HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

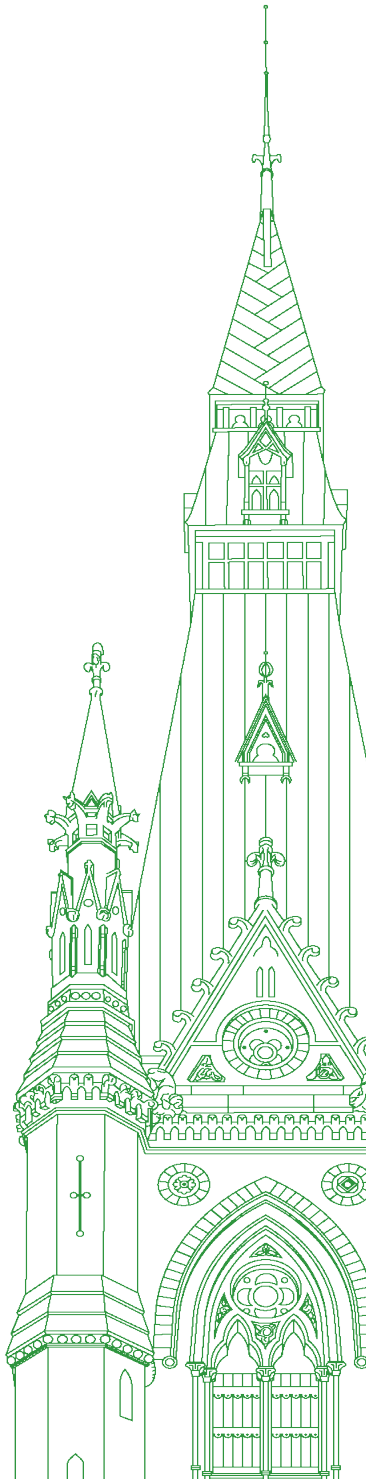
45th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 042

Thursday, June 4, 2026



Chair: Ben Carr

Standing Committee on Industry and Technology

Thursday, June 4, 2026

● (1105)

[*English*]

The Chair (Ben Carr (Winnipeg South Centre, Lib.)): Good morning, everybody.

[*Translation*]

Welcome.

I hope everyone is having a good week.

[*English*]

We're going to start a new study this morning, one that is of significant importance to Canadians across the country.

I'd like to just begin with a reminder for witnesses.

If you're using your earpiece, please ensure that, if it's not on your ear but plugged in, you have it on the sticker in front of you. That's to protect the health and well-being of our interpreters.

[*Translation*]

I confirm that we've done all necessary tests and that both video and sound are working well.

[*English*]

Colleagues, we will have one hour of testimony with the witnesses before us this morning, and then we will go in camera to hopefully finish the second version of the mould-maker study report that we were working on previously.

With that, I'd like to welcome the witnesses who are here with us today.

From the Canadian Bankers Association, we have Anthony Ostler, president and chief executive officer; and Hartland Elcock, assistant general counsel and vice-president.

Gentlemen, welcome.

From the Canadian Telecommunications Association, we have Eric Smith, senior vice-president.

Welcome, sir.

From Telus, we have Carey Frey, chief security officer.

Welcome, Mr. Frey.

Witnesses, you'll each have up to five minutes for your introductory remarks. You don't have to use them all, but you're certainly entitled to them.

Following the introductory testimony from our three witnesses, we will then turn to members around the table from the various recognized political parties to get into questions and answers.

For the Canadian Bankers Association, Mr. Ostler, I suspect it will be you who will be speaking. The floor is yours, sir.

[*Translation*]

Anthony Ostler (President and Chief Executive Officer, Canadian Bankers Association): Thank you very much.

Good morning.

I'm very grateful to the committee for giving us the opportunity to contribute to its work on financial fraud and scams in Canada.

My name is Anthony Ostler, and I'm the president and chief executive officer of the Canadian Bankers Association, or CBA. I'm joined today by Hartland Elcock, assistant general counsel and vice-president at the CBA.

The CBA represents more than 60 Canadian and foreign banks operating in Canada. It supports the adoption of public policies to maintain a strong and dynamic banking system capable of helping Canadians achieve their financial goals.

[*English*]

Addressing financial crime is a top priority for the CBA. As a board member of the International Banking Federation, IBFed, I saw first-hand at our November 2022 meeting in Sydney how Australia was responding through a growing cross-sector public-private approach. Cybercriminals were exploiting the digital connectivity accelerated during the pandemic, stealing from individuals and laundering proceeds, often supporting organized crime, bad actor nation-states and terrorism.

In 2023, Canada was continuing to see an increase in fraud and scams, while Australia began reducing them through its cross-sector program. By early 2024, it was clear that we should apply those lessons in Canada. Two years ago, the CBA brought together some 50 public and private sector partners, including regulators, financial institutions, telecommunications providers, law enforcement and digital platforms to create the Canadian anti-scam coalition. The coalition coordinates education, awareness and prevention efforts, including the development of a national taxonomy, a fraud detection pilot, and the ongoing Stand Against Scams campaign.

While I'm here today as head of the CBA, I also continue to chair the coalition's steering committee, now housed in the Canadian Cyber Threat Exchange.

The CBA has also provided comments to Finance Canada in support of a national anti-fraud strategy. We support a federal cross-sector approach to strengthen consumer protection and reinforce trust in Canada's digital economy, starting with the financial services, telecommunications and digital platform sectors. These sectors intersect across the fraud life cycle, and the Canadian anti-fraud centre has found that over 85% of fraud dollar losses can be traced back to telecom or digital channels. Coordinated action across sectors, alongside responsible consumer behaviour, is critical to reduce fraud-related harm to Canadians.

In January 2025, I became chair of the IBFed and launched a task force to share international best practices on fraud and scams. In March, I led an IBFed delegation to the United Nations-Interpol Global Fraud Summit in Vienna. Key outcomes included a call to action for countries and a global public-private partnership framework for institutions. Thirty-seven member states, including Canada, have endorsed the call to action, and the CBA, IBFed, governments, digital platforms, NGOs and other organizations have endorsed the framework. This international work continues through pilot projects to strengthen fraud protections.

As Australia's experience and the recent future of financial information sharing research show, cross-sector information sharing is essential. Supported by strong governance and privacy protective guardrails, this voluntary and conditional information sharing will allow Canada to fight fraud across its full life cycle.

Public awareness and education are also critical to an effective national anti-fraud strategy. They support earlier detection, better decisions, prevention and improved reporting. We encourage the government to further support the coalition's multi-sector Stand Against Scams campaign. A whole-of-government strategy can help organizations contribute their expertise, but roles and mandates across this system must be clearly defined. Better coordination among Canadian law enforcement at all levels and with international partners will require a clearer intelligence-informed operating model.

We also believe the Canadian anti-fraud centre should remain Canada's primary hub for fraud reporting and intelligence aggregation. As I have noted, the financial crime environment is evolving quickly, and the AML-ATF regime must keep pace. That is why we support the government's creation of a financial crimes agency, the FCA, which promises to help Canada's fight against complex financial crime. As it develops, the CBA supports the FCA's becoming the national operational lead on combatting financial crime, with a coordinating and priority-setting role to help guide the AML regime's continued evolution into a more risk-based, fit-for-purpose framework.

In closing, the CBA appreciates the opportunity to contribute to the committee's study. Canada's banks know first-hand the financial and emotional toll that fraud takes on their clients. Banks invest heavily in fraud prevention, cybersecurity training and client awareness, but no single organization or sector can successfully stem this tide. If we work together across government and sectors collaboratively to solve this threat, together we can protect Canadians, Canadian businesses and the economy.

● (1110)

We look forward to your questions.

