim to these door-to-door scams. Guess who's really good at encouraging or educating senior citizens about fraud and cybercrime: other seniors. We operate a program with volunteer senior citizens whom we train. They go out and give in-person presentations. Sometimes we actually get the victims on the phone and talk to them to say how they shouldn't fall victim again. In some cases, they're in a scam and they should cease and desist. I go back to tailoring the prevention campaigns for the audience.

On the youth question, it has to be a societal approach. It has to be in schools. We have to engage them online. That's where they are to a certain extent. Parents, absolutely, have to have conversations with their children about how to recognize a scam or know the dangers if they send intimate photos. They should be told, “Please do not engage in this type of activity; it will ruin your life.” I use that example, but there's not going to be only one way on the prevention side. It has to be tailored to specific audiences.

● (1300)

Doly Begum: Thank you very much.

The Chair: Thank you very much.

Mr. Lynam, I really appreciate your being here today. Thank you for the ongoing work of you and the RCMP in doing everything that you can to assist in putting an end to and mitigating the risks associated with all of this. We certainly look forward to any further input that the agency may have in terms of public policy development on the part of the federal government.

Colleagues, I'm going to suspend briefly as we turn over. I will just let you know—so that the parties can discuss this in advance—we will not have time for the third questioner in the next hour. That means there will be be two from the Conservative side and two from the Liberal side. Mr. Ste-Marie's time will be reduced. I will let you spend the next few minutes deciding how you want to order your affairs.

Again, Mr. Lynam, thank you very much, and enjoy the rest of your day.

We're briefly suspended.

● (1300)

_____(Pause)_____

● (1310)

The Chair: I call the meeting back to order.

Colleagues, we are going to enter into our third and final hour of today's meeting. We have two new witnesses joining us. We have one in person and one online.

From the Canadian Association of Retired Persons, joining virtually, we have Anthony Quinn, who serves as the president of the organization. Here in the room with us, from Wealthsimple, is Colin Smith, who is the vice-president of risk and decision science.

Gentlemen, you will have up to five minutes for your introductory remarks, followed by questions and answers from the recognized political parties around the table.

Mr. Quinn, I'm going to start with you. You have five minutes, sir.

Anthony Quinn (President, Canadian Association of Retired Persons): Mr. Chair and members of the committee, thank you for the invitation to appear today.

My name is Anthony Quinn, and I'm the president of CARP, the Canadian Association of Retired Persons. We represent more than 250,000 members across Canada and advocate on issues affecting older Canadians, including financial security, health care and freedom from age discrimination.

For older Canadians, fraud can be a life-altering event. When a senior loses money to a scam, they are often losing retirement savings accumulated over decades. The unique peril for senior victims is that they may have little or no opportunity to return to the workforce to earn that money back. For the vast majority of older Canadians, the consequences of fraud are permanent.

CARP recently surveyed our members, and over 8,000 replied. More than 82% reported that they had been targeted by a scam and nearly one in five reported having lost money to fraud. All available and reliable sources tell us that only between 5% and 10% of frauds are reported. We therefore believe the true scale of the problem is significantly larger than even our own polling reveals.

For the last decade or more, Canadians have been told to be more careful, and seniors have heeded that message. They have attended seminars, watched public service announcements, read bank brochures and learned to be skeptical of unsolicited texts, calls and emails.

Banks, telecom companies, digital platforms, governments and advocacy organizations like our own have encouraged Canadians to remain vigilant, yet fraud losses continue to rise. At some point, Parliament must ask whether the burden of prevention has been placed too heavily on the victims and too lightly on the institutions through which these scams are delivered.

From the perspective of an older Canadian who has lost a lifetime of savings, educational programs, corporate platitudes, public relations campaigns and reminders to be careful are not enough. Our message to this committee is that fraud prevention must become a system responsibility, not merely an individual responsibility. That means telecoms providers must do more to authenticate calls, prevent spoofing and block fraudulent texts before they reach Canadians. 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.

In this case, Parliament should be asking whether the incentives for prevention are properly aligned.

