HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 043

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, June 8, 2026

Chair: Ben Carr

Standing Committee on Industry and Technology

Monday, June 8, 2026

● (1630)

[*Translation*]

The Chair (Ben Carr (Winnipeg South Centre, Lib.)): Good afternoon, everyone.

Unfortunately, because of the votes, we're running a bit behind this afternoon, but we're going to make up the time over the next few hours.

[*English*]

I hope you've had a good day thus far despite some interruptions with votes.

Witnesses, I apologize for keeping you waiting. That is simply the way things work in Parliament, although, seeing that the clock is at 4:29, we're actually starting right on time. I'm glad we're able to move forward.

Colleagues, this is our second meeting in relation to the study on fraud and scams in Canada.

[*Translation*]

Colleagues, I want to let you know that all of the audiovisual tests have been carried out and that everything is working.

[*English*]

This is just a reminder to witnesses that if you are using your earpiece and it's plugged in but not on your ear, please ensure you place it on the sticker in front of you. That's to protect the health and well-being of our interpreters.

With that, colleagues, we have four witnesses here in the room with us today. From Beauceron Security, we have David Shipley, who is the chief executive officer. From the Canadian Cyber Threat Exchange, we have Jennifer Quaid, the executive director. From Meta Platforms, we have Jon Camfield, defence lead, security policy; and Rachel Curran, director of public policy at Meta Canada.

Welcome to all of you.

Witnesses, you'll have up to five minutes each for introductory remarks. I understand that it will be Mr. Camfield speaking on Meta's behalf.

With that, Mr. Shipley, I'm going to give you the floor.

David Shipley (Chief Executive Officer, Beauceron Security): Thank you, Mr. Chair. I appreciate the opportunity to testify before this committee again.

At Beauceron Security, we have helped educate more than one million individuals on how to spot and stop cyber-attacks and online scams. I've spent more than a decade studying how cybercriminals exploit human trust online. Their business is booming. Erin West, founder of the international anti-fraud effort Operation Shamrock, has called it the “scamdemic”.

Fraud rose once again in Canada in 2025, hitting more than $700 million in reported losses, but with losses likely ranging between $7 billion and $14 billion, as only 5% to 10% of fraud is reported. Fraud losses are up in Canada 326% since 2020. We're losing, and we're losing more than just money. It's shattering Canadian families, and it's leaving seniors destitute.

Let me be blunt about where this fight is being lost. If we think of the scam economy as a funnel and think of where each group sits, the online platforms that profit by selling scammers advertising sit near the top. One company's products stand above all others. The Independent recently quoted Lloyds in the U.K. as stating that two-thirds of their customer fraud cases start on Meta platforms. It's deeply ironic that Facebook bans real Canadian news content but happily runs fraudulent AI videos featuring deepfaked politicians promoting investment scams and pays fake accounts promoting Alberta separatism.

By Meta's own internal projections, reported by Reuters last November, the company expected to earn about $16 billion globally in a single year from scam and banned goods ads. That's roughly 10% of its global revenue. I'd love to know what the estimates are for the value and number of fraudulent ads targeting Canadians. Meta knows.

Both Silicon Valley's own county and a U.S. coalition are suing it for allegedly knowingly profiting off scam ads. The rot starts at the top. Everyone else pays the fraud tax while Meta makes billions.

Here is what I'm here to talk to the committee about and ask it to consider in its studies.

First, we have to make online platforms liable for scam ads that they profit from. If they fail to properly police their platforms, they foot the bills, not the banks and not Canadians. Make them accountable to federal agencies for reporting on fraud and their efforts to combat it.

Second, legislate a 24-hour cooling-off period for material, unusual transactions that a financial institution flags as suspicious. Customers can opt out, but if they do, they should give up reimbursement. This alone would massively protect people from romance and investment fraud, the two costliest categories. It would help break the emotional spell many can find themselves experiencing during this sophisticated scam.

Third, do not build a bank-only liability model. We have learned the hard way on this in cyber with ransomware. When insurance began paying out, the attacks exploded. If you put banks alone on the hook, fraud costs will only grow for everyday Canadians. The banks never pay these costs in the end. The costs will be passed on to your constituents in service charges and interest.

We need shared responsibilities among online platforms, banks and bank customers. Banks should provide and track fraud education with their customers. Without a feedback loop, fraud awareness programs are just noise. With one—and we've proven this in our work in employee education—it guides people to less risky behaviours. If a customer won't take 10 minutes to learn, that should factor into their reimbursement. That's shared responsibility.

Here's what our data has shown. In our work with employees, we've shown that those who do not think they play a role in protecting themselves or their organization click 37% more on scam emails than those who do. Those who are educated and motivated to protect themselves fall victim less and report more suspicious activity.

Fourth, properly resource the Canadian anti-fraud centre. They are unable to meet the call demand they are receiving, and their work is about more than just taking down the details. That group is a lifeline to someone who is despondent and contemplating harm because of fraud. Be clear in the funding for this agency so Canadians can understand how we're investing in fighting fraud. This is perhaps where fines on big tech companies profiting from fraud on the backs of Canadians could be directed.

I have one last request. I urge the committee to use all of the powers at its disposal to investigate whether Meta knowingly profited from fraud, as is alleged in the Reuters story. Canadians deserve to know the truth.

I thank you and welcome your questions.

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

Ms. Quaid, I'll turn the floor over to you now for up to five minutes.

Jennifer Quaid (Executive Director, Canadian Cyber Threat Exchange): Thank you, Mr. Chair.

Thank you to all members here for the opportunity to appear today on behalf of the Canadian Cyber Threat Exchange and the Canadian anti-scam coalition.

The Canadian anti-scam coalition is Canada's largest coordinated effort to fight scams, bringing together leaders in financial services, telecommunications and technology, alongside government, regulators and law enforcement. We do it because fraud is no longer a nuisance. It is the defining financial crime of our era. Each year, it affects millions of Canadians, costs billions of dollars and erodes public trust in our systems. This is not a trend. It is a persistent and growing threat.

I want to talk about three ways Canada can begin to turn this tide.

First, we need a genuine whole-of-society approach. Financial institutions, telecommunications companies, digital platforms, regulators, law enforcement and government must actively collaborate with shared objectives, coordinated policies and a focus on upstream prevention. Scammers do not respect organizational boundaries. Their operations move through telecom networks, banking systems and social media platforms and into the phones of Canadians every single day. No single organization can stop them alone.

Other countries have recognized this. The U.K. built Stop Scams UK, Australia created the National Anti-Scam Centre, and Singapore unified banks and telcos within a single operational framework. Canada has the will and the talent to do the same. What we need is the architecture.

Second, fraud must be understood as part of a broader cybercrime and money-laundering ecosystem. The same infrastructure used to steal credentials is used to commit fraud. The same networks used to launder drug proceeds are used to move stolen funds offshore. We need a coordinated approach that connects FINTRAC, the Canadian anti-fraud centre, cyber-defence functions and the private sector, and treats fraud as the common thread throughout them.

Third, and perhaps most urgently, fighting fraud depends on timely information sharing. Today, a bank, a telecommunications provider and a digital platform may each identify the same scam activity, yet there is no effective mechanism to share that intelligence in real time. As a result, each organization sees only part of the picture, while fraudsters share information instantly and exploit the gaps created by siloed systems and outdated regulations.

The Canadian anti-scam coalition was created in part to address this challenge, but we need legislative and regulatory frameworks that enable responsible information sharing. Other countries have taken this step. Canada can too, and we have an opportunity to lead.

The threat we face is not coming from opportunistic amateurs. These are organized criminal networks using sophisticated technology and professional operational models. If our response remains fragmented, we will continue to be outmanoeuvred.

Prevention must be our primary objective. That means real-time transaction intervention, network-level disruption of scam infrastructure and meaningful public education that reaches vulnerable Canadians where they are and in ways they can understand.

Canada has the opportunity to build a world-class response. We have an engaged private sector. We have law enforcement that understands the threat and wants to do more. What we need now is a framework that breaks down silos, enables real collaboration, provides meaningful resources where they are needed and puts prevention at its centre. The Canadian anti-scam coalition and the Canadian Cyber Threat Exchange stand ready to help build that framework.

● (1635)

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

Mr. Camfield, I'll turn the floor to you for up to five minutes.

Jon Camfield (Defence Lead, Security Policy, Meta Platforms Inc.): Thank you, Mr. Chair.

Good afternoon. Thanks to all of you for the opportunity to appear before the committee today. My name is Jon Camfield. I lead our global trust and safety policy work on fraud and scams. Joining me is my colleague Rachel Curran, director of public policy of Canada at Meta.

Meta takes the threat of fraud and scams seriously. Financially motivated criminal actors are among the most persistent and agile threats we face online today. These networks operate across platforms, exploit multiple sectors and often operate with impunity from jurisdictions with limited rule of law.

In 2025 alone, we enforced on over 10 million accounts linked to criminal scam centres, which are organized criminal organizations that traffic and exploit people to run scam operations at an industrial scale. There are hundreds of thousands of victims driving these scams. We invest significantly in detecting and removing fraudulent actors and content, and we maintain active partnerships with Canadian law enforcement, regulators and industry to combat fraud.

Our approach is multi-layered and outcomes-driven.

We have dedicated policies on fraud, scams and deceptive practices for all of our platforms—Facebook, Instagram, Threads, Messenger and WhatsApp—and also across all of them on ads. In 2025, we removed more than 159 million ads globally for violating these policies. We removed 92% of them proactively before they were reported to us. Overall, we achieved greater than a 50% reduction in scam ad reports across our platforms in the same time period.

In addition to policy enforcement, we're continuously strengthening efforts on our platforms to deter these scammers. Here are some examples. First, we are expanding advertiser verification, with a goal of 90% of our ads revenue coming from verified advertisers by the end of 2026, up from 70% at the end of 2025. Second, we deploy advanced AI tools to prevent scammers from misusing the images of public figures to bait people into fraudulent ads. Third, on Messenger, we are also rolling out on-device AI to detect scam patterns inside conversations and warn users in real time, even within end-to-end encrypted chats.