The Chair: Thank you very much, Mr. Ostler. I appreciate that. You clearly timed that out, as you were right on the dot.

Mr. Smith, I'll turn the floor to you.

Eric Smith (Senior Vice-President, Canadian Telecommunications Association): I'll try to come in five seconds under that.

Thank you, Mr. Chair and members of the committee, for the opportunity to appear before you today on behalf of the Canadian Telecommunications Association.

Our association is dedicated to building a better future for Canadians through connectivity. Our members include telecommunications service providers, equipment manufacturers and other organizations that invest in, build, maintain and operate Canada's world-class telecommunications networks.

Fraud is a serious issue. It causes financial harm, undermines confidence in digital services and affects Canadians in every region of this country. The telecommunications industry takes this challenge seriously. Our members invest significant resources in fraud prevention and work continually to identify emerging threats, strengthen network protections, support law enforcement investigations and help educate Canadians about scams.

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

At the same time, it's important to recognize that fraud is an ecosystem-wide challenge. Telecommunications networks are often the pathway through which fraudulent communications travel, but they are typically not where the scams originate, where the fraudulent content is created or where financial losses ultimately occur. Today's fraudsters frequently use digital platforms to originate, optimize, amplify and execute scams or use over-the-top messaging applications to communicate with their intended victims. While telecommunications networks are used to deliver these communications, telecoms service providers generally do not see the content of these communications.

To use a common analogy, while telecoms providers deliver the envelope, they do not read the mail.

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

Some of the previously mentioned measures taken by our sector to combat fraud were possible only after careful scrutiny by the CRTC, and only after the commission was satisfied that such measures would be effective, were in the public interest and would not negatively impact the delivery of legitimate traffic.

As the government develops its national anti-fraud strategy, we think it should focus on the following four priorities.

First, strengthen coordination and information sharing across sectors. Fraud prevention is most effective when telecommunications providers, financial institutions, digital platforms, government agencies and law enforcement work together and share information.

Second, strengthen international co-operation. Many, if not most, fraud operations originate outside Canada's borders, making cross-border collaboration essential.

Third, expand public awareness and education. Most fraud ultimately relies on social engineering. Helping Canadians recognize scams remains one of the most effective tools available.

Fourth, ensure that any new anti-fraud measures under consideration complement existing regulatory frameworks and avoid unnecessary duplication. Building on existing authorities, expertise and industry-led initiatives will help ensure that resources are directed toward preventing fraud rather than navigating overlapping compliance obligations.

In closing, the telecommunications industry is committed to being part of the solution. Our members will continue investing in network protections, collaborating with partners across sectors and supporting efforts to protect Canadians from fraud. We look forward to working with the government, regulators, law enforcement and other stakeholders to develop a national anti-fraud strategy that is practical and effective and reflects the shared responsibility required to address this evolving threat.

Thank you. I'd be pleased to answer your questions.

● (1115)

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

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

Carey Frey (Chief Security Officer, Telus): Chair and members of the committee, thank you for the opportunity to appear before you today.

My name is Carey Frey, and I serve as the chief security officer at Telus.

With over 21 million telecoms connections, we take seriously our responsibility not only to connect Canadians but to protect them.

I want to begin with a simple statement of fact. Fraud is now a central feature of our economy. It is highly organized, international in scope and growing at a rate that no individual sector or government can contain on its own.

While Telus fights fraud daily, I want to offer a story that illustrates the type of fraud Canada is contending with today and say that the only model to fight it with is collaboration between industry, law enforcement and government.

Last November, Telus received a tip about a suspicious text message hitting phones in Toronto. These messages had links designed to impersonate legitimate payment websites. We launched an investigation and found nothing. There was no record of these messages anywhere in our network logs. That absence itself was a clue. We suspected we were dealing with an SMS blaster, which is a piece of complex telecommunications equipment that mimics a legitimate cell tower and floods nearby phones with fraudulent text messages. It's a portable cyber-threat used by criminals to cause chaos and defraud unsuspecting victims. We had never seen an SMS blaster deployed in Canada before.

Eventually, it became clear that someone was driving this device around Toronto, moving through communities and targeting thousands of phones at a time. Industry reached out to Toronto police to report the text messages and also reported the unauthorized airwave use to the Department of Innovation, Science and Economic Development, or ISED. These reports kicked off a five-month investigation called Project Lighthouse.

Thanks to the information-sharing efforts between industry and law enforcement, three individuals were arrested and now face 44 charges. In total, these individuals are responsible for more than 13 million network disruptions.

While the criminals' primary objective was to commit fraud, their technology also doubles as a new and destructive type of pre-positioned cyber-threat. These devices can disrupt 911 calls, cause network outages and be used to launch cyber-attacks against critical infrastructure from inside Canada's borders. They can even be used to install malicious software on nearby smartphones. These new tools of international fraud create threats to Canadians beyond financial losses. We must locate and disable these technologies rather than merely shield our citizens from their criminal application.

Project Lighthouse succeeded not because of a new law but through sustained collaboration across major financial institutions, Canada's telecoms, three police forces and several federal agencies. We prevailed because we established trust, information sharing and the willingness to act among all partners. This is the model Canada that should pursue.

Canada already has much of what it needs to fight fraud more effectively. The Canadian anti-fraud centre, sector regulators, law enforcement agencies and the private sector coalitions are there. What is missing is a central coordinating force that ensures that the best tools and intelligence reach the people who need them. That is a role only the federal government can play, and it should establish itself in that role before reaching for new powers.

Project Lighthouse taught us four lessons that Parliament can implement to combat fraud.

First, we need to strengthen co-operation across industry and government as well as globally to disrupt fraud rings that abuse our digital platforms. Trying to block individual frauds becomes an endless and futile game of whack-a-mole against international crime. Most digital fraud against Canadians operates abroad, making strong international collaboration essential to stop it. Within Canada, the federal government is best positioned to lead fraud prevention, disruption and response efforts across the public and private sectors.

Second, telecommunications companies could block more fraudulent traffic on our networks, but today liability risk constrains what we can do. Safe harbour laws protecting good-faith anti-fraud actions would help protect Canadians at no additional cost to taxpayers.

Third, provide law enforcement with the explicit mandate and necessary resources to effectively apprehend fraud perpetrators and dismantle their technical apparatus.

Fourth and finally, Parliament should look at existing policies and how they unintentionally assist fraud. For instance, the CRTC's customer confidentiality regulations restrict cross-industry information-sharing. Another example is the CRTC's device unlocking rules, which currently make it easier for criminals to defraud Canadians of their smartphones, leaving them with significant debt and damaged credit scores.

● (1120)

To conclude, Telus sees ongoing fraud against our customers—and, frankly, against all Canadians—every day. It is growing, but it is beatable if we act with coordination and urgency. Telus is ready to be a partner in that effort.

I look forward to your questions. Thank you.

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

We'll go into our first line of questioning.

Madam Dancho, the floor is yours for six minutes.

Raquel Dancho (Kildonan—St. Paul, CPC): Thank you, Mr. Chair.

It's an honour to start this important study. I know that every corner of the country has been impacted by frauds and scams. Members of Parliament came together on this committee quite collaboratively to pursue recommendations to government so that we can safeguard Canadians, their finances and, as outlined in testimony, their safety as well in their access to 911 and other resources.

Thank you to the witnesses for being here. Your testimony is very important to us. I have a number of questions for each of you, but I first want to outline part of the inspiration for pursuing this study from my end.

At my constituency office, we received a call about a year ago. It said “RBC online banking”. My assistant answered the phone. It seemed very legitimate, but there was something that didn't sit quite right with her. She wasn't sure, so she hung up and called me. We decided to call RBC directly and just see. Sure enough, it was a scam. My assistant is young and with it. We often say that if you don't have that, it provides more vulnerability, but she said it would have been extremely easy for her to have given over the information. They were very convincing. How are people supposed to defend against this?

