HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

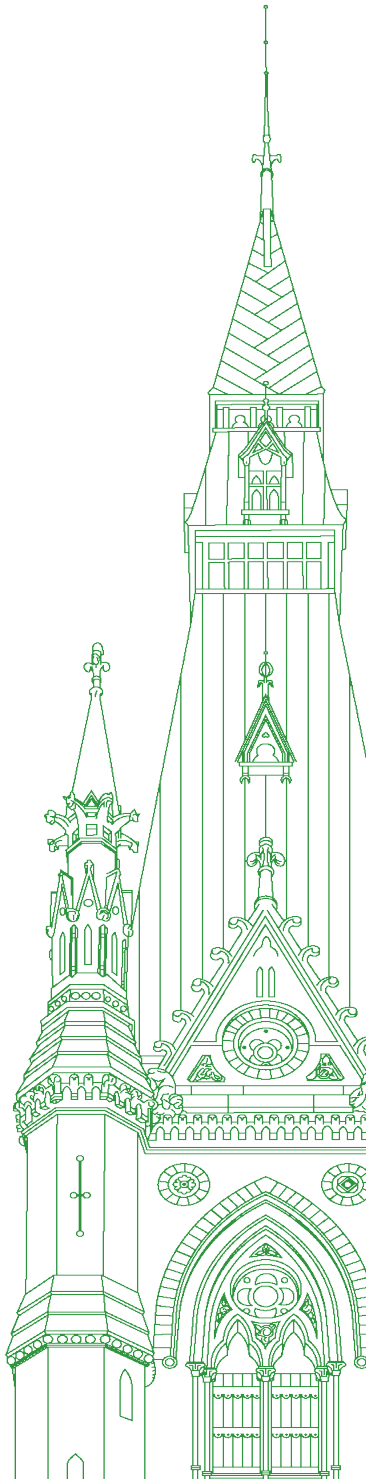
# Standing Committee on Industry and Technology

EVIDENCE

**NUMBER 046**

**PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT**

Tuesday, June 16, 2026



Chair: Ben Carr

# Standing Committee on Industry and Technology

**Tuesday, June 16, 2026**

● (1530)

[*Translation*]

**The Chair (Ben Carr (Winnipeg South Centre, Lib.)):** I call the meeting to order.

Good afternoon, everyone.

[*English*]

We are continuing with our study on fraud. We'll conduct one more meeting after this one. That will take place on Thursday, as discussed at our meeting yesterday.

To start, I have a couple of housekeeping things.

For witnesses who are in the room with us, this is a little reminder that if you are relying on your translation piece and it's plugged in but not on your ear, place it on the sticker in front of you. That's to protect the health and well-being of our interpreters.

[*Translation*]

I can confirm that we carried out all the tests to verify that the audiovisual equipment is working properly.

[*English*]

Colleagues, my calendar says—it could be wrong, depending on what's going on in the House—that there's a possibility for us to have bells at the outset of the meeting. As you know, I require unanimous consent in order to work through the bells. I'll circle back to each member on the committee if and when that occurs. This is just a quick heads-up for you to please give that some thought. If I don't get unanimous consent, we'll have to pause for half an hour. That will be the decision we live with. I'll come back to that if and when it's necessary.

We have a number of witnesses with us today. First, from the Canadian Radio-television and Telecommunications Commission, the CRTC, we have Steven Harroun, vice-president, compliance and enforcement; and Scott Hutton, vice-president, consumer, analytics and strategy.

Gentlemen, welcome.

From Desjardins Group, we have Bernard Brun, vice-president, government relations; and Frédéric Lapalme, senior director and deputy head, fraud and financial crime management and supervision unit. They are joining us by video conference.

From Interac Corp, joining us in the room is Mark Hines, who is the head of fraud—not of fraud, but of fraud product.

It's probably an important distinction to make, Mr. Hines.

On that note, why don't I turn to you first?

Witnesses, you will have up to five minutes for an opening statement, following which we will turn to members around the table for a question and answer period.

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

**Mark Hines (Head of Fraud Product, Interac Corp.):** Good afternoon, and thank you, Mr. Chair and members of the committee.

As the chair said, my name is Mark Hines. I lead fraud product at Interac. Thank you very much for the invitation to take part in today's study.

I'd like to begin by acknowledging that we're gathered on the traditional unceded territory of the Anishinabe Algonquin nation and by recognizing the enduring presence of first nations, Inuit and Métis peoples.

Interac is a Canadian-owned payment and digital verification company. Nearly 300 financial institutions connect to our networks, and Canadians use our products more than 20 million times every day. We sit at the centre of how money moves in Canada, which gives us a unique system-wide view of fraud and of financial crime in particular. Our teams monitor the network around the clock, sharing signals with financial institutions so they can act on suspicious activity in real time.