Let me give you just one example of a CARP member. Peter Squire is a 70-year-old retired market analyst from Winnipeg. He is not inexperienced or financially unsophisticated. Mr. Squire received what appeared to be a legitimate call from a senior investment professional. The documents sent to him carried bank branding. The phone number appeared legitimate. The proposal looked legitimate. He sought assistance from established financial institutions and proceeded with what he thought was a secure financial investment. Instead, nearly $650,000 of his retirement savings disappeared in a sophisticated fraud.

What struck me about Peter's story was that he did many of the things we tell Canadians to do—he asked questions, he dealt with recognized institutions and he sought professional assistance—yet he still became a victim. That's why CARP believes fraud prevention cannot rest primarily on individual vigilance. The systems through which these scams are delivered must do more to prevent them from succeeding in the first place.

There's another contrast that many seniors find difficult to understand. When approximately $20 million in gold was stolen from Toronto Pearson airport, there was an immediate, all-hands-on-deck response. Police agencies mobilized. Federal authorities became involved. Insurance companies activated recovery efforts. Security experts were deployed. International investigations were resourced and engaged. Canadian authorities worked with police agencies and partners in the United States, India and other countries. The story dominated national headlines. Resources were marshalled. Accountability was demanded. Recovery became a priority.

However, when a senior loses $650,000 in retirement savings to fraud, the response can feel very different. The victim is often told to call their bank, then the police and then the Canadian anti-fraud centre, and although they are met with sympathy, the typical response is, “I'm sorry, but there's not much we can do to help.”

● (1315)

Seniors in Canada are asking why Canada appears to be capable of mounting coordinated national and international responses when institutional assets are stolen, but when ordinary Canadians lose billions in the aggregate, not much happens. From the victim's perspective, their consequences are far more devastating. When institutions bear the cost of a loss, they tend to act in a more coordinated and more international response. CARP believes the system deserves prevention, accountability and consumer protection built into the infrastructure, rather than relying primarily on individual vigilance.

I would also note that CARP is engaged in a separate but related initiative concerning competition, transparency and the quality of investment advice available to Canadians through branch-based investment channels. Over the past year, we have raised these concerns directly with banks, regulators, the Competition Bureau and officials in the Department of Finance. We have appreciated the constructive dialogue we've had with the Minister of Finance's office. While it is distinct from today's discussion on fraud and scams, the underlying principle is similar. Canadians must have confidence that their financial system is working in their interests, that conflicts are properly managed and that consumers receive fair treatment and meaningful protection.

After a decade of rising fraud, increasing losses and missing opportunities to act, Canadian seniors are asking for protection and accountability. They are asking for financial and communication systems that are working as hard to prevent fraud against consumers as they are to prevent losses in the institutions themselves.

Thank you. I look forward to your questions.

The Chair: Thank you very much, Mr. Quinn.

Mr. Smith, the floor is yours for up to five minutes.

Colin Smith (Vice-President, Risk and Decision Science, Wealthsimple): Thank you, Chair.

Thank you to the members of the committee for the invitation today.

Wealthsimple is Canada's leading financial innovator. We are trusted by more than four million Canadians and hold over $150 billion in assets. Protecting the trust that Canadians place in us is central to what we do.

What does fraud look like today? We've spent years hardening our systems against direct attack, but fraud has increasingly moved from attacking those systems to attacking the people using them. Clients of all financial institutions find themselves on the front line.

The most damaging attacks are also the hardest to detect, because the fraudster never touches our systems at all. Instead, they get the client to move the money themselves, often while the client believes they're being helped. The tactics are old, but what's new is the speed. With AI, a fraudster can clone a familiar voice or forge a convincing document using tools anyone can download, collapsing what used to take weeks into minutes.

This has changed how we fight fraud. We've come to believe that prevention works best when technology and people work together. Everything we do behind the scenes to detect fraud is paired with real tools that let clients take part.

A pass-key, for example, is a simpler, safer way to sign in to your account using your device's biometrics or PIN. Unlike traditional passwords, pass-keys are uniquely tied to your personal device and to Wealthsimple, meaning that they won't work on fake or fraudulent websites. When we launched pass-keys in the first quarter of this year, our clients immediately moved to protect more than $10 billion dollars behind them.

Another new tool is trusted places. Clients can mark locations like home or work as trusted. Moving money from anywhere else triggers extra verification on terms that they set. More than 500,000 of our clients' transactions have already been verified in this way.