As the government develops Canada's first-ever anti-fraud strategy, it is imperative to remember that cross-sectoral collaboration is essential. No single company or sector can see the full fraud attack chain. A consumer may first encounter a scam on SMS or on social media, or they may be moved through a phone call or a fraudulent investment site and ultimately lose money through a crypto or bank transfer. Each sector has a limited view, with no one company or platform seeing that complete picture. Effective disruption therefore requires sharing intelligence across these boundaries.

That is why Meta invests heavily in cross-sector information sharing. Through the fraud intelligence reciprocal exchange, or FIRE, we exchange signals bidirectionally with financial institutions, enabling faster enforcement. Through the Global Signal Exchange, we share structured scam indicators—URLs for malicious websites, phone numbers and also ad accounts—with governments and industry across multiple jurisdictions around the world. Government entities are able to participate within GSE at no cost.

Here in Canada, Meta supports the stand against scams campaign alongside the Canadian Bankers Association. We maintain dedicated reporting channels with the Canadian anti-fraud centre, the RCMP, the Canadian Securities Administrators investment fraud task force and the Competition Bureau.

We participated in Operation Maple Disruption with Canadian law enforcement, securities regulators and financial institutions. Alongside Canada, Meta has similarly endorsed the UNODC's global public-private partnership framework against fraud. We're also founding signatories to the Industry Accord Against Online Scams and Fraud with Google, Amazon, Microsoft, OpenAI and many others.

As Parliament considers how best to protect Canadians from fraud, we encourage three actions. The first is a whole-of-ecosystem approach that brings all sectors of the fraud attack chain to the table from the outset: digital platforms, telecoms, financial institutions, fintech and law enforcement. The second is strong information-sharing frameworks with legal safe harbour protections so companies can collaborate in good faith without fear of liability under privacy or competition law. The final one is an outcomes-focused framework that measures results rather than mandating specific methods, allowing all of us to remain as agile as possible as fraud tactics evolve rapidly.

Thank you for your time today. We welcome questions.

● (1640)

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

Colleagues, we'll now move into our first round of questions.

Ms. Borrelli, the floor will be yours for six minutes.

Kathy Borrelli (Windsor—Tecumseh—Lakeshore, CPC): Thank you Chair.

My first question is for Mr. Shipley.

Mr. Shipley, seniors are often told to watch for warning signs, but the warning signs are becoming much harder to detect, with spoofed numbers, AI-generated voices, fake investment ads and impersonation scams. From your experience in cybersecurity education, what types of prevention actually work for older Canadians? More specifically, what should Canada be doing differently so that seniors are protected, since the sophistication of scams has evolved past a level of just red flags?

David Shipley: The first thing we noticed in our research—and yes, you are correct—is that the technical indicators for being able to tell if something is a phishing email or a scam are incredibly difficult to see now, thanks in part to AI companies making tools that make it easier to make things look faster and slicker than ever.

The research we've done and that Toronto Metropolitan University has done has shown that teaching people about emotional intelligence helps—listening to their gut and thinking about why someone is trying to make them feel a certain way, whether it's giving them a rush or getting them excited about an opportunity. They are often preying on the loneliness epidemic in this country.

The biggest thing that can help our seniors right now is the 24-hour hold. I've talked to so many banks, and their teams know it's a scam, but a person has fallen in love. They think that someone they care about is in danger, and they need to act. If we had that hold—and it's important to understand it's opt-out only; everyone starts with the hold in place—we would stop so much of the most expensive fraud targeting our seniors.

● (1645)

Kathy Borrelli: You've partially answered my follow-up question already, which is this: What would be the three most important pieces that would help seniors in a fraud prevention program?

David Shipley: In my remarks, I've given footnotes to all of the stories I've referenced. Darren Taylor wrote a heartbreaking story in Orillia Matters on June 5 that I encourage you all to read, titled “Senior lost almost $1M in ‘increasingly common’ deepfake scam”. These are increasingly happening on the platforms, including Meta but not exclusive to Meta. They're portraying our Prime Minister and others. Premier Doug Ford was also portrayed, and a senior in the GTA lost $100,000.

We have to hold the platforms accountable to police them. If they cannot responsibly offer advertising, then they should stop.

Kathy Borrelli: Should there be stronger rules around first-time transfers, crypto purchases, international wires or payments made after remote access software has been used?

David Shipley: Yes, and there's so much we can do on that side, but remember that some of these attackers, once they develop long-term relationships, will coach people through a variety of controls and other things. As my colleague Jennifer from CCTX pointed out, it requires a whole-of-society effort to combat this, but all of those things will help.

Kathy Borrelli: Ms. Quaid, I want to ask about what happens after a senior has already been scammed. In many cases, the victim reports the fraud, but the money has already moved through the system via crypto wallets, mule accounts or foreign channels. For the victim, the system can feel like it records the loss but does not move quickly enough to recover it.

What would Canada need to do to improve the speed of tracing, freezing and recovering stolen funds after a senior reports a scam?

Jennifer Quaid: Sadly, evidence shows that seniors tend not to report when they have been the victim of a scam, more so than any other segment of society. Most of the senior reporting we see is from seniors who have lost less than others or who have seen a scam as opposed to having fallen victim to one. That, in and of itself, is a problem.

What can the system do? The system has to focus on prevention. No matter what we do, it will never be fast enough. It will never be good enough. AI and frontier AI are making it too hard for anyone to catch, not just seniors. If we're not focusing on prevention, we are simply continuing to play whack-a-mole.

Kathy Borrelli: Thanks very much.

I'm good.

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

Mr. Bains, I'll go to you. I understand you'll be splitting your time with Mr. Ntumba. I'll allow the two of you to work that out.

The floor is yours, sir.

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

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

I couldn't help but notice that many of the recommendations coming from Meta and Madam Quaid were very similar.

Mr. Shipley, you referenced the Reuters report. I'm going to talk a bit about that and then ask questions of the folks at Meta.

Meta projected that roughly 10% of its revenue in 2024 would come from ads tied to scams, banned goods or misleading content.

Mr. Camfield, you talked about removing over 159 million scam ads last year alone. These same documents indicate that Meta users were reportedly served 15 billion high-risk scams daily, often letting them run unless 95% fraud certainty was detected.

My question to you is this. For less certain violations, Meta instead charged higher ad rates to deter offenders who were effectively still profiting from the potential fraud. Why is Meta's threshold for confidently identifying a scam so high? Why is it 95%?

● (1650)

Jon Camfield: Let me speak a bit to the specific numbers there. The 10% was based on some internal research to identify the topline ceiling of potential violations. That included non-violating content that is often caught up in our systems. It included things that are not actually frauds and scams as well. That is a higher number than the reality.

The same document that was leaked and referenced in the Reuters article in 2024 pointed out that the actual number is likely in the 3% to 4% range. Again, that was in 2024. We reduced that by 50% in 2025, and we continue to work on that today.

On the angle of charging more, the ad auction system is incredibly complex. What it does is it reduces the value of a bid in an auction if we suspect but cannot prove that an ad is a scam.

This speaks to where we are on the scam attack chain. What we see is the very early stages of a scam, often with potentially innocent-looking ads, innocent-looking engagements or new friendships being formed. It is challenging—

Parm Bains: I'll jump in because of the time.

How do you verify the legitimacy, then? Do you do a reverse process of some sort?

Jon Camfield: We have a couple of processes. One is through information sharing. One of our most valuable signals is banks saying, “Hey, these scam accounts are using these URLs, domains and identifiers. Can you look in your systems?” We take those, put them into our systems, fan out, and look for other signs of that. We're often able to turn up to 600 times more assets in our systems from any one seed that we receive from the banks. That is the most valuable piece of information.

Parm Bains: Finally, before I cede the rest of my time to Mr. Ntumba, the advocacy group Consumer Federation of America filed a similar complaint alleging that Meta failed to block scam ads while charging advertisers more to display their content and rolled back efforts to reduce scams. What is your response to that claim?

Afterward, Mr. Ntumba will take the floor.

Jon Camfield: To directly answer that, we do not charge advertisers more. We reduce the value of the potential scammer—the suspected or possibly uncertain ad—in the auction system. That means in the long term we're making less money off the ad slot by letting other ads win the auction by penalizing that ad. It does not mean we're charging them more, and they cannot pay more to get a better ad slot. It just reduces the value of the auction they already bid into.

Parm Bains: Thank you.

[*Translation*]

Bienvenu-Olivier Ntumba (Mont-Saint-Bruno—L'Acadie, Lib.): Thank you.

Mr. Camfield, as you know, Meta is almost like a town, a nation, a community or a shopping plaza, with many homes and businesses and lots of people going around. Each person is responsible for setting the alarm at their home's front door. You're in charge of security for the whole place, the main entry. I know the banks' approach is to tell customers that if they have a bank card, they're responsible for it. At my home, I set the alarm and I lock the door with my key. I make sure my home is secure.

If people invade my country, I don't blame my neighbour. I blame the government for not keeping the country secure. That's kind of what Meta is like.

Why is fraud on the rise within Meta? I'm asking you this question because you're the ones responsible for keeping Meta secure.

[*English*]

Jon Camfield: It is a challenge. The scammers we deal with today are, as I said, the most adversarial we face online, including nation-state actors and espionage and spyware actors. They are industrialized and scaled in a form that's hard to put into words.

It's important to think about the jurisdictions they most often come from. We're talking about hundreds of thousands of victims who've been trafficked and are beaten if they do not scam and meet their quotas. We're talking about places where the GDP of the countries they're operating from is 40% driven by scam activity, not just on our platform but on all platforms around the world. They have a high incentive and low accountability for what they do and how hard they do it.

The challenge is how you deal with such a scaled, determined and financially empowered adversary. We deal with disruptions. We deal with product change to make our products more hostile to scammers without raising barriers to normal users or legitimate businesses. It's a difficult balance, but we do invest heavily. We take the threat seriously.