I want to turn it over to you, Mr. Frey. Can you explain how that could have happened in my office and in the homes of other Canadians? The bank was the name on the call, but obviously fraudulently. How does that happen, and how can that be prevented?

Carey Frey: The unfortunate reality is that telephone calls and SMS messages can be impersonated. That is due to limitations in the security of the telecommunications infrastructure that was developed decades and decades ago and that we still rely on, at its very fundamental layers, all around the world.

Our industry has developed many new, secure protocols to prevent impersonation. However, every country in the world has to adopt those. Countries that don't adopt them provide a safe haven for criminals to route calls and SMS messages from those jurisdictions, which we then have to process into Canadian networks. We block the vast majority of those—probably over 99% of scam and impersonation telephone calls and SMS messages—yet some are still able to get through at a significant enough volume that it sustains an industry for scams.

Raquel Dancho: Thank you very much. You're saying that part of the problem is not necessarily something that's within your control as Telus. You're not restrained based on legislation. You alluded to some legislative constraints, but for that specific issue, there's not a legislative change or something that you can do domestically to stop that. You are doing a lot, but you're saying that because these calls are coming internationally and routed through your network, that creates some issues. Is that right?

Carey Frey: Yes. That's correct.

Raquel Dancho: Okay.

Is there any recommendation you can provide to us that would support you in preventing that?

Carey Frey: I don't see a recommendation to prevent that. It is a reality of the telecommunications infrastructure globally. Options we could look at are communicating in different ways or, as I mentioned in my testimony, revisiting greater international collaboration on this question and seeking to upgrade networks in other countries around the world and have them shut down older versions of telecommunications infrastructure, which is the vulnerability that is sustaining much of this activity.

Raquel Dancho: Do you see artificial intelligence playing a role, both in the increase of the threat and also combatting it? Would that help in this scenario or others similar?

Carey Frey: It would, yes. My concern overall is that the example you cited, which is one I'm certainly familiar with, is in a small minority of what is causing fraud at a large scale if we look at the total financial losses in the country. While that would be an important aspect to continue to focus on, there are many other examples of abuse of our digital platforms, not just telecommunications infrastructure but also hyperscaler cloud platforms and the applications on our mobile phones that fraudsters are also using to perpetrate these scams.

It is a fact that even if we take away the vulnerable portions of our global telecommunications infrastructure, they will simply pivot their activities 100% onto the digital platforms. We have to be very mindful of being holistic in our strategy.

● (1125)

Raquel Dancho: To the credit of the telecommunications platforms, I have noticed, and maybe others have as well, that in the last year it will show that a call is incoming but will say, “blocking: likely scam”, or something like that. I had not seen that before, but it's quite frequent now. It's much appreciated, but as you said, it seems that some are still sneaking through.

Mr. Smith, did you have anything to add to this conversation about prevention or legislative change or anything that you think we can do?

Eric Smith: No, I think I'll just add to what Mr. Frey said. Some of the tools that telecommunications providers in Canada and elsewhere in the world have adopted have been to target those types of things. In fact, with the CRTC, they implemented the STIR/SHAKEN technology, which helps verify the identity of callers but doesn't verify the purpose of the call. However, as was mentioned, if that technology is not adopted in the jurisdiction where a call has originated, for example, it doesn't provide that function.

There are also other programs that carriers have brought in, like do-not-originate programs. For example, if a bank has 1-800 numbers that they do not use for outbound calls—they're just for people to call into customer service—they can register that with telecoms, so that if a call purports to be coming from that number, it is automatically blocked.

There are different things that companies are doing, but as noted, once you close one loophole, fraudsters go to other things. What we're seeing a lot is on social media platforms, digital platforms and those types of things.

Raquel Dancho: Thank you very much.

The Chair: Madam O'Rourke, the floor is yours for six minutes.

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

In 2024, the Canadian Bankers Association, major banks, telecoms, technology firms, law enforcement and the Government of Canada formed the Canadian anti-scam coalition to support a coordinated response to scams.

I'm wondering, Mr. Ostler, what concrete results the Canadian anti-scam coalition has achieved to date. How are those results being measured? How will it work with the new financial crimes agency that the government has announced?

Anthony Ostler: There are multiple elements to the progress of the coalition. A key thing to note is that the coalition is voluntary. Probably one of our biggest accomplishments was the launch of our education awareness campaign in fall 2025, called Stand Against Scams. The call to action for Stand Against Scams is “Stop. Check. Talk.”

That is to try to help Canadians get greater skills to better protect themselves. The reality is, if you talk about one type of scam vector or style of scam, the bad actors, as these guys have been saying, will change their route of doing it, so we're trying to help Canadians get better skills.

Additionally, we have developed a taxonomy of information sharing so that we can see what telecoms, banks, digital platforms and law enforcement would need, and so that we can have one version of the truth when and if we set up an information-sharing exchange on a formalized basis.

Finally, we've had a great partnership with the telecommunications industry from the point of view of doing a pilot. One of the large telecoms and a couple of my members are doing a pilot on information sharing, where they've identified meta-information around bad actors doing scams. What's interesting about that is they may find, let's say, a phone number that's been used fraudulently in a telecom, and then discover it's been used with a fake identity at a bank. Then they've been able to figure out that, okay, that person must be using that as a mule account. Then we can pause the account and that kind of stuff.

That pilot has been really quite interesting. We're leveraging the backbone of the telecom industry to facilitate securely sharing that information. It's not a sustainable solution. It's not automated. However, when the pilot participants compare the information, the networking effect of having multiple parties is quite significant. We're hoping to build upon that now that we have the taxonomy, and to move forward on information exchange on a more formal basis.

I think a critical element will then also be adding in the digital platforms from an information-exchanging perspective. The digital platforms have been members of the coalition since the beginning and have been key contributors to education awareness, including programs like Meta is doing now with the World Cup to try to stop people from being scammed. A special part of our campaign is around that.

We've really welcomed that investment from all sectors in the education awareness campaign, but I'd say there's more to do. That's why the opportunity to be at this committee and participate in this study is welcome.

Australia has reduced scams by 30% over the last three years. Our reported scam volumes have increased 32%. Since 2022, we're up 32%; they're down 30%. They're the only country that, over the last three years, has reduced scams. They've done that through a cross-sector program that is government-led. That has brought not just the sectors together, but also law enforcement and justice, through Crown attorneys and that sort of thing. There's a whole coordinated, integrated approach. That's done an amazing job of protecting Australian citizens. We'd like to do the same in Canada.

● (1130)

Dominique O'Rourke: That's fantastic.

I'm mindful of the time. I have two things in terms of your perspective on the new financial crimes agency that has been announced by the Minister of Finance.

In the spring economic statement, the government said that we are going to ban crypto ATMs because they're frequently used in scams. We should tell people, “Do not buy gift cards for scammers. Do not go to a crypto ATM. The government is not going to ask you for these things. Your bank is not going to ask you for these things.”

I'm wondering whether you support that move to ban those crypto ATMs that are in a lot of corner stores.

Anthony Ostler: Very much so. If you think about financial crimes, scams and fraud are a subset of financial crime. The financial crime is connected to cybercrime. It's connected to money laundering. Of the people who are perpetrating these scams and fraud, 60% to 70% are outside the country. They need to get the money out. They're laundering the money. One of the easiest ways to do that is through crypto channels.

Most of the use cases for crypto are for financial crime of some form or other. That's why we need a financial crimes agency. Other large countries have them, such as Italy, the U.S. and the U.K. What we need is an agency that can coordinate with those agencies, if we think about the risks that are involved here. That would better enable us to disrupt these bad actors. We may not be able to take to jail the ones who are overseas, but if we can coordinate across countries and stop them from victimizing our citizens and businesses, then we're better able to protect them.