We also protect clients by reaching them in real time. If someone is moving money in our app while on a phone call, we show a warning that the call is not from us. When a client appears to be a victim of a scam, a specially trained team we call our spell breakers group reaches out to talk to them before the money is gone.

Financial institutions and clients can work together to fight fraud, but most fraud originates outside of the financial system. Preventing it must be a shared responsibility across financial institutions, telecom providers and social media platforms, especially as AI accelerates these scams.

Many fraud attempts against our clients begin on social media, where scammers use our name and logo to run fraudulent ads that pull Canadians into scams like pump-and-dump investment schemes. Between October 2025 and January 2026, we reported more than 10,000 such ads on Meta platforms. During this period, it took an average of four days for these ads to be removed after we reported them to Meta.

More recently, we caught and reported as many as 1,500 fraudulent ads in a single day. We do what we can to protect our clients from these scams. We built an AI-powered system to identify potential pump-and-dump stocks in real time and automatically warn clients who might who might be about to buy in.

Reporting ads one by one is a losing game. We have yet to see a platform-level or policy solution from Meta to address this issue. 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. That is the central recommendation in our submission to the government's national anti-fraud strategy.

We welcome the government's and this committee's focus on protecting Canadians. Fraud is not going to slow down.

What gives me confidence is that our clients have shown that they want to be active partners in their own protection, and that partnership is how we will keep Canadians safe.

Thank you. I look forward to your questions.

● (1320)

The Chair: Thank you very much, Mr. Smith.

I'm going to take the rare opportunity off the top to ask a question, because you piqued my interest on something that came up earlier this week in testimony.

How many days did you say it took Meta to take down a fraudulent ad that you had flagged for them?

Colin Smith: During that period, it was an average of four days.

The Chair: Did Meta acknowledge that it was a fraud at the outset, or was their rationale that they were uncertain as to whether or not it was fraudulent?

Colin Smith: We would submit them for review, and that review process—which they do internally to determine whether or not the ads are scams—took that amount of time to complete.

The Chair: Okay.

I'm sure other members will follow up on this. If they don't, I may return with some questions at the very end.

With that, Ms. Borrelli, the floor is yours for six minutes.

Kathy Borrelli: Welcome to our witnesses. Thank you for being here for this important study.

My first question is for Mr. Quinn.

Many seniors are targeted through fake tech support scams or bank impersonation scams, where the victim is convinced to install remote access software. Once that happens, the scammer may be able to guide them to divest all of their life savings.

Should banks or payment platforms be required to add extra verification or temporary holds when high-risk payments are attempted from a device showing symptoms of remote access?

Anthony Quinn: Thank you for the question.

I do believe that the banks must take a higher level of responsibility for those losses. There are no scams taking place, typically, that are taking cash out of the hand of an individual. The scammers are required to use the systems, electronically, that are owned and operated by the banks. The money is typically transferred from one institution to another using their systems. Our members believe that a greater responsibility must be placed on the institutions themselves. Without that, education alone—despite the efforts across the board—will not be enough to prevent the frauds and scams from taking place, and there's no opportunity to recoup.

Kathy Borrelli: Thanks, Mr. Quinn.

One challenge is that seniors need protection from fraud, but they should not be treated as incapable of managing their own money. Any solution has to protect independence while stopping high-risk manipulation.

What kinds of safeguards would your members accept? Examples are trusted contact, optional transaction limits, delays for unusual transfers or things of the like.

● (1325)

Anthony Quinn: We're always concerned about a paternalistic attitude toward older adults and the sense of taking away their ability to control their own financial decisions. We have to balance that with the pressure that fraudsters use to encourage the victims to act hastily on a limited-time offer or when presented with the case of an emergency situation, like the grandparent scam where the grandchild has some kind of criminal or health-related concern.

I believe our members would rightly give up a little bit of that control for some delay in the transfer if that meant they were being protected by the banks and were able to ensure that the transfer was legitimate.

Kathy Borrelli: Do you think there should be one clear front door for senior fraud victims with banks, platforms, telecoms and police—like a hub they can go to once they've been divested of funds?