● (1655)

[*Translation*]

The Chair: Mr. Ntumba, unfortunately, your time is up. Thank you.

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

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

Greetings to all my colleagues. I'm sorry I can only be with you virtually.

I want to thank the four witnesses for joining us. I'm very grateful to them.

Mr. Shipley, you ended your opening remarks by suggesting a question that we could ask Meta.

Could you repeat it for us?

[*English*]

David Shipley: I would love to know what Meta estimates is the value and number of fraudulent ads targeting Canadians.

[*Translation*]

Gabriel Ste-Marie: Could the Meta representatives respond?

[*English*]

Jon Camfield: I regret to say that I do not have those numbers, but I can look into them and get back to you.

[*Translation*]

Gabriel Ste-Marie: Okay.

The committee would appreciate it if you could send us the numbers. Thank you very much.

On May 11, Le Journal de Montréal's investigative bureau published a report on how Quebeckers are losing a lot of money to deepfakes on Facebook. Fake videos of Mark Carney, François Legault, Doug Ford and influencers are showing up on social media. There are even fake videos of Keanu Reeves and people like that. Le Journal de Montréal spoke to four people about their experience. Two of them had lost more than $100,000. I don't know if you heard about that article or that investigation. The journalists said they had contacted Meta, but it declined to speak to Le Journal de Montréal.

What do you have to say to the people who were taken in by deepfakes posted on your platforms? Many of them have lost their life savings, their retirement savings.

[*English*]

Jon Camfield: It is horrible. These crimes are horrific, and it is deeply troubling to see that type of loss in any situation, but particularly from retirement savings as people are looking towards being done and being retired. That is horrific. We don't want to see these types of actions coming from our sites.

We do everything we can to detect deepfakes and to detect celeb bait being used in our ads and on our platforms. We've deployed multiple layers of AI technology to look at not only the face itself but also the context around deepfake ads.

As we have deployed this, we've seen immediate adversarial adaptation. We started with the topmost global celebrities, and immediately we saw country-level celebrities, government celebrities and government figures. As we enforced further down the chain, we saw scammers go local. This is useful, because it drives a lot of effort on their part. It takes some effort on our part, but we're happy to do that.

This adaptation and adversariness is something we must expect from scammers, and only by truly undermining the entire economy of scams will we be able to change that.

[*Translation*]

Gabriel Ste-Marie: It is horrible, you're right, but it's happening on your platforms. I know you're making an effort, but scams are still happening on your platforms.

How much responsibility do you bear for these thefts?

[*English*]

Jon Camfield: I would say there's incredible value in discussing across and working together across the entire fraud attack chain. Things that start on SMS or social media metastasize and move. They go onto websites—fake, fraudulent investment sites—but even after we block them, we see them stay on the open Internet for up to three years, meaning they're also being used in other campaigns, other tools and other practices on different platforms.

It truly is only through a whole-of-society response that we can share and take down how to deal with this.

● (1700)

Rachel Curran (Director, Public Policy, Meta Canada, Meta Platforms Inc.): I'll add to that, if you don't mind, Jon.

We have reduced the number of scams that are reported by over 50%, so our efforts have had a real impact in reducing the number of scams that are reported and scams that appear on our platforms. The efforts we're undertaking with Jon and his team are having a real impact. Have we reduced them to zero? Not yet, but we're making good progress towards that.

[*Translation*]

Gabriel Ste-Marie: Thank you for your answer.

Obviously, you need to keep doing more. I'm worried, because there are a lot of scams, and while some are happening on websites, it seems that many, if not most, of them are happening on your platforms. You have the power to fix that.

I have another point to make. For the past several years, Facebook users have been banned from seeing news content or sharing news articles or videos.

However, there are deepfakes with fake reports from Radio-Canada, TVA and other media outlets.

Is Meta planning to bring back news sharing in the near future, or is your model really just based on spreading disinformation to the public?

[*English*]

Rachel Curran: Yes, we would love to bring back Canadian news content onto our platforms, and I'm saying that as a Canadian, not as an official representative of Meta. We've said this before.

In terms of where scams are happening, look, we are here to talk to the efforts we are taking to reduce scams. I understand a number of our colleagues, other tech platforms, have been invited and have declined to appear before this committee to talk about the work they're doing to reduce scams. We think this is important enough that we want to talk to you about the efforts we are taking.

[*Translation*]

Gabriel Ste-Marie: I have one last question.

Why is Meta more successful at stopping news content from being shared than stopping deepfake videos from being used to scam the public?

Why are you more successful at taking down news content than fraudulent videos?

[*English*]

Rachel Curran: I don't think that's correct. The Online News Act says that either we need to compensate news publishers for the material they place voluntarily on our platforms, or we need to remove news content from our platforms entirely. We have chosen to comply with the Online News Act by removing news content from our platforms. Unfortunately, that's the situation we are in today.

We have spoken to the minister of heritage about options to restore news to our platforms. I'm hopeful we can get there at some point, but we're not there yet.

[*Translation*]

Gabriel Ste-Marie: Thank you.

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

[*English*]

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

Ted Falk (Provencher, CPC): Thank you.

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

You said that two-thirds of scams—online scams and fraud—are on the Meta platform. What are the other platforms that fraudsters are using?

David Shipley: The precise sourcing for that was the Lloyds Banking Group in the U.K. On the weekend, The Independent said that two-thirds of their consumer fraud cases start on Meta-owned platforms. We also see in the literature other platforms on the social media side, and downstream, it's telecommunications, SMS text, fake phone calls, etc., on that side.

This has been consistent. In 2023, Lloyds reported that over 54% of APP fraud—authorized push payment—was happening on Meta-owned platforms. They own the market by dint of their size, so of course the scammers want to go there.

Ted Falk: Would you propose any solutions?

David Shipley: Well, I would say this. If you—

Ted Falk: Give me some low-hanging fruit, some easy wins.

David Shipley: Make Meta liable for the hundreds of thousands of dollars in fraud lost by Canadian seniors—a member mentioned the individuals in Quebec—until such time as the fraud ads stop. When they're properly financially motivated, they'll be able to make their billions in ads, but they won't be victimizing Canadians.

Ted Falk: Mr. Camfield, I'd like to ask you a few questions as well.

It's clearly been identified that Meta is a medium for lots of online scamming. Based on the Reuters article, it would appear that Meta is well aware that it's being used as a conduit for scammers. What level of responsibility do you think Meta should take, and what are they taking?

Jon Camfield: We know we have a critical role to play in combatting scams. We are at the upper level of that funnel as described, or in the fraud attack chain, where a lot of fraudsters will seek out potential victims. To our credit or our downfall, we are one of the larger social media platforms, so we are an attractive target, as has been said.

That size comes with a responsibility and many challenges. We must balance free expression and the interests of small business alongside combatting scammers as hard as we can. We have to find ways to differentiate the bad actors and scammers, who will do their best to get around our defences, while making sure that normal users can access and use the platform successfully.

● (1705)

Ted Falk: Would that suggest that you knowingly allow scammers on your site and do a cost-benefit analysis or risk-benefit analysis as to whether or not they stay?

Jon Camfield: I would not discuss—

Rachel Curran: I'm going to disagree wholeheartedly with that. That's bullshit.

Jon, you can talk about this.

We are working towards 90% of our revenue coming from verified advertisers by 2026. We currently are at between 70% and 80%.

Is that correct, Jon? You can speak to this further, but we're working towards 90% of our revenue coming from verified advertisers. There's a reason we're not working towards 100%, which Jon can get into, but we have absolutely zero interest in getting revenue from advertisers who are scammers or fraudsters. That creates an experience on our platforms that is unpleasant and not good for our users, and we want to prevent it to the extent that it's possible.

Ted Falk: Okay. I appreciate what you've just said.

Many times, when banks are confronted with clients, customers or consumers who have been defrauded, they come to the table and provide compensation—not in every case, but in a lot of the cases. What do you as Meta do for your customers who have been defrauded on your site? How do you back that up? What recourse do people have with Meta?

Jon Camfield: It's a challenge because we have no control over the act of fraud, the act of money transfer. We do not touch. We do not see. That happens in financial institutions.

Ted Falk: I understand that, but what are you doing for people who have been defrauded based on advertising that originates on your platform?

Jon Camfield: To be clear, if we know an ad is a scam, we take it down. It is against policies, and it is removed.

Ted Falk: What do you do for the person who has been scammed?

Jon Camfield: We don't have a route or a path to know—

Ted Falk: You don't really care about people, then.

Jon Camfield: We do.

Ted Falk: No, you don't.

Jon Camfield: I disagree. We absolutely—

Ted Falk: Those are all of my questions. Thank you.

Jon Camfield: Users are our only valuable commodity as Meta.

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

For the next line of questions, I have Mr. Ma and Mr. Bardeesy.

Mr. Bardeesy, I'll turn the floor to you first.

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

I want to ask a couple of questions of Meta, and I want to start with Ms. Curran.

I think Canadians are watching this hearing with a lot of interest, given the gravity of what is before us, and I think they'd be very concerned with the unparliamentary language they just heard.

I want to pick up on a point that Mr. Ste-Marie made around the Online News Act. There was a very strong article in the Globe and Mail over the weekend—in which Ms. Quaid was quoted—about the kinds of fraud being seen online, the kinds of protections Canadians should be expecting and the kinds of measures they can take around the all-of-government and all-of-society approach. A colleague of mine just tried to share that article on Facebook platforms and received the following response: "In response to Canadian government legislation, news content can't be shared."

This is an article that could help millions of Canadians—if they had access to this article through your platforms—respond to the very things that are the subject of this study. Today, could you commit to ensuring that that one Globe and Mail cover article from Saturday in which Ms. Quaid is quoted is not blocked for Facebook and Instagram users?