I'd like to use my time today to explain what has changed about fraud, why it's harder to fight than it used to be and where the greatest opportunity lies for protecting Canadians.

Fraud and scams are serious and growing threats. Behind every scam is someone who has lost money and often their confidence with it. However, the nature of the threat has evolved. Historically, fraud defences were built around the sender because the main threat was unauthorized access to an account. Scams work differently because the genuine account holder is authorizing the payment. This moves the focus to the receiver side of the network and requires new capabilities and investment across the system. At the same time, AI has dramatically increased the velocity of scam attempts. It's not just that they're more sophisticated and convincing. They're now automated at scale and only need to catch someone off guard once to be successful.

The most important thing I want to get across to the committee is that this problem cuts across multiple industries and sectors. We at Interac are investing heavily, but taking the next step requires a coordinated approach.

Interac deploys anti-fraud and scam capabilities on e-transfer today, and we have invested heavily in being the first approved fraud provider on Canada's new real-time system. Unlike other jurisdictions, we will launch the RTR with fraud protections built in, with the goal of preventing the spike in scams that other countries have encountered. This means Canadians will have greater levels of protection from day one.

No single company or sector can solve this alone. Fraud does not start and end in the same place. It often begins with a phone call, a text or an online scam. By the time the money is moved, the institution completing that transaction often has the least visibility into how it began. The key metric is the time between detection and intervention. The faster a trusted signal reaches the right place, the more often an institution can act before the money is gone.

We see the government's work to develop a national anti-fraud strategy and establish a financial crimes agency as an important step. Enforcement matters, but enforcement acts after harm is done. It needs to be paired with the coordination that prevents harm in the first place—that prevents money from leaving Canadians' bank accounts.

That's why the single most effective step Canada can take is enabling better data sharing across sectors, including financial institutions, telecommunications providers, digital platforms and law enforcement. To be clear, it's not about pooling data in a single open utility. It's about targeted, risk-based signals that let institutions act on the right information at the right time. This is a prevention-first approach, which is where we believe the greatest opportunity lies for Canada.

Thank you. I look forward to your questions.

● (1535)

**The Chair:** Thank you very much, Mr. Hines.

I'm not sure who is speaking for the CRTC. Is it Mr. Harroun?

Okay. The floor is yours, sir.

**Steven Harroun (Vice-President, Compliance and Enforcement, Canadian Radio-television and Telecommunications Commission):** Good afternoon.

Before I begin, I would like to acknowledge that we are gathered on the traditional unceded territory of the Algonquin Anishinabe people.

I am joined this afternoon by my colleague, Scott Hutton, vice-president, consumer, analytics and strategy.

Thank you for the opportunity to appear before you as part of this study on financial fraud and scams in Canada.

As you know, the CRTC is an independent quasi-judicial tribunal that regulates the Canadian communications sector in the public interest. We hold public consultations on telecommunications and broadcasting matters, and we make decisions based on the public record.

The CRTC is also part of a broader federal effort to address unwanted telephone calls, emails and text messages. In this context, we administer civil regulatory regimes. Because the CRTC does not have the mandate to assess or investigate conduct that may be criminal in nature, we encourage Canadians to report suspected fraud to the appropriate law enforcement authorities. In limited circumstances, we may share information with those authorities in accordance with applicable legal and privacy requirements.

● (1540)

[*Translation*]

Today, I'll touch on our civil roles under both the unsolicited telecommunications rules and Canada's anti-spam legislation. Under these regimes, we help protect Canadians by setting clear rules, helping businesses follow the rules, addressing non-compliance through enforcement and educating Canadians.

Regarding unwanted telephone calls, the Canadian Radio-television and Telecommunications Commission administers the national do not call list. Canadians can enter their telephone number on the list for free. In recent years, we've put in place a robust strategy to prevent unwanted calls from reaching Canadians in the first place.

Since this is a complex and ever-evolving challenge, there's no single solution. Instead, our approach combines both regulatory and technical measures.

[*English*]

For example, telecommunications service providers are required to block calls that display numbers that would not normally be dialed, such as 123-456-7890. Providers also offer call-filtering services, giving Canadians greater control over the communications they receive.

We are also taking action on caller ID spoofing, where the caller disguises their phone number from the person receiving the call. To address this, we required service providers to implement STIR/SHAKEN. This technology helps verify whether a call is actually coming from the number displayed on the caller ID screen, making it easier for Canadians to identify which calls can be trusted.

New technologies are also playing an increasing role. Artificial intelligence, for example, can be a useful tool. In 2021, the CRTC approved an application by a Canadian telecommunications service provider to implement an AI-based solution that can stop suspicious calls in the provider's network before they ever reach Canadians. Billions of these calls have already been blocked to date.