Anthony Quinn: We heard from the Canadian anti-fraud centre. When we speak to the Canadian anti-fraud centre, they say they're not able to answer the majority of the phone calls coming in. They're directing those who have been scammed to fill out online forms. They've been scammed online. They try to get some kind of attention from the RCMP and other police forces, and they're told to file a form online. We need some type of immediate action from the banks, if they're able to recover.

Ensuring that the banks are trying to prevent the fraud at the front end is far more important than having a place for seniors to report after they've had their money stolen. The case right now is that it's too late and everyone expresses regret at the loss. There's a sense that the system isn't really there to protect them.

Kathy Borrelli: In our previous hour, we spoke with Chris Lynam of the Canadian anti-fraud centre. He advised of a program they have where seniors are helping seniors. Do you know of that program? Have you seen it work successfully at all?

Anthony Quinn: That is just one of likely thousands of fraud prevention programs going on across the country. The point that we're trying to make today is that education is only a small part of the problem. It has proven not to be effective. Even those who have heard the messaging are still falling for the frauds. We need the institutions to play a greater role in protecting seniors from these frauds.

Kathy Borrelli: I get a lot of inquiries. I get a lot of emails and calls from seniors who have fallen victim to some of these fraudsters. Where's the best place to send them? How can I help them?

Anthony Quinn: I wish I knew, Madam.

We're asking Parliament to take a lead on this—to encourage and perhaps require institutions to play a greater role, to invest in enforcement and to increase the penalties and punishments in our country so that fraudsters will be less inclined to participate.

Kathy Borrelli: What is your biggest ask? What do you want the most from government?

Anthony Quinn: My biggest ask is that the institutions, particularly banks and telecoms, be held to a higher degree of accountability in this and 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.

Kathy Borrelli: Thank you, Mr. Quinn.

Anthony Quinn: Thank you.

The Chair: Thank you very much, Ms. Borrelli.

I believe we're going to have Mr. Fanjoy splitting some time with Mr. Bains. I'll let the two of you sort that out.

For now, the floor is yours for six minutes, Mr. Fanjoy

Bruce Fanjoy (Carleton, Lib.): Thank you, Chair.

I'm really pleased to see the Canadian Association of Retired Persons present. I'm sure everyone around this table has members of their own family who are getting older and more vulnerable to sophisticated financial crimes. We all share a desire to protect them while respecting their independence and agency.

I'd be interested in your thoughts on how to strike that balance of making sure we don't take away their independence while actively protecting them, but recognizing that some of our seniors are dealing with undiagnosed dementia, which would make them especially vulnerable.

● (1330)

Anthony Quinn: Thank you very much.

The fraudsters are using more and more powerful psychological tricks and efforts to convince Canadians to fall for these scams. It's not necessarily related to cognitive issues. It's more likely to be someone's exaggerated sense of their own awareness and ability to interpret these financial decisions. I think we have to look to international jurisdictions that have put more effort into protecting them, beyond education—the U.S. and the U.K.—and really encourage....

Again, parliamentarians, require these institutions, particularly banks and telcos, to play a greater role in the protection of Canadians, seniors being the largest number and losing the most money. Put in requirements that if they are not making these provisions and protections and are not putting them in place to prevent the frauds, they will be responsible for the financial losses. If they are put in that position, they will be more likely—more incentivized—to increase protections for Canadians.

Bruce Fanjoy: Thank you.

I will pass the remaining time to Mr. Bains.

Parm Bains: Thank you, Mr. Fanjoy.

Thank you to the witnesses for joining us. I'm going to try to quickly get into this.

Mr. Quinn, I'm from Richmond, British Columbia. It has the longest life expectancy in Canada and a lot of seniors living here.

I know you talked about telecoms. We heard from previous witnesses today about the sophistication behind the fraud and the scam compounds. You talked about the emotional side and how clever the fraudsters are becoming. We also heard, previously, about loneliness. They target people who are lonely. Can you talk about some specific gaps and provide recommendations for our financial crimes agency, moving forward? Are you participating in submissions for the financial crimes agency?

Also, telecoms provide alerts if there's a call that appears to be a potential scam. Do you wish there were alerts available in the banking system, in some way?

Anthony Quinn: I think all of the above apply, sir.