Rachel Curran: I wish we could MP Bardeesy. The reason we can't is the Online News Act, which prohibits us from sharing Canadian news content on Facebook and Instagram, unless we are willing to sign up to the compensation framework that the government has set out in the Online News Act.

I'm hopeful that we can resolve this with the government and can share Canadian news online again on our platforms. We are working towards that resolution.

● (1710)

Karim Bardeesy: Ms. Curran, I'm talking about one article that gives actionable information to Canadians on how they could help fight fraud.

Rachel Curran: That's the problem, though. The Online News Act does not allow us to share even a single article on Facebook or Instagram unless we are subject to the entire framework that is set out in the Online News Act. That is the way the law has been drafted.

Karim Bardeesy: It's a piece of legislation that has been duly passed by this Parliament.

I'll share the rest of my time with Mr. Ma.

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

All of our witnesses seem to agree that collaboration is critical for fraud prevention.

I'm going to start with a question for the Meta group. What collaborations have you implemented already?

Jon Camfield: As I mentioned briefly in my introduction, we launched the fraud intelligence reciprocal exchange in 2024, and it has scaled the past couple of years. It is bidirectional with banks. We have representation from FS-ISAC, which has many Canadian members as well, and from other banks around the world. There are over 50 banks actively exchanging signals with us for takedowns.

We're also members of the Global Signal Exchange, which is an international non-profit that works with industry, governments and regulatory agencies. They provide their services for free to regulators, and industry pays to participate. We use that to engage with other governments and directly with industries, and we do information sharing for multiple activities.

Michael Ma: You said you collaborated and implemented a number of measures, yet we're still seeing repeated scams, over and over again.

I'd like to ask Mr. Shipley and Ms. Quaid to comment on that.

David Shipley: One has to almost admire the ingenuity of the criminals.

The reality is that we could be doing so much more. It's just that the financial incentives aren't there to force us to act to align on this. If all of a sudden this starts to cost billions of dollars in revenue, I think they'll get better at stopping the Mark Carney investment scam ads on their platforms.

Jennifer Quaid: I would add to that.

It's about more than financial incentives not being there to align us. We currently have rules and regulations in place that prevent the sharing of meaningful information in a timely manner. If we cannot enable banks, telcos and social media platforms to share information in order to get ahead of the scams, we're just going to keep paying more money.

That's what we need out of this proposed strategy.

Michael Ma: What seems to be stopping it? What particular legislation is preventing that?

Jennifer Quaid: Part of it is that a lot of organizations fear reprisal. Mr. Camfield mentioned this in his remarks. There is a need for safe harbour legislation so organizations can share information among themselves and not fear reprisal for doing so.

Part of it is due to rules around sharing—with whom, how, when, why and the length of time it takes for sharing that information. We have to wait days or weeks to share information, and the scammer moves on. These things are immediate. That's what we need to enable.

Michael Ma: I believe you have all mentioned the timeliness of that. Do you feel it's adequate, at this point? Given that AI operates in the background, we should be able to detect it right away.

Mr. Shipley, I don't know if you....

David Shipley: I want to add this on timeliness. As we move to real-time payment systems that go beyond our traditional reconciliation, there's no getting the money back. It happens instantaneously.

My colleague's point about prevention is absolutely vital. We can't put the horse back in the barn once the fraud has already happened.

Jennifer Quaid: In terms of sharing information, if it is timely and meaningful, we will start to see patterns of activity very quickly. That's when we head towards prevention. We can stop the next person from being a victim.

Michael Ma: Thank you.

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

[*Translation*]

Mr. Ste-Marie, the floor is yours.

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

My next questions are also for the representatives of Meta.

Your profits are astronomical, both globally and in Canada. Meta is a large corporation. It doesn't pay tax in Canada, thanks to its tax schemes and use of tax havens, among other things. You and the web giants [*Technical difficulty—Editor*] the Canadian government to suspend the digital services tax, which was supposed to make up for the tax you don't pay here. You refuse to allow news content to be shared because then you would have to pay royalties to the media. The media industry is in crisis, because all of the advertising is shifting to platforms like yours. Today, we're discussing fraud. You're making an effort to curb fraud, but it's still going on anyway.

Do you think Meta is a good corporate citizen?

● (1715)

[*English*]

Rachel Curran: Listen, we pay all of our applicable taxes in Canada. That includes corporate income tax. It includes payroll taxes. We pay every tax levied by the Canadian government.

What we were not willing to sign up for was the framework outlined in the Online News Act, which would have required us to pay money to publishers for content they voluntarily placed on our platforms because they received a huge benefit. We estimated that it was about $300 million annually for sharing their content on our platforms. They benefited from distribution on our platforms. We think the value exchange flowed towards publishers, not towards Meta. We declined to pay publishers an additional sum for sharing material voluntarily on Facebook and Instagram.

[*Translation*]

Gabriel Ste-Marie: I'm going to ask my question again.

Do you think Meta is a good corporate citizen?

[*English*]

Rachel Curran: I'm sorry. I didn't hear that question.

[*Translation*]

Gabriel Ste-Marie: Do you think Meta is a good corporate citizen in Canada?

[*English*]

Rachel Curran: We really value our presence in Canada. We value our Canadian users. We value our interaction with the Canadian government on a range of issues.

Personally, as a Canadian citizen, I would love to see Canadian news content back on Facebook and Instagram. I used to follow Canadian news outlets on Facebook and get all my news from Facebook. I would love to see that content back on our platforms, and I'm hopeful we can reach a resolution there.

[*Translation*]

Gabriel Ste-Marie: You say you pay taxes and follow the letter of the law, but the law allows American companies with subsidiaries in tax havens to use them to avoid paying taxes here.

How much income tax did you pay last year?

What percentage of your revenue did it represent?

[*English*]

Rachel Curran: We have no tax shelters. We pay to Canada the taxes that are due to Canada, and we comply with all applicable Canadian tax authorities here. Whatever Canada imposes in terms of tax laws, Meta complies with.

[*Translation*]

Gabriel Ste-Marie: I would humbly remind you that the digital services tax was implemented by the G20, at the behest of the Organisation for Economic Co-operation and Development, because, thanks to tax schemes, online platforms like yours aren't paying their fair share of taxes. I'm disappointed by what I just heard.

The U.K. Payment Systems Regulator released a report in late 2024 stating that, in 2023, your platforms in the U.K. were linked to 54% of push payment scam incidents.

Do you acknowledge that? Do you acknowledge that the same is true for all the countries where you have a presence, including Canada?

Do you acknowledge that that needs to be reduced? The majority of push payment scams are happening on your platforms.

[*English*]

Rachel Curran: I can't speak to what's happening in the U.K. I can say that we pay all applicable taxes in Canada. I think when you're talking about the digital services tax, you're talking about an additional tax that the government wanted to levy on platforms like ours because they felt like we should be paying more tax than was outlined in Canadian law. That is a decision for the government, but we pay all taxes that are required in Canada currently.

[*Translation*]

Gabriel Ste-Marie: We will have to agree to disagree.

The Chair: Mr. Ste-Marie, you have time for one more question.

Gabriel Ste-Marie: I'm going to repeat my last question, the one about the U.K.

The report wasn't about the digital services tax. It was about scams. Their analysis found that 54% of push payment scam incidents were happening on Meta platforms. In other words, the majority of these scams were being carried out on your platforms.

Will you acknowledge that the same thing is happening here and that it's unacceptable?

Thank you very much.

● (1720)

[*English*]

Jon Camfield: I would need to look at the very specifics of this to answer the specific nature of the question. Push payment fraud is a trend that we see pop up in scams, and we have to deal with that as well. It is against our policies, and we take it down when we find it.

[*Translation*]

Gabriel Ste-Marie: Okay.

Thank you, Mr. Chair.

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

[*English*]

Mr. Hoback, the floor is yours, sir, for five minutes.

Randy Hoback (Prince Albert, CPC): Thank you, Chair.

I'd like to thank the committee for letting me participate today. I'm normally not a member of this committee, but it's really timely. Scams, online fraud and things like that are happening in my riding.

We just did a community event about online fraud. We worked with our local Affinity Credit Union, which brought in their banking specialists. We brought in the RCMP—or city police in this case. We limited the audience to 120 people. We could have had 300 people in that room talking about scams they faced either online or not online.

One big thing the police said is a limiting factor is getting information out to people of the existing scam that's going around the community at a point in time. For example, in Prince Albert, there was a scam going on where little Johnny, my grandson Johnny, got arrested because he did something. It was not bad, and it wasn't his fault, but someone had to pay his bail. They're knocking on the door and saying, “We're here to collect Johnny's bail money.” Seniors are very believing and trusting people, especially when somebody is dressed nicely and have a uniform. They're getting caught.

These 120 people were made aware of that scam, and they went to coffee row that week and talked about that scam with all their friends. Now everybody in Prince Albert knows the scam that was going around Prince Albert that week.

I'm curious. You talk about Meta taking down scams as you come across them. Do you do a proactive disclosure saying, “This is a scam” and put it out there so people can see what types of scams are out there?

Jon Camfield: Yes. We maintain a scam prevention hub with exactly that sort of content. It's not always localized to a community as targeted as you mentioned, but it is localized to countries. We also have a series of newsroom posts talking about specific targeted scams that we see. We work with external research firms to look at different communities and different trends. We had one recently on elder fraud and on current trends and tactics targeting elders around the world. We had one on romance scams and so on.

Randy Hoback: You're talking about this hub. I didn't know it existed. I don't think anybody in this room knew it existed. What are you doing to proactively disclose that you have this hub?

Are you actually shaming these scammers? If you come across a scam that's in, say, another country, are you able to actually go after those people in that country? Can you say, “Hey, you're scamming in Canada, so we're going to take you out”, whether that be in Asia or wherever they're coming from?