Let me now turn to the CRTC's role under Canada's anti-spam legislation, or CASL. We work alongside the Competition Bureau and the Office of the Privacy Commissioner to promote and monitor compliance within CASL. We also raise awareness to help Canadians better protect themselves and reduce the effects of spam. We collaborate with partners and stakeholders in this effort.

In closing, the CRTC will continue to work within its mandate to help protect Canadians from unwanted calls, spam emails and text messages.

Thank you for the opportunity to appear before you. We are happy to take your questions.

**The Chair:** Thank you very much, Mr. Harroun.

[*Translation*]

The next witness is Mr. Brun.

[*English*]

The floor is yours for up to five minutes.

[*Translation*]

**Bernard Brun (Vice-President, Government Relations, Desjardins Group):** Thank you, Mr. Chair.

Members of the Standing Committee on Industry and Technology, on behalf of the Desjardins Group, I would like to thank you for the invitation.

My name is Bernard Brun. I'm the vice-president of government relations for the Desjardins Group. I'm here with my colleague, Frédéric Lapalme, senior director and deputy head of the fraud and financial crime management and supervision unit.

It's a privilege to contribute to your study on financial fraud and scams in Canada, a key concern for Desjardins. Remember that Desjardins currently has over $524 billion in assets and over 10 million members and clients across the country. We serve close to half a million businesses—ranging from small and medium-sized businesses to large organizations—across all sectors of the Canadian economy. We're the largest co-operative financial group in North America and the eighth-largest financial group in the world.

Fraud is now one of the most widespread, sophisticated and damaging forms of economic crime in Canada and abroad. Fuelled by the digitalization of the economy, artificial intelligence—as my colleagues said earlier—and global access to digital platforms, the problem is evolving at such a rapid pace that public and private institutions can hardly keep up.

Fraud has become a low-risk and highly profitable crime. Criminal networks now operate with greater capabilities, without geographic boundaries. They use digital technologies, cryptoassets and even artificial intelligence-powered impersonation capabilities.

A number of structuring challenges are currently limiting the effectiveness of fraud prevention efforts. I'll list five of them. These challenges are the fragmentation of data and information-sharing mechanisms; the increase in regulatory initiatives and compliance frameworks; the transnational nature of criminal operations; the consequences for victims; and the ability of fraudsters to adapt quickly and their growing use of artificial intelligence.

In this environment, every improvement in security quickly leads to the emergence of new workaround strategies. This dynamic creates an ongoing technological race. This places significant pressure on governments, but also on financial institutions and businesses. The impact goes far beyond monetary losses. Victims frequently report long-lasting consequences, such as psychological distress, loss of trust in institutions, social isolation and compromised personal financial security.

As a Quebec-chartered financial group, most of our oversight comes from the Quebec government and agencies. However, we operate across Canada. This gives us experience and insight into the importance of coordination and regulatory complementarity in achieving tangible results.

We're pleased to see the federal government's commitment to encouraging the various stakeholders to work together to combat financial fraud. The many stakeholders working to reduce incidents of fraud must be brought together. This specifically goes hand in hand with the work of the Canadian Anti-Scam Coalition, of which Desjardins is an active member.

Last April, we submitted a brief to the Department of Finance in response to its consultation on the national anti-fraud strategy. We would be happy to share this brief with the committee if it would help with your work.

In conclusion, if we had to prioritize a single action to effectively combat financial fraud and scams in Canada, we would first focus on facilitating a form of information sharing among regulated organizations in order to improve prevention and detection.

With this in mind, yesterday we saw the introduction of Bill C-36. This bill seeks to strengthen privacy and to amend the Personal Information Protection and Electronic Documents Act. The text notably includes an exception to the consent requirement in order to make it possible to share information for the purposes of preventing, detecting and reducing fraudulent activities. In our view, this positive development should be pursued and carefully analyzed in order to align and coordinate efforts with the provincial legislative frameworks.

Thank you for your attention. My colleague and I would be happy to answer your questions.

● (1545)

**The Chair:** Thank you, Mr. Brun.

[*English*]

Colleagues, we're going to get into our first round of questioning.

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

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

Thank you to the witnesses for their opening testimony today.

Mr. Hines, a recent survey done by Interac showed that 79% of Canadians believe AI is making scams more convincing and making it much easier for fraudsters to create these scams in the first place. How specifically would you say that AI has changed the landscape over the last two years?

**Mark Hines:** I won't dwell on the sophistication point so much, because my guess is that the committee has heard a lot about that. What I would really emphasize is the velocity, which means not only the speed but also the volume of suspicious activity that hits both individual institutions and networks. What that means is that the likelihood that you'll catch somebody....