The idea that banks and telecoms are not doing anything is not what I'm trying to get across, but there is certainly room for more. We see on our phones the alerts indicating that this may be a scam call, but many calls are still getting through. On the social media side, as my colleague from Wealthsimple mentioned, there is literally a deluge of fake and phony ads on social media, which is where seniors are gathering for much of their information and their digital lives.

When it comes to gaps, I think my answer would be that we would like parliamentarians to really take an aggressive approach to regulating the institutions, through the CRTC and the control you have over financial institutions, to require them to play a greater role.

We cannot ask the victims—seniors and younger Canadians—to be experts in all of these developing fields, but we should be requiring these large, national institutions, which have no competitors and are earning billions of dollars a year in revenue from Canadians, to be true partners in protecting us from the fraudsters.

Parm Bains: Thank you. I believe that's my time completed.

The Chair: Thank you very much, Mr. Fanjoy and Mr. Bains.

[*Translation*]

Mr. Ste-Marie, you have the floor for six minutes.

Gabriel Ste-Marie: Yes, thank you, Mr. Chair.

I would like to thank both witnesses for being here.

Mr. Smith, you're telling us that other countries require digital platforms, such as Meta, to verify the authenticity of companies offering financial services through their advertisements, and you're asking that this be done here as well. Is that correct?

● (1335)

[*English*]

Colin Smith: Yes, that's correct. You can see listed on Meta's website the list of countries that require additional verification for any advertisements in a number of industries, including financial services. This is something that Meta has the technical capability to do but chooses not to do in Canada.

[*Translation*]

Gabriel Ste-Marie: I'm stunned.

Do you know if other countries with stricter checks have seen this type of fraud decrease among their populations?

[*English*]

Colin Smith: That is my general understanding, yes. I'm not necessarily an expert in all the stats in other countries, but this verification step is definitely important. In the context of what we've seen impersonating Wealthsimple, it's been as egregious as deepfakes of our CEO pitching stocks to Canadians. It is clearly fraudulent material using our brand.

[*Translation*]

Gabriel Ste-Marie: This is truly concerning. Thank you very much.

Do you know why Meta does not offer this additional verification process in Canada? In other countries, did this require the passage of a law or regulation—something the government hasn't done here yet?

Do you believe that the fact that this process hasn't been implemented here constitutes a form of laxity on the part of digital platforms?

[*English*]

Colin Smith: Yes, I believe a big part of why they haven't done them here is that it's just extra friction in the process of putting ads on the platform. I do think it's a spot where the government could step in.

[*Translation*]

Gabriel Ste-Marie: Thank you very much.

Mr. Quinn, thank you very much for being here as well.

We hear too many horror stories like the one you referred to, where seniors find their accounts drained of their life savings, and nothing is done about it. This has to change. There are many cases in the Quebec media, on public affairs programs, that report on the scams that have taken place. It's been a few years now. Things are moving very slowly.

From your remarks, I clearly understood that telecommunications companies, financial institutions, and digital platforms must be held more accountable. On that note, I'd like to hear your opinion on the issue of civil liability. If someone has been defrauded and there are reasonable grounds to believe that the platform where the advertisement was posted was negligent, should the platform be held jointly liable?

[*English*]

Anthony Quinn: I don't think I could argue against that, sir.

We have arrived at a situation in Canada of blaming the victims for not educating themselves or not being aware enough. I believe we have to turn the tables to protect Canadians. If this means holding the platforms themselves accountable—the telecoms, the digital service providers or the financial institutions—I would not think that our members would disagree with that.

[*Translation*]

Gabriel Ste-Marie: Thank you. Obviously, we're talking about crimes here; what's being done and these thefts are criminal acts.

Earlier this week, Meta told us that it is making significant efforts to reduce fraudulent ads, even though it takes an average of four days to remove them once they've been reported. Furthermore, as you mentioned, there is a flood of fake ads on these platforms. We've also heard that perhaps 10% of the ads are fraudulent, but that Meta generates revenue from them.

In your opinion, what percentage of fraudulent ads should mean that an organization is designated as a criminal organization?