Dominique O'Rourke: Thank you.

Mr. Chair, do I have a minute? MP Begum would take it.

The Chair: I'll give it to you on the back end.

Ms. Begum, you can tag on to Mr. Ntumba for a few seconds when we get to the next round.

[*Translation*]

Mr. Ste-Marie, the floor is yours for six minutes.

Gabriel Ste-Marie (Joliette—Manawan, BQ): Thank you, Mr. Chair. It's a pleasure to see you again at committee. I can tell you that Ms. Dancho did an outstanding job as chair. I'd also like to thank her for proposing this important study.

I'd also like to thank the four witnesses for being here. They have provided us with a great deal of information in their responses and, of course, in their opening remarks.

First I'll address Mr. Ostler and Mr. Elcock, from the Canadian Bankers' Association. I would, however, like to thank Mr. Smith for his recommendations, particularly the fourth one, which relates to Bill C-29, on which debate is due to begin shortly in the House of Commons and continue in committee thereafter. I therefore thank him for his recommendations.

Mr. Ostler, I'd like to discuss two types of fraud that have been widely reported in the media and are seen internationally, but which have devastating effects in Canada.

First, I'd like to invite the Canadian Bankers Association representatives to provide the committee, if possible, with further information on the pilot project they referred to, as it's very interesting, as well as on the measures taken by Australia, the broad outlines of which they have shared with us. We could draw inspiration from this and perhaps succeed in producing a better committee report.

Let me give you an example of the first type of fraud we've seen on public affairs programs. A young pensioner with a pension fund goes on social media and stumbles across a deepfake video in which the Prime Minister or Elon Musk is seen spouting falsehoods and encouraging people to invest in cryptocurrencies by providing a link to click on. The young pensioner clicks the link and invests $20. He's then told that his investment has paid off and tripled in value, so he withdraws his money: $60. Thinking it must work, he does it again, this time investing $1,000 and subsequently receiving $3,000. He ends up investing his entire pension fund—say, $500,000 or $1 million—and, just like that, all his money is sent abroad, and he never sees it again.

I can't wait for representatives from social media platforms to appear before the committee so we can question them on this matter. It makes no sense that circulating fake videos like this is permitted.

What can banks and financial institutions do once the money has left the country? We've talked about coordination, but it seems that's no longer the case. Is there any way, based on the laws and regulations currently in place, to do more when we see that $500,000 is being sent abroad and we suspect a problematic situation, or even fraud?

As for FINTRAC, the Financial Transactions and Reports Analysis Centre of Canada, it doesn't appear to have any powers. It receives information, produces reports and is overwhelmed.

So, what can be done under current rules and laws? What can you, as bankers, do to stop this phenomenon and prevent criminals from stealing people's life savings?

● (1135)

Anthony Ostler: Thank you very much.

[*English*]

For sure, we will provide you with information on the pilot and on Australia. We've already provided some stuff on Australia to the committee, and we've encouraged the Australian Bankers Association and the experts who do their information exchange to be witnesses. Hopefully that will be arranged for the committee, but we will help facilitate that follow-up.

Regarding the deepfakes, that is a very challenging situation. One thing our members do is constantly scan the web, be it social media or wherever, looking for deepfakes that may have their representatives in them, be it the CEO or well-known financial pundits. When they identify those, they notify the appropriate platform to have them taken down, because they don't want that contributing to the noise or lending credibility to fake investment things.

Also, it's not just fake crypto investments, but the crypto one is common, unfortunately.

What's interesting is that scammers play on emotions. They're playing on fear, greed, lust and loneliness. Unfortunately for consumers, if someone's playing on your emotions, often your critical thinking skills get pushed away. If it's fear, maybe you're worried about a grandchild or something. If it's loneliness, maybe it's about a friend. Maybe it's greed, and you need more money. Those dimensions then have people push through.

Our members have lots of programs. If someone is trying to send a large amount of money externally, they ask them what the purpose is. If they're taking money out, it's a common local scam, or at least local people are involved—it's not international players—to try to convince people to take money out of their bank and give them cash because there's a security risk or something. In those instances, if they don't normally take out large amounts of cash, the tellers have been trained to ask individuals about what's going on.

In regard to what we can further do, obviously a key part of it is building the ability to share information and learn the patterns. If something is happening in Trois-Rivières or in Thunder Bay, where we can connect the dots, be it with our telecom or digital platform partners, we work with law enforcement to cut those things off.

In regard to FINTRAC, our members spend billions annually on compliance and on fighting financial crime. Our system is not effective, because we're focused more on compliance instead of on risk, so there's a real opportunity to reform our AML regime. If you want more detail, Hartland, who's here with me, is our expert on financial crime.

Hartland Elcock (Assistant General Counsel and Vice-President, Canadian Bankers Association): That's an excellent question. I appreciate it.

First, we need to contextualize FINTRAC's role. They're an intelligence agency rather than an enforcement agency. Our members are the largest reporters to FINTRAC of suspicious transactions, which is where an institution has seen suspicious activity that leads to reasonable grounds to suspect money laundering, and it sends that information to FINTRAC.

Again, it's money laundering, terrorist financing and sanctions evasion. It's not the predicate offences of fraud; it's the treatment of the money after those initial incidents, and what FINTRAC does is package that information to send it on to law enforcement.

I think the FCA is a critical ingredient here. You can have a lot of reporting, as we do currently. In fact, I think the Cullen commission has noted that we have magnitudes more reporting than other jurisdictions, but we're not seeing the results in terms of investigations and prosecutions.

What the FCA can do is offer what all my colleagues have mentioned, which is coordinated, integrated investigations of complex financial crimes to yield results for Canadians, to protect them and to take the information and translate it into real results.

That doesn't mean that the AML regime itself doesn't need improvement along the lines of what you're referring to. As Anthony, our president, mentioned, focusing on risk is critical. We have a lot of reporting into FINTRAC. That's a lot of noise in the system.

What we think is critical is that we see a reform of the AML regime overall. We need a modernization of our AML laws to look at the type of reporting that's going into FINTRAC to ensure that it's targeted at risk and the priority risks of the government. Then law enforcement is getting exactly the information it needs. There's not a deluge of information. It's really targeted at bad actors.

We can do that through changes to legislation. We can do that through changes to information-sharing powers. Currently, we have private-to-private information sharing. That's currently being stood up. We're looking for some additional changes around public-to-private information sharing, so that law enforcement can share key pre-production indicators with banks to help guide efforts to detect and then mitigate money laundering.

Finally, we also need to look at how we enforce the regime. Do we need to consider sector-specific regulation? FINTRAC has 39,000 reporting entities. That is a big job, and I think it's important that the right regulators are looking at the right industries.

We've mentioned other sectors, like MSBs. It's important that in areas where there's high risk, supervisory resources are dedicated to those areas of high risk so that we have compliance. Our members are highly compliant. Our members are also prudentially regulated, so there are several lines of defence, but it's important that we have comprehensive regulation across the board.

Again, I'll close with the financial crimes agency itself. I think that everything that's being tabled is very promising in its structure, in its mandate and in its powers. We also hope that as time goes on it evolves into a coordinating agency—something that can set national priorities. It's hard to focus on risk if you don't have the priorities, and we hope the financial crimes agency can play that role.

● (1140)

[*Translation*]

Gabriel Ste-Marie: Thank you very much.

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you.

Mr. Falk, the floor is yours, sir.

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

Thank you to our witnesses for your testimony here this morning.

Mr. Ostler, I'd like to begin with you.