A busy parent opening the front door sees a link and clicks it without taking the extra 30 seconds. A grandmother who's worried sends money to a grandchild. It simply statistically increases the likelihood that these things are happening. That really is the other element that we don't focus on enough, in my opinion. I don't mean to underplay the sophistication element, because it's real, but that's the element we don't focus on quite enough.

● (1550)

**Michael Guglielmin:** Are there any scams in particular, as you guys look forward, that you're concerned with more than others?

**Mark Hines:** We break down the types of scams that we encounter on our network. I would say that by a country mile, the most prevalent kinds are investment scams. There's a range of scams, including romance scams and bank impersonation scams, but investment scams are by far and away the highest frequency that we see.

**Michael Guglielmin:** Would you say that in Canada our fraud prevention systems across banks, payment systems, telecom platforms, etc., are keeping pace with this new sophistication and the velocity of scams, or do you see a gap there?

**Mark Hines:** From my perspective, I see people investing large amounts of money to try to keep up. Our view, to really get the most out of that significant investment, is to have cross-sector data sharing. To use scams as an example, they will occur entirely outside of the network that we operate. We don't know where it started. We don't know the details around how it started. Our ability to react is limited.

If I may, I have one more detail that I think might be useful to the committee. With scams, often it's not the initial sending that you will catch. It's my account. It's when you see payments collecting at the other side that you begin to see a problem. Feedback loops that give you a greater insight to that other side of the network are the things that really would stop us pushing the money out in the first place.

**Michael Guglielmin:** What type of investments is Interac making to help prevent some of these scams that are AI-generated?

**Mark Hines:** We are in the middle of a three-year strategy cycle at Interac. We're investing a very large amount of money over those three years. The focus of those investments is in building the new system for the RTR. On e-transfer, when it migrates to the RTR clearing and settlement system, we will also significantly upgrade that system to have comparable controls.

It's a major institutional investment for us, at the moment.

**Michael Guglielmin:** When you look out at the broader ecosystem, across banks and other platforms, would you say that every sector is moving along at the same pace or are some falling short?

**Mark Hines:** I think there is variation, for sure. In particular, I think you see that financial institutions and payment networks of all types, not just ours, are investing, because that's where the monetary losses are happening at the moment. Again, to return to my point, broadening that spectre and requiring other parts of the ecosystem to have skin in the game in this fight is for us a key element.

**Michael Guglielmin:** Thank you very much.

I have a few questions for Desjardins.

In 2019 data was stolen from your members. It was found circulating underground on criminal forums as recently as November 2025, more than six years after the breach. Are you guys actively monitoring for your members the stolen data on the dark web?

[*Translation*]

**Frédéric Lapalme (Senior Director and Deputy Head, Fraud and Financial Crime Management and Supervision Unit, Desjardins Group):** Thank you for the question.

I won't go into the details of the 2019 incident, since Desjardins has commented on it publicly many times. That said, we invest hundreds of millions of dollars every year to combat fraud and ensure data security. Our security office has 1,800 security experts.

Regarding the data circulating on the dark web, we do indeed monitor this information for our members. We've introduced a number of protection systems since the incident. We've recently introduced certain protections related to the dark web. These protections have been added to our scope of coverage. We understand that our members and clients have concerns about the data found on the dark web. We're addressing these issues in a very targeted way.

[*English*]

**Michael Guglielmin:** When you guys find data, what can be done with it? Can you have it removed from the dark web, or does monitoring it just mean that you're watching it spread?

[*Translation*]

**Frédéric Lapalme:** It's extremely difficult to remove data from the dark web, or even from the Internet. Once it's on the Internet, it's in the public sphere.

There's another point to consider. While the exact number may remain a matter of debate, hundreds or even thousands of data breaches have occurred. Unfortunately, in general, Canadians and Quebeckers have been victims of multiple data breaches on multiple occasions. This doesn't let Desjardins off the hook. I can assure you that we take this extremely seriously. However, the data is found at multiple levels.

This can be useful for fraud, especially for scams, in particular the fake official scams. In these scams, a fraudster pretends to be a police officer or an employee of a financial institution. The fact that these officials can access certain information helps build trust with the potential victim. When we answer the telephone and the person on the other end already knows a number of key details, it creates a sense of trust in the fake official. It gives the official a certain amount of credibility. That's my answer.

● (1555)

[*English*]

**The Chair:** Thank you, Mr. Guglielmin.

Mr. Ma, I understand you might be splitting your time with Madam O'Rourke. I'll let the two of you figure that out. Between you, there are six minutes.

The floor is yours.