● (1340)

[*English*]

Anthony Quinn: It would be hard for me to speak to the percentage, but when we know the funnel through which the majority of these crimes are being perpetrated is Meta and similar organizations, I think we have to hold them to a higher standard, require them to be part of the solution and not allow them to continue to be the funnel through which these international or domestic criminals are working.

[*Translation*]

Gabriel Ste-Marie: Thank you.

Mr. Chair, I am yielding my remaining 10 seconds of speaking time to you.

The Chair: You had about 15 seconds left. As always, thank you for your generosity, Mr. Ste-Marie.

[*English*]

Ms. Kronis, the floor is yours for five minutes.

Tamara Kronis: Thanks so much.

Mr. Smith, I'm going to ask you a few questions.

I thought you put it really well when you said that the system has moved to attacking the people who are using the systems—as opposed to attacking the systems—and getting the clients to move money. Of course, the big challenge with that is that it's happening at the speed of cyber. There has been a huge focus on trying to get data after the fact, but prevention, at this point, is largely reactive. Is that fair?

Colin Smith: The way we've been tackling this at Wealthsimple is to think about putting security features more directly into the client experience in our application so that they're part of how our clients interact with Wealthsimple. It's not just the behind-the-scenes fraud rules and models that we run.

Tamara Kronis: Of course, the hard part for you is that the financial institutions really are the face of this. When someone finds out that they've been scammed, the first place they call is the financial institution. In many investment scams, once the money is sent, especially if it's sent through crypto or some kind of offshore platform, recovery is virtually impossible. Is that correct?

Colin Smith: That's generally true. We do attempt recovery on behalf of our clients in fraud cases, but there can absolutely be challenges in doing so.

Tamara Kronis: From a systems perspective, you do try to do some proactive things, but from a legislative perspective, the system's still really dependent on the victim spotting the fraud and reporting it after the fact. Is that fair?

Colin Smith: I don't think that's entirely fair. We take a lot of proactive measures on behalf of our clients. That could be placing warnings in the app if we see something that seems suspicious for a client before they do a transaction. For example, if we have a client who is attempting to move money in crypto for the first time, there's a non-dismissible breather screen that goes up, warning about the typical types of scams that happen on crypto, and they have to accept it to move past it.

We're definitely thinking about how we can be more proactive, despite the legislation that you mentioned.

Tamara Kronis: That's really helpful to know.

As a financial institution, do you have any way to police things like big investment ads, other than having someone sit there and behave like the user?

Colin Smith: As for the ads themselves, we report these ads daily. It's an incredibly manual and time-intensive process, where we scan for new ads using our trademark or our brand name, and we report them to the social media platforms. We've had to then build a more sophisticated infrastructure on the back end.

Since we can't prevent the ads from showing up, what we've tried to do and where we have control is in seeing which clients are making which investments on our platform and how those stocks are being talked about either on social media or in the news. After combining those different signals together, we are able to place warnings to clients before they buy into something like a potential scam.

Tamara Kronis: When you talk about the things that you can control, is there anyone who has control over those fraudulent ads and whether or not they're going to appear? Is it the telcos? Who's in the best place to be able to prevent that?

Colin Smith: That would be the social media platforms.

Tamara Kronis: What do you think the most effective way would be for us, using our federal telecommunications power, to bring all the parties together and, in a compulsory way, address some of the issues that Mr. Quinn brought up and some of the things that you're seeing in terms of losses?

● (1345)

Colin Smith: First and foremost, requiring the social media platforms to verify that all advertisers of financial services are legitimate and are verified advertisers would go a long way. What we see is that these ads are spun up by many different accounts very rapidly, all of which are using something like Wealthsimple's logo or brand name, but are not associated with us in any way.

Tamara Kronis: We see the government moving in a number of different bills, which are sometimes hard to follow, to try to deal with some of the things online. Is there anything in any current legislation that really helps get at the heart of this problem?

Colin Smith: Not that I'm aware of.

Tamara Kronis: Thank so much.

The Chair: Thank you very much, Ms. Kronis.

Ms. O'Rourke, I believe you intend to split a bit of your time with Mr. Ma, so I'll let the two of you sort that out.

The floor is yours, between the two of you, for five minutes.

Dominique O'Rourke: Thank you, Chair Carr.