I want to carry on a bit further on the FINTRAC compliance and the regulations that you're subjected to as banks in Canada. Are they asking for the right kind of compliance?

I know the burden is significant. I fully understand and have experience with that.

Are they effective in what they're asking you to do?

Anthony Ostler: It's a great question. Thank you.

Do you understand the concept of diminishing returns?

Ted Falk: Yes.

Anthony Ostler: FINTRAC's suspicious transaction reporting has 400 fields. The equivalent report in Australia—which we've seen is effective at fighting financial crime—is 30 to 50 fields. After 30 fields, there are diminishing returns.

If we want to move quickly and look at risk, I think there's a significant opportunity—as an example—to reform the reporting process and put more focus on action.

Ted Falk: Do you think that all of the FINTRAC regulations and compliance issues should undergo a significant reform?

Anthony Ostler: Certainly.

Ted Falk: I don't disagree with you. That's good.

You also indicated that, in a lot of other jurisdictions, scamming and crime have gone down by about 30%, but here in Canada—

Anthony Ostler: That's Australia.

Ted Falk: That's specifically Australia.

Anthony Ostler: It's Australia, and it's 30% in the last three years.

Ted Falk: Ours is up 32% since 2022.

Anthony Ostler: That's correct.

Ted Falk: Why is that?

Anthony Ostler: It's gone up everywhere outside of Australia over those three years.

What's been happening is that the bad actors have been getting more sophisticated. Their AI is more powerful; their tools are more powerful. They've developed international teams—tiger teams and virtual teams—that come together. They have people who are experts at digging into the dark web and people who are experts at psychological profiling. They'll develop a playbook that may be working in Australia. If it gets cut off in Australia, then they do it in Canada. It's that sort of thing.

These bad actors—

Ted Falk: It's kind of like electricity. You go where there's the least resistance.

Anthony Ostler: Exactly. You go where the least resistance is.

Ted Falk: My question is also this: Once these bad actors are identified and you actually get to the bottom of an incident or an entire scam, are you finding that the prosecution is effective?

Anthony Ostler: I was at the UN's Global Fraud Summit. They mentioned that 60% to 70% of the sources of scams and frauds are international.

It depends on the home country. This is what our telecoms peers are seeing as well. If you have countries that aren't upgrading their telecoms systems or don't have a good rule of law, they can become a backdoor or the conduit for a lot of issues.

Ted Falk: When some of your member organizations, some of the banks that you represent, have experienced fraud and they've caught the bad guys, are they reporting to you that the penalties are significant or appropriate?

● (1145)

Anthony Ostler: On the bad guys, we've just not seen.... For instance, on anti-money laundering, we've just not seen a lot of convictions. On scams, the statistics I've seen on fraud are that only 5% to 10% of people report their scams. A small portion of those, I think it's 0.1% or 0.2%.... It's a rounding error on actual conviction.

On scams themselves and money laundering reporting.... There are not a lot of convictions happening in Canada when it comes to financial crime.

Ted Falk: The risk-reward ratio is actually in their favour.

Anthony Ostler: Yes, very much so.

I think part of this is why we want to move upstream and have that cross-sector public-private partnership. If we can put a higher wall around Canada and stop these bad actors coming in via multiple channels, we can better protect and reduce the risk of our citizens being fooled by these people.

Ted Falk: I have one more question for you before I move to Mr. Frey.

What level of responsibility or onus should the banks take in these types of situations where there are scams?

Anthony Ostler: We're highly regulated, potentially. We have a code of conduct.

If the consumer is truly a victim, from the point of view that they've not given out any information or sent stuff out and they've been defrauded, then our members obviously look after them. Unfortunately, a lot of people voluntarily send the money. The banks ask when they're sending it, are you sure? What are you doing?

Ted Falk: I appreciate when I get those texts that ask, is this actually you buying this?

Anthony Ostler: Right. We do a lot to try to help our clients. What we've realized is that we want to move upstream to try to stop them from being fooled in the first place.

Ted Falk: Mr. Frey, I've run out of time. I'm sorry.

The Chair: Colleagues, we're going to have bells at 12 o'clock for votes if everything goes according to plan. I need unanimous consent to work through bells. I'd like to establish that first. If I don't have it, we're going to have to stop. If I do have it and folks are willing to vote virtually, then we can keep going.

Can everyone please very clearly indicate whether they're okay with this?

Go ahead, Mr. Ma.

Michael Ma (Markham—Unionville, Lib.): I support that, but we need to pause for a few minutes to do the vote.

The Chair: Yes, it's to vote, but I need unanimous consent to work through the bells themselves. The vote wouldn't occur until about 12:30, so we would be okay.

Do I have unanimous consent to work through them?

I do. Okay. In that case, I'm going to be a little more lenient. We went substantially over with Monsieur Ste-Marie. It seems to be a pattern. I myself have a few questions, and since it's our first meeting, maybe I'll be a bit more lenient.

Ted Falk: The other chair was tough.

The Chair: Mr. Falk, she was tough, yes.

Be very quick with Mr. Frey, and then I'm going to get a couple of questions in as well. We'll just keep going, and when we hear the bells at 12:00, that doesn't mean it's the start of the vote. It just means it's the warning period.

Mr. Falk, I'm going to give you about 45 seconds.

Ted Falk: That'll be great. Thank you very much, Mr. Chair.

Mr. Frey, you indicated that three of those fraudsters doing the SMS blaster were charged with 44 different counts. What level of...? What was the punishment? Are you satisfied with what the Crown is asking for?

Carey Frey: Yes, but certainly they stacked a number of charges in this case, in many different categories. I think one possible interpretation of that is that the individual crimes in and of themselves were probably minor, but 44 crimes in aggregate may result in a much longer sentence.

It's before the courts, so we'll have to see what the outcome is.

Ted Falk: Thanks.

The Chair: Thank you, Mr. Falk.

[*Translation*]

Mr. Ntumba, you have the floor for five minutes but, as I said, I'll give Ms. Begum a few seconds to ask a question. I'm giving everyone here a bit more time.

So, Mr. Ntumba, you have the floor for five minutes, then on to Ms. Begum for 45 seconds.

Bienvenu-Olivier Ntumba (Mont-Saint-Bruno—L'Acadie, Lib.): Thank you, Mr. Chair. No worries.

My question is for Mr. Ostler or Mr. Frey, whoever wants to answer.

Artificial intelligence now enables fraudsters to create increasingly convincing scams. Is Canada sufficiently prepared for this new generation of fraudsters? What measures should be prioritized over the next three years?

[*English*]

Anthony Ostler: Unfortunately, as we've seen by the statistics, Canada is not fully prepared. Because we've had our voluntary anti-scam coalition in place for a couple years, we're probably ahead of many or most countries from the point of view of better understanding the risks, but like every country except Australia, we don't actually have a comprehensive, cross-sector, public-private initiative in place.

I think we could get there fairly rapidly. The government does have a national anti-fraud strategy. It is creating the financial crimes agency. It has an opportunity for AML regime reform. I could picture us being in a position to actually bend the curve on this and reduce scams and fraud within a couple of years.

Once Australia figured out how to do it, they very quickly had results. We're on the cusp of getting there, but a key part of that is thinking about how we work across aligning clear definitions with a cross-sector framework, so that all the different players know the roles they need to play and we have controls for the various sectors.

As our colleagues have mentioned here, each sector has its own regulators, but we need some sort of overlay to make sure there's coordination. As part of making it effective, we need improved fraud data sharing, oversight of that and public education.

We've done a lot on the public education front—

● (1150)

[*Translation*]

Bienvenu-Olivier Ntumba: Actually, your comment on the exchange of fraud-related data pretty much answers my next question. I was going to ask you whether banks have the necessary tools to quickly share information about fraudsters with their financial partners, as well as with other security organizations, governments and law enforcement agencies.