Jon Camfield: I have two things. On the proactive side, one of the tools we use, which is actually one of my favourite tools, is a series of just-in-time warnings that we deliver to users, whether it's in messaging or with a new friend contact. We'll say, “Hey, this user isn't part of your social graph. They say they're coming from here, but we don't think that's where their location is actually based.” Any one of these signals is easy for a scammer to get around, break, and get through, but we can feed a collection of them to the user and say, “This looks suspicious. It could be legit, because it could be your friend travelling, but you should have your guard up.”

That's really the key to prevention. It's about not focusing on one specific trend, because the more you do that, the faster the scammers will move. It's to really focus on that—

Randy Hoback: I agree with that. “Buyer beware” also has to be a factor in all this. It's just like the news on Facebook: “Watcher beware”.

You talked about 90% of your advertisers being verified. Where I have a problem with this—I agree that they're verified—is that the posting they're advertising with is garbage. It's an influencer who's getting paid by somebody else in the background. It can be the Lego guys from Iran or groups like that. All of a sudden, my face is being posted in that reel.

What are you doing to allow me to make sure that I can't be part of that reel and I don't end up endorsing a post that we know is actual BS?

Jon Camfield: We have multiple different ways to do impersonation protection, particularly for public figures. We can—

● (1725)

Randy Hoback: It's not impersonation in this case. You're taking my name without my consent and saying I'm endorsing something. That's problematic to me, especially being a public figure.

My friend says, “I didn't endorse that”, but everybody in their media platform tells them, “No, you were on that platform endorsing it.” Is that good corporate behaviour?

Jon Camfield: I would say that our reaction to it and our tools to defeat and deal with it are very powerful and are of good behaviour. We work with brand owners and IP owners, including celebrities and public figures, to give them tools to report, identify and proactively detect—

Randy Hoback: This is the average person. It's my neighbour down the street. I think he's an honest guy, and all of a sudden he's endorsing something that he's never even seen before. You've yanked his information and put it into that reel.

You talked about things changing. The other thing I'm seeing right now is fairly new. It's where the newscaster looks really real, but it's AI 100%. They're talking about a current event, and there's enough accuracy on that current event that you think it's true. It sways your opinion, but it's all BS. That's coming at people more and more. They can't determine what's real and what's not.

Is it fair to say that Facebook should be viewed as just an entertainment platform and not be viewed as a newsworthy platform?

Rachel Curran: I don't think it's news versus entertainment. It's that where that violates our policies and where it's misleading people and providing misinformation, we should be taking that down, or at least be applying a label to it so that people understand that it's generated by AI, it's not real and they ought to view it with some degree of skepticism. Those are all the tools we're deploying now.

Look, I agree that we can and should do more on this front, but where people are employing AI-generated deepfakes, for instance, or videos that are AI-generated, we require them to use labels and to label that as AI content. When it presents a significant risk of misleading the public, we will take down video material or AI-generated material, or we will put a label on it saying that it is not true and it should be viewed with significant skepticism.

Randy Hoback: I have one question on that, then. I don't want to talk about the Online News Act. We've talked about that enough and we have our opinions on it. With your proactive activities in trying to take this off your platforms, what legislation or regulations—what else—are there that could allow us to empower groups to have more control of what's being put on your platform so that you can make sure that I'm not endorsing somebody I don't want to endorse or that you have the tools to remove these people more quickly?

I also want to know what you are going to do. You talked about your hub. Nobody knows about it. You need to do a better job of getting out there and identifying scams.

For the last thing, I'll use an example. On Facebook Marketplace, there's a set of patio furniture for sale in the next town. It looks beautiful. It's super cheap. It's too good to be true. When I look in the background of the picture, there are palm trees. I'm in Saskatchewan. Now, we're not as cold as Winterpeg, but how is AI going to interplace...?

You have two questions here. Get legislation that could actually open the door and make it easier to get after these folks. We need to punish the person doing it, somehow. We need to figure that out. Also, on the preventative side, how do we identify things quickly and say, “No, this is not real”?

Jon Camfield: In terms of legislation, I absolutely agree with my colleague on the protective measures for information sharing. Enabling us to do real-time signal sharing will get a lot of incredible benefits. As I mentioned, the result of any one seed we get back from banks is that we're able to take 600 times more assets down, which are not necessarily active assets. They could be completely dormant and not being used but will be used at some point in the future. That gets into some preventative measures as well.

In terms of direct enforcement, that's the value we see coming from government interaction. Sharing with law enforcement and having law enforcement share with their counterparts around the world have been incredibly powerful. That results in real arrests of real scammers, particularly when they cross borders seeking medical care or R and R. Otherwise, they are operating with impunity, from Cambodia, Myanmar and other places where there's no functional enforcement of their bad behaviour. Sharing that information gives a chance to actually make an impact.

Randy Hoback: I have another little one.

The Chair: Ask it very quickly.

Randy Hoback: You talked about law enforcement. Have you been proactively working with law enforcement to create a system in which they can plug into you quickly so that when they come across a scam—in this case, little Johnny being arrested for scamming—they can get that out into a region? You have the ability, through advertising, to say, “We're only going to advertise in this region.” Are you doing that with police forces? Are you doing that with local RCMP, local city police and county sheriffs?

● (1730)

Rachel Curran: Yes, we are—regularly.

I can speak to what's happening in Canada. We're working with the RCMP and with regional and municipal police forces on issues like scams. We liaise with them regularly about what we're seeing. What they're seeing, they report to us. We have a special portal for law enforcement through which they can report to us, and if there's an emergency request, they can send it to us very quickly. If it's not an emergency request, we can work together on how to take material down and address it over the long term.

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

Ms. Begum, I understand that you may be splitting some time with Madame O'Rourke. The floor is yours.

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

Good afternoon—or good evening, almost—to all of you. Thank you so much for being here and for giving us the opportunity to ask you questions.

I'll start with Ms. Curran.

Do you think Meta has a solid enforcement mechanism for tracking down misinformation, disinformation, scams and frauds at this very moment?

Rachel Curran: These are all different issues—misinformation and disinformation, yes, and scams, yes—but there are always gaps between what we prohibit under our content policies and what we enforce against. We're constantly working to try to close that gap.

Doly Begum: In that case, from what MP Bardeesy was talking about, it seems that you were able to take down a Globe and Mail article very quickly. Meta does have an enforcement mechanism to take something down quickly, like an article that was harmless and in fact would have actually added to the quality of life of people and society.

I want to quote the Reuters article that was mentioned by Mr. Shipley and others here. The unreported document showed that Meta “failed to identify and stop an avalanche of ads that exposed Facebook, Instagram and WhatsApp’s billions of users to fraudulent e-commerce and investment schemes, illegal online casinos, and the sale of banned medical products.”

You're able to track down a Globe and Mail article that fast, yet you have an avalanche of ads that exposed billions of users. Do you not have mechanisms for that?

Jon Camfield: We do. The vast difference is the scale of the adversary. It's about how dedicated and well funded the scammer industrial complex targeting our systems is.

Doly Begum: Speaking of funding, it was projected that Meta has earned 10% of its annual revenue in the last years from scam ads.

Jon Camfield: The 10% number is a misrepresentation of the actual research.

Doly Begum: What was the percentage?

Jon Camfield: From the research at that time, it was in the 3% to 4% range, not 10%.

Doly Begum: Okay. I have between 5% and 10%. Even then, if we add up the ad revenue by taking, let's say, your 5%, that's about $6 billion in revenue that Meta made just from ads that were scams and fraudulent. People were getting scammed. Seniors were getting scammed.

Jon Camfield: We've taken that number down. That was the 2024 number.

Doly Begum: That's astounding.

Jon Camfield: We reduced it by 50% last year, and we're trying to reduce that number—the scam reports number, at least—by another 50% this year.

It's going to be a very long fight against these scam compounds. We're in it to continue to represent...and take them down.

Doly Begum: Mr. Camfield and Ms. Curran, while I appreciate the ongoing effort you may have made, those in my community and people across Canada can't put food on their table. They can't buy groceries. They spend $50, $100, $200 or $300—a significant portion of their income—and come home with bags of groceries that are not enough to get through the weekend. Meta made, let's say, $6 billion because people were scamming. Meta allowed that. That's what I see, so I don't know what kind of effort you made, but you're able to take down articles that would inform people on how to be more informed and not be taken advantage of.

I don't have enough time. I have so many other questions about your community standards guidelines.

The Guardian reported that Meta is the “marketplace for predators”. You recently lost a case where children were being sold, and Meta was a top platform for that. Do you have anything to say there?

● (1735)

Rachel Curran: Look, these scammers are industrial-level organizations operating in jurisdictions outside of Canada, and they're targeting digital platforms across the spectrum. They're targeting telecommunications companies. We all get scam calls and scam texts constantly, every day.

I think it is really going to take a whole-of-industry approach to address these industrial networks and take them down. It's going to involve working with law enforcement globally—law enforcement in other jurisdictions—to address these industrial networks. They are not just targeting our platforms. They are targeting digital platforms across the board. They're also targeting our telecommunications companies.

Doly Begum: We had telecom companies, the banking sector and others here. They're making efforts. The difference I see here is that Meta is making billions of dollars by becoming a platform for scammers, for fraud, for other things like sextortion and for predators. To me, that's mind-boggling. We need to have much better mechanisms to tackle this. Right now, Meta is failing to do that.

Chair, I'll give the rest of my time to my colleague. Thank you very much.

Dominique O'Rourke (Guelph, Lib.): Thank you.

This topic has done what is challenging to do. I feel this committee is really galvanized around the issue. We're tired of hearing from constituents who have been scammed. We read about it in the newspaper every single day. The platforms are the conduits for this—platforms where they just want to share pictures of their grandchildren or catch up on news from friends around the world.

In December 2024, the U.K.'s Payment Systems Regulator stated that in 2023, Meta platforms were linked to “54% of the volume and 18% of the total value of [all authorized push payment] scams.” These are frauds that manipulate people and businesses. We're not talking a lot about businesses. We're not talking a lot about romance scams either, which are almost doubly devastating because they prey on people's loneliness.