Mr. Smith, it is terrific to hear about your spell breakers group and your proactive measures.

I want to circle back. You said that you identified 1,500 fraudulent investment ads in one day on the same platform. You reported them, and it takes on average four days to take those down. It's stunning, because Meta can block any news story from being posted at all, so it's quite shocking for this committee to hear.

You are a regulated, legitimate fintech. You are digital first, so I'm guessing you have to prove you're a legitimate platform in order to advertise there. What should the threshold for advertisers be to prove that they're legitimate?

Colin Smith: The threshold should be the same as for other verified ads on other platforms, which is that for any advertising platform, you know who's paying for the ad and that should be the same as the brand name that's featured in the ads, particularly in places like financial services.

Dominique O'Rourke: For an industrial-sized company like that, should they have the tools to do that?

Colin Smith: They do this in other jurisdictions, yes.

Dominique O'Rourke: That's beautiful. Thank you.

I'll cede my time to Mr. Ma.

Michael Ma: Thank you very much.

Mr. Smith, you spoke earlier about the platforms needing to verify ads, and you also just mentioned that payments are one way of doing that.

Why do you think platforms such as Meta take four days to take them down, when they can take down news articles within an hour or so?

Colin Smith: I guess I would be speculating that it's because they make money on these ads. It's like anything in this space. You have to balance that.

Michael Ma: Thank you.

My next question is for Mr. Quinn.

You mentioned in your opening remarks that financial institutions should do more regarding fraud prevention. Can you also speak, then, to what roles these social media platforms should be playing more often to help prevent frauds?

Anthony Quinn: The focus I put on financial institutions was specifically because that is the means through which money is being transferred. The introduction to the scam is perhaps happening through a Facebook ad, where someone is posing as Wealthsimple or as the Prime Minister touting a “too good to be true” investment opportunity. When the financial transaction is occurring, as in our members' case, the money is taken out of that individual's or senior's bank account, which is held with a trusted financial institution, and the bank's resources are being utilized to move that money.

That's why I was focused more on the financial institutions rather than the advertisers or the purporters of the message, but we have no less concern about that than we have with the financial institutions.

Michael Ma: Thank you.

Along that line, can you speak to the importance of public awareness, as we heard earlier from the RCMP, in terms of combatting financial fraud and scams for, especially, seniors and retired people?

Anthony Quinn: There's no doubt 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. CARP believes we now have to focus on the financial institutions and the telcos and hold them to a higher degree of responsibility to ensure that they are doing everything in their power, hopefully with the pressure of Parliament, to protect Canadians from frauds and scams.

● (1350)

Michael Ma: Thank you.

Along that line, Mr. Quinn, CARP sent a letter to the government in which you advocated for enhanced federal coordination and enforcement capacity in addition to stronger actions to hold banks accountable. How do the upcoming measures to fight financial fraud, such as the anti-fraud strategy, the Bank Act amendments and the financial crimes agency, demonstrate meaningful progress in protecting seniors and retired people from financial fraud and scams?

Anthony Quinn: I would say that those provide great signals that the government is starting to pay attention and take action, but we have yet to see the fruit of many of those natal programs. I would like those to have greater strength in prosecution. Many of the criminals are hiding behind the theft of under $5,000 or other slap-on-the-wrist crimes and are still stealing millions of dollars annually. Criminal along with institutional protections are two things that CARP is asking the government to take action on.

The third thing, I would add, is just the inability of police to go across jurisdictions in chasing these criminals domestically. We know how difficult it is to go across international borders, but even within Canada, police and victims are reporting to us that a criminal in Vancouver is stealing from a victim in Saint John. The police aren't able to take action despite knowing who, where and why the crime took place.

Michael Ma: Thank you, Mr. Chair.

The Chair: Thanks, Mr. Ma.

[*Translation*]

Mr. Ste-Marie, you have the floor for one minute and thirty seconds.

Gabriel Ste-Marie: Thank you, Mr. Chair.

Mr. Smith, currently, in cases of fraud where someone makes an unauthorized transaction, it is the financial institution that is expected to pay.

In the context of an open banking system, there is a risk that the financial institution and the exchange platform will pass the buck back and forth, or that the fintech company may not have the means to pay. How, then, can we ensure that the consumer is not left holding the bag?