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

Thank you, gentlemen, for being here today.

My first question is for the CRTC.

The government has announced the creation of a new financial crimes agency. What opportunities do you see for stronger coordination among telcos, regulators, law enforcement, financial institutions and this new agency in disrupting the fraud network?

**Steven Harroun:** As you heard from many witnesses over the course of this study, that collaboration is key. Even today, all of my colleagues suggested the same thing. I think the new Canadian financial crimes agency will be exactly where you can get TSPs, banks and others in the room to combat this activity.

That's the biggest challenge we see at the CRTC—making sure everyone is speaking to one another. Everyone, I would suggest, is doing their part to keep abreast. That collaboration is key.

**Michael Ma:** Thank you.

Before I pass it on, my next question is for Interac.

Mr. Hines, you talked about the importance of data sharing. What sort of data are we looking at, and how timely is it? Quite often, these procedures are more afterthoughts than help in preventing fraud. I'd like to hear what you have in mind, in terms of that data sharing.

**Mark Hines:** Absolutely. If it's helpful, I can give you as an example a scenario with the data element.

A scam appears on a digital platform. The user clicks on it. They're taken to a chat, where they're encouraged to invest in an investment scam. If the digital platform or the telecommunications company identifies this as suspicious activity, they could share on a network the link and the telephone number associated with the chat. When it hits a payment system, we would be able to identify it as an element that goes into our magic sauce. What that would do is allow me to correlate whether the destination for this scam payment is associated with a scam that happened off my network. It would mean I don't let the payment go. We would advise our FI, “Please don't send this payment because we think there's a high risk the destination is a scam.”

It's those types of pieces of information that can have a large impact if we have them before we process the payment.

**Michael Ma:** Thank you.

My very last question is, do you believe public awareness and education will help?

**Mark Hines:** It's a great question.

What I will say is that scammers focus on the most vulnerable, so education, while very important, has limitations in terms of how it can protect those particular populations. This is why Interac's position is that responsibility is broader than that. It's on all of us who play a role in the example I just gave.

**Michael Ma:** Thank you.

I'll pass it on.

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

Mr. Hines, I think it's fascinating that you said, “The key metric is the time between detection and intervention.” We heard in Wealthsimple's testimony that they found 1,500 fraudulent uses of their logo and deepfakes of their CEO in one day, yet it took the platform, Meta, four days to take these down.

Do you think the platforms are doing enough?

**Mark Hines:** I think that the platforms have to be part of the solution. Whether or not they could take them all down is not the point. The point is that, by giving us those signals as they take them down, each of those data elements significantly increases our chances of stopping the money moving, which is the point at which Canadians are harmed.

Our approach from a responsibility in the ecosystem is that every player should have clearly articulated obligations, and that responsibility for it flows from meeting or not meeting those obligations, and we would include ourselves in that.

● (1600)

**Dominique O'Rourke:** I think it's helpful that you told us that investment scams are far and away the most prevalent, because sometimes we frame them as an issue about seniors who may not be tech-savvy. We hear that the sophistication of the scams is increasing. We hear that only 5% to 10% of scams are being reported. Clearly investment scams are high as are romance scams in addition to all kinds of scams that target seniors.

You said that the most effective measure is cross-sector data sharing. Can you outline for me what some of the privacy considerations are? Ontario still has never really realized e-health. Can we get to that cross-sector data sharing fast enough? What do you need in terms of legislation, or what's your recommendation?

**Mark Hines:** When I talk about data sharing, what I mean very specifically are very specific data elements that are shared between very specific parties. I think there are two elements from a legal perspective to focus on. One of them was mentioned earlier about having a clear basis to process data for fraud. That exists in PIPEDA today.

My experience with negotiating data-sharing agreements as an FI at a fintech and now at Interac has been that we focus very much on consent as the core of our focus, and that re-emphasizes that grounds to process data is important.

The other one is around safe harbour provisions for that intelligence sharing. They exist in other jurisdictions for financial crimes sharing. Why I think it's so important is, in my experience that I just mentioned, our participants really take very seriously their responsibility for data, and they will only share it if they feel the risk is low or acceptable. That safe harbour provision encourages the type of intelligence sharing that we think is key if we're going to stop the problem at the outset.

**Dominique O'Rourke:** I'm out of time. Thanks.

**The Chair:** Thank you, Ms. O'Rourke.

[*Translation*]

Mr. Ste-Marie, it's your turn. You have the floor for six minutes.

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

I would like to extend my greetings to all the witnesses. Thank you for being here.

My questions are for the representatives of the Desjardins Group. I would like to hear more about restrictive or contradictory legislative frameworks.