Mr. Camfield, you said that you can identify fraud patterns, even in end-to-end encrypted messages. You said that you have impersonation protection and that we need to fight these industrial-scale networks. However, Meta is an industrial-scale global giant, so I'm really at a loss.

By allowing that volume of fraud on your platform, how are you not being reckless or a party to this misleading advertising? Are you doing enough with your scam prevention hub? Do you care about the people in those fraud centres who you say are perpetuating these crimes and about the people in our ridings who are being scammed?

Jon Camfield: The challenge with scams is that the victims truly are on all sides. All these stories of victims losing money to scams are horrific. The stories coming out of the scam compounds are also horrific.

We work in-region. We actually have an advertising campaign to intercept people looking for jobs, which is how they're often trafficked into these scams. We search-intercept, if people are looking for jobs, in the regions where they are most trafficked. We pop up and give this real-time information. Those pop-ups also direct people to the scam prevention hub for education.

Education is only one part of it. It really takes a lot of just-in-time messaging to get in front of people and prevent that engagement. It is a challenge.

Dominique O'Rourke: I would submit that the action that needs to be taken is to prevent those scams from being on your platform in the first place. Remove them and direct much more funding to scam prevention.

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

I'm going to take a few final minutes before we break into the next session, colleagues.

Ms. Curran, my questions will be for you.

The first is this: If a senior in my riding of Winnipeg South Centre were to lose their life savings in a scam that originated on Facebook, would you see yourself as being accountable for that loss?

● (1740)

Rachel Curran: I'll turn that over, MP Carr, to my colleague—

The Chair: The question is for you, Ms. Curran.

You are here before a—

Rachel Curran: —Jon Camfield, who's the expert on frauds and scams internally.

The Chair: No, you are here in front of a parliamentary committee, at our calling. I'm asking this: In the scenario where a senior in my riding loses their life savings to a fraud that occurred on your platform, do you, as the head of public policy for Facebook in Canada, see yourself as accountable for that loss?

Rachel Curran: I think we are accountable to reduce frauds and scams on our platform as much as we possibly can, working in collaboration with industry, with government and with law enforcement. I think that's our responsibility.

The Chair: Okay, so if that took place on your platform, you would say that it's partly your responsibility but partly the responsibility of the police.

Rachel Curran: I think the fraud attack chain, as my colleague Jon Camfield has described, occurs across a variety of players. It may start on Facebook. It may start with a telecommunications company or on SMS. It may continue to a bank transfer. I think Meta has a part to play in this fraud attack chain. Our part is to reduce the incidence of frauds and scams on our platform to the maximum extent possible.

The Chair: Ms. Curran, how much money does Facebook spend in Canada or globally per year on its investments around fraud prevention and scam prevention?

Rachel Curran: I don't know the answer to that question, but we can follow up with the committee.

The Chair: You do not know how much money Meta is investing annually to solve a problem that is costing Canadians billions of dollars.

Rachel Curran: I don't, but I can say that over the last decade, we have spent \$30 billion on safety and security on our platforms, and that includes frauds and scams.

The Chair: Do you worry that investment in fraud prevention will hurt your bottom line as a company?

Rachel Curran: Not at all. Listen, Meta does not want to be making money from frauds and scams. I think my colleague, Jon Camfield, can speak to that. We want our platform—

The Chair: But are you making money?

Rachel Curran: —to be a safe, pleasant place for our users, and that does not include having them scammed or defrauded on Facebook or Instagram.

The Chair: Are you making money off of fraud?

Rachel Curran: To my knowledge.... I don't know. I can't answer that question.

Jon....

The Chair: I'll allow Mr. Shipley, perhaps, as an expert in this field, to offer a quick view on that.

Rachel Curran: Well, Mr. Shipley seems to be offering stats from the U.K.—

The Chair: The question is for Mr. Shipley, Ms. Curran. The floor is not yours.

Rachel Curran: —which are not applicable to Canada.

The Chair: Mr. Shipley.

Rachel Curran: He also seems to be getting his statistics from U.K. media coverage, which—

The Chair: Ms. Curran, I'm going to call you to order. I know you have a long history in Parliament, Ms. Curran. Surely you're familiar with the rules of Parliament. As chair of the committee, I dictate who has the floor, and I'm going to provide Mr. Shipley with the floor for a moment. I'll return with one further question before we suspend.

The floor is yours, Mr. Shipley.

David Shipley: Thank you, Mr. Chair.

I would go back to a member's question from earlier when we were doing some calculations where the number was not \$16 billion but \$6 billion. That was from the percentages we heard, and we did the quick math. That was revenue. They made money off of fraud. They may not have wanted the money—I genuinely believe them—but they absolutely made the money.

There's one last point I want to make. I used to be a reporter. Our local media is gone in this country. We're deserts. The advertising revenue that used to support local journalism that didn't have page after page of fraud ads in it was eaten by companies like this. They've taken no responsibility for these deserts, but they offer them a pittance with this line about $300 million. They enable the theft of billions of dollars. It's an outrage.

Rachel Curran: Now we see Mr. Shipley's actual motivation, which is—

The Chair: Ms. Curran, you don't have the floor.

Rachel Curran: —to ensure news publishers get money from companies like Meta.

The Chair: You can cut the mic for Ms. Curran, please, at the moment.

Rachel Curran: Well, that is his real motivation. It's not—

The Chair: I'm going to ask for a bit of order here. Thank you.

My final question will be for you, Ms. Curran.

You've committed—and I appreciate that commitment—to providing the committee in writing through the clerk how much money Facebook has invested in Canada or globally on fraud prevention. I have a feeling that if members from political parties around the table don't receive that information in a timely fashion, they may be interested in raising that in other parliamentary platforms.

Assuming that you get that number back to us in a timely fashion, that the number is accurate and that it proves, once you've done your research internally...there's a second component we need. There are three things I'd ask you for. The first is how much money Facebook Canada is investing in Canada—or internationally if you feel that you can't dissect the two markets—on fraud prevention. Second, how much do you estimate you have earned from fraud or scams that have occurred on your platforms in Canada or internationally?

Then the third thing I'd like you to please provide to the committee would be this. If it turns out that the amount of money you have made—to Mr. Shipley's point, perhaps unintentionally—on your platforms through fraud ends up being more than what you've invested, which I suspect it is significantly, will you commit in writing back to this committee that you will invest the difference back into fraud prevention?

Those are the three things I would ask you to report back on, please, Ms. Curran, to the committee at your convenience.

● (1745)

Rachel Curran: Yes, we can absolutely do that.

I would say we have invested $30 billion in anti-fraud measures, safety measures and security measures on our platforms over the last decade. I would be very surprised if that number was less than what has been lost, unfortunately, to really tragic and unfortunate instances of scams on our platforms, but we will certainly report back to you on that.

The Chair: My final question, Ms. Curran, for you is this. Perhaps it's more of a point of reflection than anything regarding technical policy. It gets to a question my colleague Madam O'Rourke asked you a few moments ago.

I've been a parliamentarian for a number of years. I've been around Parliament for a very long time. I have never seen in my capacity as a chair or as a member of Parliament a set of witnesses receive as much unanimity across parties in relation to the subject line or content of the questions you have received today. I'd like you to offer a reflection on that. Why do you believe that Conservative, Bloc and Liberal members of Parliament are all taking the very precious time they have around a committee table to ask you the same questions, and why do you think they are responding, as we've seen from all sides around the political spectrum today, with an attitude that shows they seem to be less than satisfied in regard to the answers they've been receiving?

Rachel Curran: I think it is because this is a serious issue. It's a serious issue for Canadians. We ought to address it. I know you invited some of our colleagues here today, other members of the tech industry, who declined to appear, but we wanted to be here because this is an important issue.

We want to ensure that we reduce the incidence of frauds and scams in Canada. We want to make sure that our platforms are not a place where Canadians get defrauded or scammed. We want to engage with policy-makers like the members of this committee to ensure that we're working together to decrease the incidence of that. Honestly, Mr. Chair, that's why we're here.

The Chair: I appreciate that.

Mr. Shipley, Ms. Quaid, Mr. Camfield and Ms. Curran, thank you for availing yourselves of the committee today for an important conversation in regard to the role that a variety of different industry players and, of course, the citizenry and public policy-makers in Canada play in ensuring the health and well-being of all people across the country vis-à-vis the protection against fraud and scams. I appreciate your time.

Colleagues, I'm going to suspend for five minutes while we turn over to our next witness, who will be appearing online.

● (1745)

_____________________(Pause)_____________________

● (1750)

The Chair: We're going to continue our second hour.

Colleagues, please take your seats. We are running significantly over time, and we are going to do our best to squeeze in a good, solid conversation.

From the Australian Banking Association, we have Nicholas Giurietto. Sir, you're on the other side of the world and it's a different time of day. You have a full day ahead of you. We have a full day behind us, and we're looking to add a bit to it. Thank you very much for availing yourself of us. We certainly appreciate the deep bond and partnership between our two countries.

Sir, you're going to have up to five minutes. I know there's a lot of interest in what you have to say. This is only the second meeting we've held in relation to this study, but the Australian example has been raised on numerous occasions, and we look forward to understanding it a bit more through your testimony.

With that, the floor is yours for up to five minutes.

● (1755)

Nicholas Giurietto (Head of Future Policy, Australian Banking Association Inc.): Thank you, Mr. Chair.

Good evening, and good morning from Australia.

My name is Nicholas Giurietto, and I head financial crime policy at the Australian Banking Association. That's the main industry representative body for the banking sector in Australia. My area of responsibility includes AML-CTF, cybersecurity and scams, and I've been heavily involved in the development and now implementation of the Australian government's scam prevention framework. This has involved collaboration with government policy bodies, various regulators and colleagues from other industry sectors.

The unifying purpose of all of these stakeholders is a shared desire to keep Australians as safe as possible from the scourge of scams conducted by global organized crime gangs. Our approach is to work together to stop scams before they happen, not simply requiring one part of the scam chain to take responsibility for protecting or refunding customers. It's about acknowledging the complexity of our digital world by working together to stop scams at the source. The Australia scam prevention framework has attracted a lot of attention around the world as the first example of an anti-scams regulatory regime based on the principle that all industry sectors must do their share to tackle scams.