[*English*]

Colin Smith: In the world of open banking, I think we will see a lot of benefits in consumers being able to more freely share their information across institutions than we see today, with bank linking and other methods, which in some instances can make account security more challenging. In my view, I don't think there would be a risk of changing liability or payments in the case of fraud, as you're asking. We would expect that to stay largely the same and that all the regulated financial institutions that would be a part of open banking would continue to meet the same obligations there.

[*Translation*]

Gabriel Ste-Marie: We can discuss this at another time.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

I'll take one minute to ask two very brief questions here.

One is for you, Mr. Smith. We've had referenced now a number of times throughout this meeting, as a result of your introductory remarks, the delay in relation to Meta's response once fraud is flagged on your organization's part. Are you able to publicly share with us the contents of any conversations you've had with similar financial bodies who have experienced the same type of delay in that type of fraudulent instance?

Colin Smith: I think we could take that away and follow up in writing with some similar conversations. Yes, it's certainly something we've discussed within the industry.

The Chair: I appreciate that. I would encourage you, where reasonable, to perhaps congregate with some of your colleagues who hold similar roles and have a conversation about what their experiences have been, and if you see fit to provide this committee with a more sophisticated and detailed report about what your collective experience with Facebook specifically has been in relation to this, we'd appreciate that.

My final question will be for you, Mr. Quinn.

Again, in relation to Meta, are your members discussing with you what their experiences have been when a fraud has occurred on Facebook? Are they reaching out to Facebook? Is Facebook reaching out to them to say, “We want to inform you that you may have been or currently are the victim of fraud?” Are your members writing to Facebook and asking for support or guidance, and if so, are they receiving any type of correspondence in return?

Can you briefly paint a picture for us, please, of what the relationship between senior citizens in Canada and Facebook looks like from your perspective when it comes to fraudulent activity that originates and exists on its platform?

Thank you, Mr. Quinn.

● (1355)

Anthony Quinn: Thank you, Mr. Chair.

We have seen no proactive efforts on behalf of Facebook or Meta in communicating with seniors.

The majority of our members who are interacting with us are interacting through Facebook. Every post that we put onto Facebook is targeted by scammers, because they know seniors are congregating on our Facebook page, and the frauds flow directly after our posts and the conversations that our members are having. Everything from romance scams to financial opportunities and job offers are all scams that are immediately flooding into our members' conversations.

I have no faith that Facebook or Meta are being proactive in protecting seniors in Canada.

The Chair: Mr. Quinn, I have one last follow-up question.

Do you see value in using the testimony you've provided today, alongside that of Mr. Smith and the questions you've received from committee members, to post something from your organization on Facebook in the next week or so asking Facebook to elevate, using its very sophisticated algorithms and capabilities to do so, that message and challenge them to see if they would be willing to do so? Is that something you might entertain?

Anthony Quinn: I would certainly entertain that, Mr. Chair. I would look for the support of your kind offices and perhaps some experts. We are not the tech experts on this side, but anything we can do to engage with Facebook and to encourage them to take proactive action would be welcome. We'd be happy to participate.

The Chair: Mr. Quinn, I'll give you my word—I can't speak on behalf of any other members around this table—that if I see that CARP posts in the next few days or weeks anything in relation to a direct call on Facebook to be more accountable for the fraud that's occurring on its platform and that you and your membership are driving a call to action, I will be honoured and pleased to use my social media networks to elevate that message.

On that note, Mr. Smith and Mr. Quinn, thank you very much for being here today. You've helped us generate a better understanding of the scope of the problem we are facing. It's quite devastating to continue hearing these stories, the most tragic of which involve the destruction of the life of an individual who's worked for decades to build a nest egg for themselves and their families to enjoy the time they have left here in our country. We will do what we can to take action, and your guidance will assist us very much in doing that.

With that, thank you, gentlemen.

Members, I'll give a very brief reminder that next week Minister Solomon will be here on Monday in relation to our AI strategy. On Tuesday, we will finalize the mould-makers report that we have been working on, I hope, and we will hear the last couple of hours' worth of testimony in relation to this study.

With that, I wish everybody a great rest of the week and weekend.

The meeting is adjourned.