Please provide a brief response so Mr. Frey can also answer.

[*English*]

Anthony Ostler: That's a good question.

We have the legal framework to share information. We have information, but we do not have a tool to exchange that information quickly. We do have our pilot under way that we're doing between a couple of our members in telecoms. That is working, and quickly, to the entity that's holding the information securely, but then the actual analysis is slow, because it's not automated.

We're not there yet, but now that we have a taxonomy that's designed that would work across, the next step would be developing an information exchange, and that taxonomy was designed so that it would work for government.

[*Translation*]

Bienvenu-Olivier Ntumba: Mr. Frey, if you had to recommend just one measure to the federal government to minimize fraud or attempted fraud in Canada, what would it be? Why would it be important?

[*English*]

Carey Frey: As I mentioned in my testimony, we need a convening power, not a committee—not attempting to address fraud holistically by committee, but a single place where an organization can take the accountability for understanding how fraud is happening and lead the strategies and campaigns that all of us can participate in to tackle whatever the solution is to rid ourselves of the particular scam or fraud ring that's perpetrating these crimes against Canadians.

[*Translation*]

Bienvenu-Olivier Ntumba: Do you think citizens are sufficiently equipped to deal with types of fraud that rely on new technology?

Although we all have access to the information, there are three groups of people: young people, middle-aged people and older adults. What are your thoughts on how perceptions of information vary across these different age groups?

[*English*]

Carey Frey: I believe that we need much more awareness and focus for Canadians on the types of new frauds and scams that are occurring. I would answer personally that I used to feel I could keep up with it. I've been a security professional for three decades, and I'm at the point where I can no longer keep up with it for my own personal considerations.

Extrapolating that across all of our society, no, I don't believe that we're prepared, and we need a much greater focus and concentration on this, because, to my colleague's point, awareness about these scams and measures that we can take to not become victim to them is paramount.

[*Translation*]

The Chair: Thank you, Mr. Ntumba.

Ms. Begum said she didn't need speaking time, so the floor is yours, Mr. Ste-Marie.

Gabriel Ste-Marie: In that case, I'd like to thank Ms. Begum for letting me use the speaking time allotted to her; but no, that's a joke.

I'm going to ask the representatives of the Canadian Bankers Association another question. That said, since I might run out of time to hear your answers—if you have any, Mr. Smith and Mr. Frey—please feel free to submit them to us in writing.

I'd like to address the issue of data breaches in all kinds of companies, whether financial institutions or others. Even Canada's telecommunications giants have experienced such incidents. These breaches lead to identity theft; fraudsters take out mortgages or loans in the names of the people whose identities they've stolen.

What can be done to put a stop to this? Everyone's data is circulating everywhere—for example, on the dark web. Canadians' data is out there. What can be done to prevent this from happening again?

Furthermore, should there be a time limit once a company knows that a data breach has occurred? Should it immediately report that a data breach has taken place? This information isn't always disclosed.

● (1155)

[*English*]

Hartland Elcock: That was an excellent question. Thank you so much.

I would look to PIPEDA and the breach reporting obligations under PIPEDA. Those are already in place, and they require, when a leak occurs, that communication happen with impacted individuals. It also outlines various other steps that need to be taken and ameliorative efforts to address potential harm that may flow from that.

As Anthony outlined earlier, it's also key to think of those online commitments when there is a breach. It's not authorized fraud or any other form of technical breach, which would be very rare. There are commitments to making customers whole as well.

I think the legal framework under privacy law is already expansive enough to address the sort of situation you're outlining. It doesn't require a specific time period, but it does require a defined time period.

[*Translation*]

Gabriel Ste-Marie: Thank you.

I have 30 seconds left. Mr. Smith or Mr. Frey, would you like to add anything?

[*English*]

Carey Frey: If I could comment, I would add that our standards for identity authentication are not uniform across the country. It's on a voluntary basis that organizations choose to do things like notify customers that they need to change their password, as an example. The solution to this is to have standards applied uniformly in this area by someone with the appropriate expertise to determine what that should be and the power to bring it into force across the country, so there is no competitive differentiation on this question in the future.

[*Translation*]

Gabriel Ste-Marie: Thank you.

Mr. Smith, you can submit your comments in writing to the committee, as my time is up.

Thank you.

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

[*English*]

Madam Dancho, the floor is yours for five minutes.

Raquel Dancho: Mr. Ostler, I'd like to build upon a few of the questions of our previous colleagues.

You've outlined this, and others have, too. Australia has been the only jurisdiction in the world to see a decrease in these frauds and scams. I believe the data shows just under a 30% reduction since 2022, which was outlined by you and others today. Everywhere else has seen an increase. It really amounts to nearly $1 billion of savings. It was just over $3 billion in losses in 2022, which decreased down to $2.18 billion in 2025. That's material savings for Australians in this regard.

We've heard you and others say that the primary issue is international. What to do about that is challenging. Yes, more international collaboration...yet Australia has found a way to deal with that. Can you outline in just a bit more detail what exactly it has done that we're failing to do?

Anthony Ostler: A key part of what it did was put in codes of conduct for the various cross sectors involved—digital platforms, telecoms and banks—and made clear the roles that it expected of those sectors. For instance, for digital platforms, if a fraudulent ad or website was identified, takedown or blocking by the digital platforms was required.

When a bank or an investment adviser does an advertisement on social media in Australia, they have to verify that the advertiser of financial services is actually a registered individual or regulated entity to be an advertiser. There's a verification or a "know your advertiser" requirement. That has a big impact if you think about fake AI ads. We had an example earlier about people being convinced to invest in crypto by a public official or persona of some sort that's being leveraged in AI. That would be taken down more quickly and/or the advertisement wouldn't be allowed to be put up.

Those elements of knowing your advertiser, verification, takedowns and blocking of sites are critical elements. If you think about moving to the root cause of how people are scammed or fooled, it's taking it down more quickly. That has been one of the biggest contributors to reducing scams or fraud.

As my colleagues here from the telecommunications sector have indicated, there are back doors into the system. There are ways to make sure that if you're a financial institution calling a customer, your logo could appear. You can't push through an SMS system. That would be a proper through-the-system thing. That's an example of something whereby consumers could see that if it's not showing the logo of the bank that they bank with, it may not be a real bank calling. Those are examples.

● (1200)

Raquel Dancho: I appreciate that very much.

I don't wish to name and shame any one country that's harbouring bad actors. We don't know the resources or the challenges that country may have, but I think it is important to include that data in the committee study. Can you just outline a few of the countries where some of these issues are coming from?

Anthony Ostler: Myanmar is a very large contributor to issues. We also have nation-states like Iran contributing to scams and fraud. Those are examples of countries that are problematic.

Raquel Dancho: Thank you for your testimony.

Mr. Chair, there is a pertinent and concerning issue that arose in Canada that the industry committee has discussed at length previously. I would like to put the following motion on notice:

> That the committee report to the House that it condemns the use of forced labour in supply chains, especially in China; rejects unjustified American tariffs that threaten Canadian workers and industries; and calls on the Liberal government to strengthen and reinforce Canada's existing ban on forced-labour imports and take more effective action to stop goods made with forced labour from entering Canada.

Mr. Chair, we have discussed this at length. I think it could be pertinent that we have unanimous consent to just adopt this today. I'm asking for that.

Thank you.

The Chair: Okay. Just to be clear here, Madam Dancho, are you moving this motion, or are you putting this motion on notice?

Raquel Dancho: I'm putting it on notice, but given that we've already talked about it at length, I'd also like to ask for unanimous consent that we adopt it today.

[*Translation*]

Gabriel Ste-Marie: I have a point of order, Mr. Chair.