**Frédéric Lapalme:** Thank you for the question.

My colleague, Bernard Brun, talked about this. We operate in Quebec, but also across Canada. When it comes to privacy, the difference between federal and provincial legislation poses a challenge. As a financial institution, we want to participate in anti-fraud initiatives. Our colleagues work for organizations under federal jurisdiction—and thus subject to federal legislation—while we operate at the provincial level. We need to analyze and identify discrepancies to ensure that we participate in this type of information-sharing initiative according to the rules. We must carry out a great deal of internal paperwork and many assessments to ensure that we're taking the correct approach. Of course, in cases of rapid fraud, this process doesn't fit within the specific time frame required for an anti-fraud initiative.

**Gabriel Ste-Marie:** When it comes to combatting fraud, you would like the stakeholders involved to share more information. Can you elaborate on this?

**Frédéric Lapalme:** It's a good point. Mr. Brun touched on this. It's the key point. The Desjardins Group handles billions of dollars for its client members and processes millions—even billions—of transactions each year. We must be able to share this information with Interac and our colleagues at the banks to ensure that we use this data wisely to combat fraud. Since transactions now take place in milliseconds—given the advent of real-time transactions—we'll face limitations. We must be able to use this data both internally and with our colleagues so that we can implement the right guidelines and safeguards to protect our client members.

● (1605)

**Gabriel Ste-Marie:** I'll move on to my next question, which is a two-part question.

I would like to hear about your experience with interactions among the various government agencies involved in fraud cases. These include the Financial Transactions and Reports Analysis Centre of Canada, or FINTRAC; the Canadian Anti-Fraud Centre; and the Royal Canadian Mounted Police, or RCMP.

In addition, what role do you see for the future Financial Crimes Agency, given that there are already institutions in place?

**Frédéric Lapalme:** These institutions, both FINTRAC and the Canadian Anti-Fraud Centre, have a role to play. These are law enforcement agencies. Desjardins interacts with both on a daily basis. Law enforcement agencies can send us requests to carry out investigations. Depending on the reporting thresholds, we provide FINTRAC with information on hundreds of thousands of transactions each year. Unfortunately, we often send information—reports—to FINTRAC, only to receive a direct request from a law enforcement agency investigating the same case. This means that organizations on both sides of the information-sharing process stand to benefit.

Regarding the agency, we would like to see the investigations lead to arrests. This aligns with the Financial Action Task Force's recommendations, published five years ago, and likely with the next report scheduled for release. We want to ensure that the system effectively combats both fraud and financial crime—these areas may overlap—in order to achieve the concrete result of an arrest and a conviction. Prevention is useful. However, certain situations reach a point of no return that requires investigations and, unfortunately, formal charges.

This is where we would potentially like to see the agency or another organization step in. Investigations into financial crimes require a level of expertise that not every law enforcement agency in Canada possesses.

**Gabriel Ste-Marie:** I would like to talk about Canada's anti-money laundering and anti-terrorist financing regime. If one improvement could be made to the regime to better combat fraud, what would it be?

**Frédéric Lapalme:** I already discussed the sharing of information and the arrests.

I would move in this direction, towards a risk-based approach. We already do this with fraud. Financial institutions don't like to lose money, of course. They certainly don't want their client members to fall victim to fraud. So we need this flexibility to manage risks, manage fraud and achieve the desired results.

We're part of the dynamics. We welcome today's initiative and the national consultation. We wholeheartedly support the government's commitment to combatting fraud. We must avoid subjecting fraud to an overly rigid regulatory framework. That would be our recommendation, with regard to both fraud and financial crime.

**Gabriel Ste-Marie:** I have one minute left. I'll ask you one last question.

A witness told us that other countries have legislation that requires digital platforms to verify the identities of people who purchase advertisements and who claim to sell financial products—including cryptocurrencies—before publishing them. The witness told us that the platforms in these countries have complied with these requirements and that scams have reportedly declined.

Do you think that Canada should take this approach?

**Frédéric Lapalme:** It's a good solution. It's another tool in the tool box for Canada and its institutions. It won't solve everything, but the principle stands that the greater the anonymity, the higher the incidence of fraud. Clearly, a transparency requirement to help us understand the players involved, the payers and the funders behind the advertisements or other activities on different platforms remains a valid option.

**Gabriel Ste-Marie:** Thank you.

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

[*English*]

Madam Dancho, the floor is yours for five minutes.

**Raquel Dancho (Kildonan—St. Paul, CPC):** Thank you very much.

Thank you to the witnesses for being here today.

My first question is for Mr. Harroun.

I've noticed there's been progress in recent years, and I think it may be from the CRTC, your work on spoofing and the caller display issues. Last time you had representation here—I believe it was in September—I mentioned that my constituency office received an RBC banking telephone call that was not, in fact, RBC online banking. Thankfully, I had a very intelligent staff member who caught on and stopped it there.