Going first is hard. There are many details to be worked through in translating an important simple policy proposition into real world implementation. That can be difficult in practice. Some of the challenges still remain to be resolved in Australia. Nevertheless, the early signs are positive, and we remain more convinced than ever that the only way to minimize the devastating harm that scams cause to everyday Australians is a coordinated cross-sectoral ecosystem approach with each industry sector doing their bit.

The scam prevention framework has two basic principles. The first is recognizing that sophisticated methods of a scam attack occur across industry sectors and indeed often deliberately exploit the gaps between them. The scam prevention framework requires all sectors in the scam chain to take appropriate action to prevent, detect and respond to scam attacks.

Each sector has a responsibility to harden their business processes against scammers with analogous but industry-specific obligations. For example, the requirement on banks to apply rigorous know-your-customer checks when opening an account is matched with an analogous obligation on telcos to check the legitimate business need for a SIM box capable of sending tens of thousands of SMS messages in an hour, or an obligation on digital platforms to confirm the bona fides of an advertiser of an investment product. The exact obligations are different, but the purpose for each sector is the same: trying to keep bad actors out of the system from the start.

In Australia, we have commenced the SPF rollout with the three core sectors: banks, telcos and digital platforms. This acknowledges the practical fact that you have to start somewhere. However, it's acknowledged that our national suit of armour against scams will not be complete until all other sectors that can be involved in a scam chain are also part of the coordinated response. These include crypto exchanges, non-bank money remitters, remote access software providers, online marketplaces, gift card providers and many more. Unfortunately, the ingenuity of scammers knows few limits, and it is of little comfort to a scam victim to know that the front door to their life savings has been kept secure when thieves have been able to climb in the window.

The second key principle of the SPF is cross-industry data sharing: facilitating the secure and privacy-compliant exchange of data that indicates a scam risk. Actionable scams intelligence, as it is described in the SPF legislation, is an essential tool in the anti-scam response.

Despite the best efforts of all participants, it is not always possible to protect the first victim from the scam, but the rapid exchange of actionable scam intelligence, followed by prompt action—for example, taking down a scam website or blocking a compromised telephone or bank account—can quickly close that vulnerability and protect the hundreds or even thousands of potentially subsequent victims. Scammers can continue to probe the defences, but by reducing their success rate and increasing the cost of their business model, we make Australia a less attractive target.

The most effective approach to deliver cross-industry data sharing is through private-to-private collaboration—for example, through the Australian Financial Crimes Exchange, which I understand will be providing testimony today—with appropriate linkages to law enforcement. The key role of government is to provide the policy framework that enables secure and privacy-compliant data exchange with appropriate safe harbour protections.

● (1800)

I will conclude my initial comments at this point and would be delighted to offer any further insights from our experience in Australia that the committee may wish to request.

The Chair: Thank you very much, sir.

I didn't ask, but where in Australia are you coming in from?

Nicholas Giurietto: I'm in Sydney.

The Chair: That's wonderful.

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

Michael Guglielmin (Vaughan—Woodbridge, CPC): Thank you, Chair.

Thank you to our witness for his opening testimony and for taking the time to come to us all the way from down under.

As we know at this committee, this is a very important and timely study. All of us have heard countless stories in our ridings about different circumstances surrounding fraud and about seniors who have been subjected to fraud.

I have a personal story of someone who, over a period of nine months, was scammed out of their entire life savings. It started as a technical scam and originated as something that popped up on their computer, and then it turned into a nine-month, long-drawn-out psychological scam. Someone thought they were dealing with the FBI and ended up forking over their entire life savings, with no accountability from any of the institutions that allowed this money to be turned over. Really, there was no recourse for this individual.

Australia is particularly important for us to hear from, because your prevention framework is described as having an ecosystem approach, one that recognizes, as you've said, that scams begin upstream, before the money ever moves. I was wondering if you could walk the committee through what that means in practice. Who's regulated? What obligations apply? How does the system link banks, telecoms and digital platforms in one single chain of accountability?

Nicholas Giurietto: The scams prevention framework legislation was passed by Australian Parliament in February of last year. The enabling regulation has begun to work its way through the system. The basic structure is that each key industry sector—the digital platforms, the telecommunications sector and the banking sector—have a set of obligations under the headings of “detect”, “prevent” and “respond to” scams. There are a few others, such as governance, but these are the three most important ones.

They are responsible to their sector regulator. In the case of the banking sector, our normal regulator, the Australian Securities and Investments Commission, is the regulator for us for scams. It's similar for telcos and their regulator, and the platforms have actually had to find a new regulator because until now there wasn't one.

Each of those sectors has code obligations that are managed by sector regulators. Across that, there's a new super regulator, if you like, that sits horizontally for the issue of scams across all sectors. Its role is to make sure that the obligations are joined up and equivalent.

In my opening statement, I made the comment that keeping bad people out of your system in the first place is one way to help protect your citizens. For banks, we do that through KYC and through telcos. If someone really wants to send 10,000 SMSes in a minute—and there are legitimate use cases for that—find out who they are. Is that a genuine use case? Don't let just anybody use that product. Similarly for the platforms, if someone wants to advertise a financial product, check that they actually hold an Australian financial services licence, which is the licence that's required to offer investment products in Australia, before you allow them to advertise their product.

The obligations are different for each sector, but they have the same flavour because they have the same purpose—

The Chair: I'm sorry, Mr. Giurietto. I thought you might have been done there.

Before passing it back to Mr. Guglielmin, I'm just going to say that another witness has joined us, David Pegley, who is the managing director of the Australian Financial Crimes Exchange.

Mr. Pegley, welcome. Unfortunately, we won't have time for you to provide introductory remarks.

However, colleagues, you are more than welcome to ask Mr. Pegley questions as a witness here today.

Mr. Guglielmin, there remain just over two minutes for you, sir.

● (1805)

Michael Guglielmin: Canada currently places the bulk of its obligations on banks, which see the fraud only after the money has actually moved. From Australia's experience, what happens if the government places that burden on banks while platforms and telecom companies have fewer obligations?

Nicholas Giurietto: The Australian ecosystem specifically makes all of those sectors, and future sectors, equally responsible for taking their share. If it's banks alone, you end up trying to stop the fire when it's already raging. There are things that banks can, should and must do to secure their platforms.

Particularly for the telcos and platforms, when they take action earlier, it's possible to intervene in scams earlier. The vital link here is sharing information across the sectors. When a bank becomes aware of a scam victim, if we can share that information with a telco or platform.... It is too late to help the first victim—that is true, and it's devastating—but at least the information can then be shared back to clean up the pipeline of future victims.

Over time, it makes it a more expensive proposition for the scammers to target Australia, as opposed to another country, so they might put their efforts elsewhere.

Michael Guglielmin: You noted that around 90% of scam losses in Australia come from individual losses exceeding $5,000 Australian. These are losses that the ABA describes as “life changing”. Who's experiencing those losses most acutely?

Nicholas Giurietto: The range of people who become subject to scams includes all of society. There's sometimes a stereotype that only the elderly become victims of scams. The reality is that scammers are brilliant psychologists, and they will find a way to get to just about everybody. It could be a parent dropping off their children at school and responding to a text message while they're trying to park their car. There are so many ways that they will do it, so there is no classic pattern.

Every citizen is a potential scam victim, and every citizen therefore needs some support to be protected from that.

Michael Guglielmin: Thank you.

The Chair: Thanks very much, Mr. Guglielmin.

We'll go to Madame O'Rourke now for six minutes.

Dominique O'Rourke: Thank you, Chair.

Mr. Giurietto or Mr. Pegley, the government currently has legislation before the House on lawful access, which would enable law enforcement to have more access to platforms in order to rapidly intercept crimes. They could be scams. They could be human trafficking.

I wonder if you can tell us how important Australia's lawful access has been in helping you tackle fraud.

Nicholas Giurietto: I might let David take some of this, but engagement with law enforcement is an absolutely vital part of the overall scam and fraud response. Like Canada, Australia has a federal system with overlapping police responsibilities that can sometimes make things a bit complicated to navigate, but being able to do the intelligence sharing and take action—either sharing the intel or, in some cases, supporting law enforcement in taking action—is very important.

Private-to-private data sharing is at least equally important, in that sometimes the private sector can use so-called scam signals that fall short of the legal standard that law enforcement might need to meet before they can initiate a prosecution or some other action. It's simply information that can be shared to say, “Watch out for this; there might be some possibilities here to take action” and flag a risk. That's very important as well. The two can operate together.

Dominique O'Rourke: Do you want to add to that quickly? I have two other questions.

David Pegley (Managing Director, Australian Financial Crimes Exchange Ltd.): Sure. Thank you for the opportunity.

I'll add to Nick's comments that in our experience, the prevention and detection side of our work invariably means that we're ahead of the crime or in the process of the crime. We've found that—

The Chair: Mr. Pegley, I'm going to intervene for a moment. Actually, this is for both witnesses. It's really important that we get the proper positioning for the microphone.

We're going to try that again with you, Mr. Pegley, to see if it's working. We'll perform a really quick test before you continue.

I'll pause the clock, Madame O'Rourke.

● (1810)

David Pegley: Does this work? Is this a better position?

The Chair: Could you raise the arm bar on the microphone a bit higher? Try that.

David Pegley: Thank you.

While we share intelligence among private sector participants, we also have formal relationships with all state and federal law enforcement agencies. This enables them to task us with operational information to support their work, which is usually after the fact. Invariably, we focus on trying to share consumer-based information as rapidly as we can across the ecosystem. After the fact, law enforcement agencies are very keen to get the mass data to support their operations work. Invariably, the crime is after the fact.