The Chair: Mr. Ste-Marie, you have the floor.

Gabriel Ste-Marie: I'd like us to have the motion in writing before we vote.

Raquel Dancho: Yes, of course.

The Chair: That's exactly what I was going to say.

[*English*]

It's for that reason, Madam Dancho, that it's not quite as simple as asking for unanimous consent. I need to know whether you're moving this motion or not.

If you move this motion, you're entering us into debate on the motion, although I have to see it. Based on what I've understood that you've read out, I'm not sure that it's relevant to the business in front of us. Therefore, I'm not sure that it's admissible at this time.

If you want me to analyze it and make a ruling on that, I can. If you are not insistent upon moving it at the moment, then you're certainly permitted to put it on notice, and we can move forward as such.

Raquel Dancho: Given that we've talked about it at length at previous committee meetings, I think everyone's really informed on this issue. We have a public record of that, so I'm asking for unanimous consent to adopt it.

The Chair: The issue, Madam Dancho, is not whether we've discussed it previously. It's that it's not relevant to the business at hand. You didn't give the appropriate notice. Therefore, it's not admissible.

Raquel Dancho: I'm not moving it yet, but I'm asking for UC, which I can do.

The Chair: Right, but for us to enter into a decision-making process on this would require the admissibility of the question itself.

Raquel Dancho: Not to ask for UC, no.

The Chair: Let me take a look at it, first and foremost.

Raquel Dancho: Sure. Thank you.

The Chair: In order for me to do that, I'll need to have it in both official languages.

Raquel Dancho: We have that.

The Chair: I would like to suggest, considering that there was a significant degree of collaboration to bring this fraud study forward, at your request and with collaboration on the part of members around the table, that it seems somewhat useful to me that we continue to have this conversation before we deal with this matter.

Therefore, as we have done previously when we had motions put before us unexpectedly, I would recommend that we navigate the rules a bit here, with your permission, colleagues, to conclude the final few minutes of witness testimony that we have, and then I can come back to take a look, Madam Dancho, at this question. I don't see any use in our making witnesses wait for us to get through this.

Raquel Dancho: Sure. That sounds good to me. Thank you.

The Chair: Colleagues, is there any further commentary on this matter before we conclude that and I take a look at it?

Monsieur Ntumba, go ahead.

● (1205)

[*Translation*]

Bienvenu-Olivier Ntumba: I think you've said it all. We have witnesses. In addition, the notice of motion was not tabled beforehand. So I agree with what you said.

The Chair: We'll finish the testimony first, and then we can continue this discussion.

[*English*]

Madam Dancho, I'll ask your team to work quickly, please, to get that distributed to members in both official languages. I'll take a look at it once we're done our testimony here.

Mr. Bains, the floor will be yours, sir, if you would still like it for some questions that you have. Then I am going to take a few minutes to ask a few questions, and then we'll get back to the matter that was raised a moment ago by Madam Dancho.

Mr. Bains, the floor is yours, sir.

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

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

Quite a significant amount of information has come forward, and I thank you for sharing much of that and for focusing on the risk side of things and more recommendations. Ultimately, the committee's purpose is to establish strong recommendations that we can take forward.

I'd like to focus on your thoughts about Bill C-22, which is before us in the House right now and being debated, and about lawful access. In my conversations with many of the police agencies locally here in British Columbia, and even with CSIS, they want more access, the ability to be involved in the lawful access piece and also the financial crime agency. They want to know how they can be engaged in those processes to ensure that they can tackle some of these things.

The Australian reference is extremely interesting to me. For most of it, it seems like it's a very doable change in regard to codes of conduct for banks and platforms, verification pieces. Could you share some of your thoughts on lawful access, and any recommendations you have?

Anthony Ostler: Is that directed to the CBA first?

Parm Bains: Yes, it's for the CBA first.

Anthony Ostler: Thank you very much, MP Bains. It's good to see you.

At the higher level, one of the critical things is that it's not so much the information that would be needed in Bill C-22 to help us fight scams and fraud; it's more the support and oversight of information exchange and the coordination with law enforcement, particularly if we determine that it's international bad actors that are contributing to the scams or fraud. It's a broader element.

I would defer to my telecoms peers to know if there's anything specific about Bill C-22 and frauds and scams that would be helpful from their perspective.

Parm Bains: Could we hear from Mr. Frey from Telus, please?

Carey Frey: With respect to Project Lighthouse, which I spoke about earlier, we did receive court orders from police so that we could provide the data they needed to conduct that investigation. I think that worked very well, with the exception of perhaps a timeliness component. The one observation I would make is that we need to find ways in our lawful access system to get data rapidly into the hands of the investigators who need it to carry out their work.

Parm Bains: Going on to the cyber-weapon, have you uncovered...?

The perpetrators with the SMS blaster have been caught, but you talked a lot about how fraudsters will find a way to move on and move into different areas. Have you noticed different approaches or other technologies that fraudsters are using? What potential investments or initiatives can the government take to combat them on the cybersecurity side?

Carey Frey: There are many more forms of pre-positioned destructive capability that we have detected within Canada. The arrest of this group in Toronto did not eliminate the use of SMS blasters completely. We know that there are more, and they are operating in other jurisdictions in the country.

Going back to my testimony from this morning, I would reiterate that law enforcement needs a direct mandate and more resources to support the dismantling and apprehension of the rings that are operating inside Canada and deploying this technology to conduct fraud on an industrial scale.

● (1210)

Parm Bains: I'll stay with you on this.

You talked about reforming the AML regime. Can you expand on that? Have we, as a government, spoken enough about that in any way, or is this something that you're bringing forward now?

Hartland Elcock: I think there is a significant amount of reform required for the AML regime.

It's been about 26 years since the PCMLTFA was meaningfully modernized. We haven't seen a parliamentary review for some time. I think we are slightly overdue on that.

We would like to see reform in various areas, but let's start with modernizing the legislation. We want to look at the governance of the PCMLTFA regime, and we want to look at the legislative tools that the regime has. Then we also want to look at information sharing. What's been discussed today is critical, but it's the amount of information flowing to FINTRAC that isn't necessarily leading to results.

There's a significant degree of reporting. As my colleague mentioned, there are 400 fields in Canada for an STR, versus 35 in Australia. There are a lot of ways we could pare down those fields. There are a lot of ways we could reduce the number of transactions that are reported and still yield tangible results—in fact, better results. You would create less noise in the system, and you'd be better able to use the information at hand to empower law enforcement. We want to see that sort of sector-specific supervision to ensure that areas of risk are receiving the appropriate oversight and then sharing information.

I note you mentioned Bill C-22. There are some changes in Bill C-2, which is still out there, that we would like to see from an AML perspective. Those are the public-private safe harbours. Those are the safe harbours that allow federally regulated organizations to use the information, without threat of liability, that law enforcement is providing to them, the pre-production information that allows organizations subject to the PCMLTFA to properly focus their efforts on risk.

First and foremost, I think a meaningful review of the legislation is required, but we have a lot of ideas, as I've just covered, as to the direction we could go in to really help boost results.

Parm Bains: Thank you so much.

I'll cede the rest of my time to the chair.

The Chair: Okay, Mr. Bains.

Witnesses, I have a couple of very quick questions here.

Perhaps, Mr. Ostler, you're best positioned to answer them. Madam Dancho did bring this up in relation to the Australians.

You were talking about quick takedowns. In the Canadian context, are social media platforms being co-operative when you reach out, having identified that there is a problem of some sort, and you ask for co-operation to take down a deepfake, a false advertisement or whatever it may be? Are they meeting you? Are they willing to work with you? If not, what's the reason?

Anthony Ostler: That's a great question, Chair.