I've noticed recently that I'm getting similar texts now from a bank that I bank with. It reminds me, for example, to pay my credit card bill—that's a legitimate one.

I received a similar one—

**The Chair:** Madam Dancho, I'm very sorry to interrupt.

I see that the bells are ringing. I'm going to get you to pause for one moment. I'll pause the clock, but I'll let you start from the top so that everyone is following the trend.

**Raquel Dancho:** Sure. I think I was ranting anyway. I have so much to say.

**The Chair:** Well, it gives you an opportunity to redo.

Colleagues, I see the bells are ringing. We don't have the TV on, but I suspect that a vote has been called. I need unanimous consent to work through the bells. Given that it's a matter of privilege, I'm going to ask every member to give me a sign of affirmation.

**Some hon. members:** Agreed.

**The Chair:** Madam Dancho, I'll let you start again with five minutes on the clock.

● (1610)

**Raquel Dancho:** I think progress has been made on the caller ID side, and perhaps that's from the work of the CRTC and your moves to.... I don't know if you've mandated the telcos to work on spoofing with the STIR/SHAKEN technologies.

What can we do about the texting scams? Those are looking quite sophisticated. I was almost fooled the other day by something that looked very much like a legitimate text. I do receive text reminders from my bank, which are great. This was very similar and almost got me. Is there anything you can be doing to encourage telcos to deal with that?

**Steven Harroun:** I appreciate the question. You've laid out a good segue for me.

On the telephony side, we've done things such as universal call blocking, as I mentioned, 123-456-7890, but also STIR/SHAKEN, which is really that call verification system. Is it your bank calling? It can at least give you an X or a “potentially fraud”, or it can let you know if you should trust that phone call.

On the SMS text message side, the timing of your question is very good, because last year we introduced a framework to allow TSPs to block emails and SMS text messages that they know to be fraudulent. I'll be honest; I'm the policy guy, but there are all kinds of technicalities behind it where they can determine whether an SMS text message is valid or whether an email has a particular attachment you shouldn't click on, etc.

We're about to release a decision in the coming weeks that will actually enhance that framework even more and allow the telcos to do more, in that they can stop those text messages from hitting your phone.

**Raquel Dancho:** That's great news.

The technology exists to do so, and it sounds like you'll be permitting them to use that technology. Is that correct?

**Steven Harroun:** Absolutely. The way the telecom act is constructed, the TSPs need permission from the CRTC to interfere with any type of traffic. When I speak about these matters, I often say that if I can't enforce it, I'll regulate it, which is that policy piece, and that if I can't actually regulate it, then I'll educate, which is about educating Canadians.

**Raquel Dancho:** Thank you.

That's excellent work, and I'm glad that's coming forward.

I want to understand how this is going to work. If I were to click on the link and send an e-transfer, that would withdraw the money from my bank. Let's say I was banking with Desjardins. It would withdraw the money, and then it would use Interac's payment rail to get to the scammer. Where does the responsibility lie with each of you?

I'll go to Mr. Hines.

If I were to e-transfer to the scammer, where does your responsibility lie legislatively in preventing that scammer? I'm just trying to understand where Desjardins' responsibility begins, where yours begins, and where each ends. Can you outline the difference for me? How would you interact with Desjardins regarding that scam?

**Mark Hines:** Today?

**Raquel Dancho:** Yes.

**Mark Hines:** Today, as the network in the middle, we don't take a direct role in compensating victims of scams. That's managed by our participants, usually a financial institution. What we're proposing, however, is that each actor in that chain—the platform, us, the bank and the individual—has specific obligations. If we don't meet them, then we should hold some level of responsibility for it.

**Raquel Dancho:** What are your capabilities versus Desjardins', for example, to stop that e-transfer? Then I'll go to Desjardins to respond. What is the difference between the two of you? Who should be stopping that?

**Mark Hines:** Each of us plays a role. The key role that we play is really.... Our core value prop is a network view. What does that mean? It means I can see certain information about the destination that the sending institution can't see by itself, regardless of whether it's the biggest FI in the country or a small FI. Getting that intelligence from the receiver side, which is really the key for scams specifically, is where we're focusing our time, because that's what we, uniquely, can do.

**Raquel Dancho:** Okay.

[*Translation*]

I'm speaking to you, the witnesses from Desjardins. Do you have any suggestions for legislation that we could pass or anything else that we could do with regard to Mr. Hines's response?

**Frédéric Lapalme:** Yes. We would like to point out that this shows the importance of the Canadian Anti-Scam Coalition launched and of our discussions today. So, it's a complete chain.