Most of the crime we've come across is offshore, unfortunately. There is some domestic money mule activity that has been identified and some SIM box work, which Nick was talking about earlier. However, invariably most of the bad actors affecting the Australian community are international.

Dominique O'Rourke: I have a couple of things. Can you remind this committee of the results you've seen in Australia in just one year following the introduction of your new framework? How have the platforms responded in Australia? How key is awareness for customers to know that it's difficult to recover funds?

Nicholas Giurietto: There are a few pieces there.

The scams prevention framework legislation passed, but it is still in the process of implementation. It's actually a bit too early to say what the direct impact of that legislation will be, although even announcing the scams prevention framework had a positive effect in terms of encouraging collaboration between the sectors.

We have seen a reduction in scam volumes. The numbers are, unfortunately, a little difficult, because there are multiple sources and there are some legitimate questions about the best way to count them. Probably, the worst description would be that they're flat, and every other option is better than that. There is collaboration among the sectors.

We have managed to do some significant pilots at this stage with the platforms. Information has been shared from banks back to the platforms, which have been able to use that information to take down scam content. As the SPF rolls out and comes up to industrial scale, we expect to see it become an even bigger driver of a reduction in scam losses.

Dominique O'Rourke: Thank you.

The Chair: Thank you very much, Madame O'Rourke.

[*Translation*]

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

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

Hello to the two witnesses joining us today. We're glad to have them here.

Mr. Pegley, you didn't have time to give your opening remarks. If you're like to do it now, you can have my question time. That will give us a chance to hear the message you want to convey to us.

[*English*]

The Chair: Mr. Pegley, did that work? Could you hear that?

David Pegley: Yes, in French.

The Chair: Okay. I'll translate it for you. We'll get that fixed.

Essentially, Monsieur Ste-Marie was saying that you did not have an opportunity at the outset to provide opening remarks, and he would be happy to provide you with some time during his question period to have you offer an opinion.

David Pegley: Thank you.

Perhaps I should briefly describe what the Australian Financial Crimes Exchange does, which is mainly to support the work that the ABA and other industry bodies are doing. We provide intelligence sharing across multiple industries. At the moment, we have something like eight different industries that we share intelligence across. We have around 100 different members with which we share intelligence in Australia. We also support, separately, the sharing of intelligence among New Zealand banks for the same purpose.

Those industries range from digital media, telcos and insurance companies to obviously banking, telecommunications companies and digital currency exchanges for the purposes of all three parts of, as Nick described, the SPF regime. In the prevention framework, we'll take information from a victim and share that with the relevant digital platform exchange, or we'll share it with the telecommunications company. This has been a very successful way of rapidly taking down in real time the bad attributes that float around the community. We'll also share intelligence that enables the detection of transactions in bad bank accounts or digital currency regimes that have been used to exfiltrate funds, therefore harming the economic benefit to the criminals.

We also support tracking—and hopefully stopping—the funds among institutions in real time to enable, as best we can, the recovery of funds for victims on their behalf across the banking sector. That's a fraud reporting exchange that enables everything from digital currency exchanges before currency is transferred from fiat to digital...and in the banking sector to try to stop the funds from flowing, because they will move very quickly offshore from Australia.

● (1815)

The Chair: Mr. Pegley, at the bottom of your screen, there should be an opportunity to switch to the English channel. That should solve our translation problem. If it doesn't, that's okay. I'll translate for you.

[*Translation*]

Mr. Ste-Marie, the floor is yours.

Gabriel Ste-Marie: Mr. Pegley, can you let me know if you have access to the interpretation?

The Chair: I don't think he does, Mr. Ste-Marie.

You can still ask your question, though. If I don't interpret it exactly right, you can correct me.

Gabriel Ste-Marie: Great.

When the new model was put in place, what challenges did you encounter? What feedback did you get from companies?

[*English*]

The Chair: Mr. Pegley, did you hear that?

David Pegley: Yes, I did. Thank you.

The Chair: Good. Please go ahead.

David Pegley: Probably the most interesting aspect of the model of the three sectors is identifying relevant attributes to be shared between those sectors. What is useful for a bank to use to detect fraudulent transactions is not the same as it is for a telco. A digital currency exchange has a very different way of tracking transactions. Digital media platforms are not used to tracking transactions in that way at all. We've worked very hard to identify the relevant attributes to be shared and the intelligence to be shared among the platforms.

An interesting aspect is that in many cases, these industries don't necessarily work together very often on common issues. Digital platforms are invariably very strong competitors. Telcos are pretty much the same. The idea that they would collaborate together is a foreign concept.

A lot of the work we're doing is in trying to build trust between parties when we're sharing intelligence and to identify the bad actors, if you like, as the rationale. The banking environment is much more familiar with collaboration around this activity. It has been for years, so that part of the picture has been much easier. The translation, if you like, among the different sectors of different intelligence that will help them stop the scams has been an effort, but we are getting there.

[*Translation*]

Gabriel Ste-Marie: Thank you very much.

Thank you, Mr. Chair.

The Chair: Thanks very much.

Since we're running behind, I'm going to cut the last round a few minutes short.

[*English*]

Mr. Falk, you'll have two and a half minutes, followed by Mr. Ma, who will have two and a half minutes. Then we are going right into a brief suspension, followed by time in camera to get to the report that we still have to get through today.

Mr. Falk, the floor is yours for two and a half minutes, sir.

● (1820)

Ted Falk: Thank you.

Thank you very much for your testimony here this afternoon, or morning—whatever it is where you are.

What have you found to be the most effective part of the legislation to combat scamming?

Nicholas Giurietto: I would say the most effective component of the legislation is the fact that it frames the responsibilities of each sector as equivalent but different. What I mean by this is that it acknowledges that each sector, because of the technological way they operate, the business model, etc., inevitably has different capabilities and different responsibilities. Some of that goes to the data issues that David was talking about.

The overarching idea that there is a responsibility to work to prevent, detect and respond to scams—those three labels—becomes really important. Working in the banks, I can look at the obligations of the telcos and the platforms and can ask what they are doing to prevent scams and what we are doing. Is it roughly the same? Are we trying to do the same sorts of things? What are we doing to detect scams? Particularly in the data-sharing space, that's very important. Is the data we're providing helpful, and what is the response?

It's about having an overarching framework that cuts across regulatory silos, because historically, each of those sectors has been regulated in its own silo. The sector has its own regulator, and they don't always work together outside of those vertical boundaries. Forcing discussion not only at the industry level but also at the regulator level—across the silos—is probably the foundational thing that is of greatest benefit in the scam prevention framework.

Ted Falk: Have you found that the social media platforms have also been co-operative?

Nicholas Giurietto: They are working with us on a number of the initiatives in the framework. It's fair to say that they had a longer journey to take and perhaps have a little further to go, but at the moment, the impetus of the legal obligation is encouraging collaboration, and we are working with them on a number of fronts to make that collaboration real.

Ted Falk: Thank you.

The Chair: Thanks very much, Mr. Falk.

Mr. Ma, the floor is yours. You have two and a half minutes, sir.

Michael Ma: Thank you.

Thank you, gentlemen, for coming on short notice.

Obviously, I applaud the Australian model, and we've seen some successes. Despite these successes, there are still vulnerabilities that exist in addressing financial fraud within the Australian banking system. For example, according to the Consumers' Federation of Australia, scam losses for first nations people increased by more than 70% to $6.5 million. This raises a bit of a good faith concern about equity.

If we were to apply Australia's model to the Canadian context, why does this disparity exist?

Nicholas Giurietto: I think I made the observation earlier that there is a scam for everybody in society, and the scammers are brilliant at targeting the attributes and vulnerabilities of every community.

As a different example, many of the people who came to Australia from Vietnam or China will be victims of scams where people pretend to be from the legal authorities of those countries. For first nations people, there's a particular challenge around what we call “scambling”, which is a type of scam that looks like an online game. They become quite popular among the communities. The main intervention there, which banks take very seriously, is community education to explain that what looks like a way to entertain yourself and perhaps earn a little money is in fact a scam.

One of the challenges is that the boundary between legal and illegal gambling is not always clear, so working with regulators to make that more precise is also important. I think your broader point is that everyone in society is susceptible to some type of scam, and education is one of the key tools to assist with that to make sure that people are aware of how they are being targeted by scammers.

Michael Ma: How can Canada build on Australia's success while ensuring that no community is left behind?

Nicholas Giurietto: I think broader success comes from an ecosystem type of approach of sharing responsibility among all of those players. I know a lot of the focus at the moment is on banks, telcos and digital platforms, but there are other sectors that play a critical role. They also need to be included to make sure that no one is left behind.

The best way to do this is to be smart about the use of data. We are working to improve the quality of the data that tells us who has been scammed, what type of scam it is, what the demographics are, etc. If we can use that data well, we can understand much better the specific nature of the scam, the target and how it's implemented. That allows preventative measures, education measures or whatever else to be focused.

A general “be careful of scammers” type of message works for only a few months—if it works at all—and then it becomes background noise. You need a targeted message around specific scams, based on data.

● (1825)

Michael Ma: I think my time is up.

The Chair: Thank you, Mr. Ma.

Gentlemen, thank you very much for appearing here today. I know it felt a bit short, but we actually had a much smaller panel than we typically would, which means we probably got more questions in than we otherwise would have, which is great.

I would encourage you, as best as you possibly can, to keep tabs on the next few meetings this committee is undertaking in relation to the topic at hand. If there are things you're seeing that you think would be a mistake for the Government of Canada to do or things that you would applaud in terms of next directions based on the experiences you've had in Australia, we would certainly welcome that feedback, as you're not only an ally, but clearly leaders in this field in your respective jurisdictions.

Gentlemen, thank you. We wish you a very nice rest of your day in Australia.

Colleagues, we are going to suspend briefly.

[*Translation*]

Mr. Ste-Marie, we're going to send you a new link.

[*English*]

We are going to take a five-minute break as we turn over, and then we'll get back to work.

We are suspended.

[*Proceedings continue in camera*]