When we started the Canadian anti-scam coalition, in the first year, we actually had a work stream on this specific item, because the digital platforms are part of the coalition. We worked through how we could better provide them with information so that they could take things down. That has improved co-operation, but their verification process for taking things down is lengthy. Things are not taken down as quickly as they would be in Australia.

It's hard to know what's driving that. It could be resources. It could be prioritization. The reality is that, although we've had great discussions and such, there's room for improvement.

The Chair: Do they recognize the scope of the problem, in your opinion, Mr. Ostler?

Anthony Ostler: Interestingly, at the UN's Global Fraud Summit, all the large digital platforms were signatories to the framework that I talked about. That framework talks about the shared responsibility of all players in the fraud life cycle, so they have recognized it.

Going into the forum, Meta said that they want to improve their verification process. Going into that, they had verification at 70%. If a bank verified only 70% of their customers, I think they would be shut down. Meta's objective is to move it to 90%.

I think those are good things, but there's opportunity for improvement.

The Chair: What I'm asking you, specifically, is this. When you speak to social media platforms about the depth of the issue, in your view, are they accepting responsibility for the role that they play as a vehicle for this fraud to occur?

● (1215)

Anthony Ostler: Yes.

The IBFed met with the global head of fraud and security for Meta at the UN Global Fraud Summit. They acknowledged that this is an issue, and they wanted to work with us internationally. We're having great discussions around ways to pilot and improve what we can.

I would say that 2026 has marked the most substantive progress we've had, and there's a lot more to do.

The Chair: Thank you.

I have a second question.

There was reference earlier to credit score—that a victim of a fraud or scam would have a credit score implication. I know it's not necessarily your area of expertise, but can you provide some reflection to the committee in relation to how a Canadian who has been victimized by fraud and then sees a negative repercussion on their credit score can remedy that credit score diminishment that's occurred by virtue of the fraud?

Anthony Ostler: The instance that was mentioned was when there's digital identity theft. Someone borrows with a fake ID, and then the person whose ID has been compromised is shown as being the person who borrowed; but they didn't. In those instances, when that's proven, the bank or financial institution involved would work with the credit bureau to update the person's credit bureau rating because they were a victim of identity theft.

The challenge for the victims, obviously, is that they have to work with the financial institutions and others to prove that they were a victim of identity theft. It can be a lengthy process.

Part of that reality is that fraudsters may take advantage of that avenue, so there are controls in place. The reality is that, if you're a true victim of identity theft and someone borrowed in your name, this will be expunged.

The Chair: Do you have any data, through the major banks in Canada, that would tell you what percentage of scam victims or fraud victims are seniors? Use the definition of senior as 65 and over.

Anthony Ostler: I don't have that data, but what I would say is that all Canadians are victims of scams. What tends to happen, though, is that the dollar values are different.

Often, people who are over 65 have spent a lifetime saving so that they are able to retire, so the dollar amount of losses, just logically, based on what we've seen, is larger.

The Chair: However, would you say that the overall percentage of fraud victims or the targets of fraud, whether successful or not, would be, disproportionately, seniors? Do you not have data that you could lean on to support that right now?

Anthony Ostler: All Canadians are victims. You could be a 15-year-old—

The Chair: I understand that all Canadians are victims. That's not my question. My question is this: Are seniors disproportionately the victims of fraud in Canada?

Anthony Ostler: On a dollar-value basis, yes.

I think you may be contemplating a meeting with the Canadian anti-fraud centre. Chris Lynam, who runs that centre, is an expert on this. They collect all the statistics and have demographics, so—

The Chair: Mr. Ostler, this will be my last point. What I'm saying is this: You represent the banks.

Anthony Ostler: Yes.

The Chair: Okay. If I am a client of a bank, and there are 100 people who have been the victim of a scam or fraud involving that bank in Canada, what I want to know is this: Are 50 or more of those people aged over 65? This is the general essence of what I'm trying to get to.

Anthony Ostler: I don't have....

The Chair: I take your point that all Canadians are victims of fraud, and the older a Canadian is, the likelihood that the amount of money in their bank account is increased would ring true. However, what I'm trying to understand is whether or not the depth of the problem we're dealing with needs to be addressed more specifically. For example, you talked a lot about public awareness and collaboration. Well, if we're talking about seniors, hypothetically, being disproportionately victimized, that requires a different exercise of conversation within government to understand who is most vulnerable and whom we're helping.

I take the point, perhaps, that you don't have that. I'd really appreciate it if you could submit through the clerk, please, to the committee, as a follow-up, the data that you do have publicly available. It could further help to shed a bit of light for us on the demographics, from an age perspective, that are being most heavily targeted in the country.

● (1220)

Anthony Ostler: Yes, we will.

One thing I'd like to add is that there is a code called the seniors' code, which the banks uphold, with the Financial Consumer Agency of Canada. There are a bunch of controls and processes that are in place for supporting seniors.

In addition to education and awareness on scams and fraud, there's elder abuse or financial abuse that occurs, for instance, so we also have programs and tools on our website to educate and support seniors to try to avoid the various scenarios, not just scams or fraud but people getting at their money. There are lots of developments, but the seniors' code is a key part of helping to protect seniors.

The Chair: Thank you. I appreciate it.

Witnesses, thank you very much for your time and availing yourselves to us today. We appreciate the insight. It starts us off on this important study in a useful and meaningful way.

Colleagues, here's what I'm going to do: Because votes are at, I believe, 12:34, I'm going to suspend until the 10-minute voting period has finished or I have been told by all of you that you have completed your voting, which would bring us to, roughly, 12:44, at which point we're going to resume this conversation. For now, we are suspended.

● (1220)

_____(Pause)_____

● (1250)

The Chair: Colleagues, we are going to resume where we left off as per the commitment we made.

Ms. Dancho, you presented a motion. So that I'm not putting words in your mouth, perhaps I'll turn to you for a moment to explain what it is you're asking for, to refresh our memories. Then I'll move forward as directed.

Thank you.

Raquel Dancho: Thank you, Mr. Chair.

I'm asking for unanimous consent to adopt the following motion:

> That the committee report to the House that it condemns the use of forced labour in supply chains, especially in China; rejects unjustified American tariffs that threaten Canadian workers and industries; and calls on the Liberal government to strengthen and reinforce Canada's existing ban on forced-labour imports and take more effective action to stop goods made with forced labour from entering Canada.

This follows quite a few discussions we've had at this committee. I think we've worded it in a way that really outlines the issue in a fair manner based on past discussions we've had. The Conservatives support adopting this motion. I know the Bloc Québécois as well supports adopting this motion and reporting it to the House, so we ask Liberal members to give us UC to do so.

Thank you, Mr. Chair.

The Chair: Thank you, Ms. Dancho.

For clarity, I'm being asked to ask for unanimous consent for the adoption of this motion.

I will remind members that the motion was presented by Ms. Dancho prior to the suspension of the meeting a few moments ago. We are not voting on there being a discussion on the motion, which is now on notice officially. We are voting on whether we are adopting the motion through unanimous consent, which is necessary because the motion had not been put on notice previously.

With that, I am looking for unanimous consent. I don't see unanimous consent. Therefore, Ms. Dancho, we will not be able to move forward.

Ted Falk: Do we have a recorded vote?

The Chair: Mr. Falk, because it's not a vote itself, we can't go to a vote. Because we need UC in order to even enter into a position that would allow us to, there will be no recording of that.

Colleagues, with that, we were scheduled to continue a conversation in camera on the mould-maker study, but seeing the time before us now, I don't think we're going to have the ability to meaningfully engage on that topic at the moment. Therefore, I'm going to suggest that the meeting be adjourned, and we will readjust the schedule in order to find an opportunity for us to finish version two.

With that, the meeting is adjourned.