In the situation described, the financial institution would bear much of the responsibility for whether the victim is compensated. However, as we have shown today, a whole chain of stakeholders all share responsibility. As a result, the Canadian Anti-Scam Coalition and other initiatives designed to bring all stakeholders together are all the more important.

● (1615)

[*English*]

**Raquel Dancho:** Last, for the CRTC, what would you say the telcos' role is? Is it their responsibility to have stopped that text in the first place? I don't mean this in a mean way, but sometimes I feel as if there's a bit of passing the buck, “Yes, it's a little bit ours, but it's kind of their fault, and we are not going to cover the cost. They should, but we could have stopped it.” Anyway, I think you get my point.

What is the telcos' role in stopping this?

**The Chair:** Answer within about 30 seconds, if you can, Mr. Harroun.

**Steven Harroun:** Ultimately, the telco's role in this scenario is to actually put that text message, call or email into your inbox. They are the pipe that delivers it to you. Fortunately, because they are well invested in stopping this type of fraud and stopping this type of activity, they often come to me seeking those permissions, "Can we stop this type of traffic? Can we stop these types of things?" That's just their role. They want network security as much as anyone else but, ultimately, their role is to deliver that traffic if they're supposed to, if it's going through their network.

**The Chair:** Thank you, Madam Dancho.

[*Translation*]

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

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

I'll start with you, Mr. Hines.

It's true that Interac isn't a full-fledged financial institution. I would say you're working with the banks to do internal financial transactions.

I'll talk about humans, about seniors, our parents and grandparents. Some have cellphones and sometimes do Interac e-transfers. Sometimes they don't have a good handle on a transaction, and then the bank says they're responsible when something goes wrong. As young parents, we weren't equipped to train our grandparents on how Interac works. If I'm at work, I can't go and sit down with my grandfather and my mother-in-law to show them how to use Interac.

At what point is it the institution's responsibility to give seniors good financial literacy to prevent fraud?

[*English*]

**Mark Hines:** As I mentioned before, education is vital, in particular for the vulnerable sectors. Seniors are, obviously, a key part of that. I've heard personal examples of folks with learning difficulties having been the victim of significant romance scams. These are tragic stories.

Our perspective at Interac is that the individual consumer alone should not be shouldering the burden of these scams, which is why our approach is to define a cross-sector approach, define what we each need to do, and then responsibility flows from that.

Education is a key part of that. Unfortunately, though, for seniors in particular—this is anecdotal—I've seen it happen that it stops those seniors from engaging with things that they really need to be engaging with online. Education is vital, but we also have a role to play to make sure that we're building a wall around them a bit to protect them as well.

[*Translation*]

**Bienvenu-Olivier Ntumba:** Thank you, Mr. Hines.

I'll quickly ask the Desjardins representatives the same question before ceding the floor to my colleague.

Mr. Lapalme, you may answer.

**Frédéric Lapalme:** Thank you for the question.

My answer will be along the same lines as what Mr. Hines just said. As we also said, seniors are no longer the only victims. Young people are victims when it comes to investments. Those who don't fall in the categories of young people and seniors are victims of other types of scams. In fact, people most likely to be targeted by scams are those who, unfortunately, don't think of themselves as potential victims, and think others are. Scams occur thanks to the speed with which transactions and frauds are carried out in the daily life of citizens and client members. I think another witness said this, but, a momentary misstep can make you a victim of fraud.

Technology is increasingly present and, unfortunately, we can't put the genie back in the bottle. We're going to have to evolve.

[*English*]

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

Thank you, all of you, for being here today.

I want to pick up where Ms. Dancho left off. You might be surprised, but I feel that, at this committee, this is where we actually align and are very concerned about what's going on. This study has become very important in finding a way to protect Canadians.

I'll start with Interac.

Mr. Hines, you spoke about some of the steps. To go back to what Ms. Dancho was talking about, could you talk about how the different players come together? We've now had conversations with platforms, basically with all of the different players. We're all here. Can we come up with, at least, a solution or a template for it that allows us to understand what we can do better?

● (1620)

**Mark Hines:** There are frameworks and structures that exist today—we don't have to make this up—both Canadian and international. In Canada there is, essentially, a similar structure with respect to cybersecurity, in which signals are exchanged between institutions. A similar approach could be taken with fraud data.

Australia is an example. I think the committee heard from a delegate from Australia. That's a market where they've taken this approach. We try to learn from other jurisdictions, from Australia, in particular, the U.K. to a certain extent, and Singapore is another one. There are standards around how you structure that to minimize the invasiveness, from a privacy perspective, to ensure integrity and security, obviously. I would point to those as very real examples that we could adopt without having to build it from the ground up.

If I might just take 15 more seconds to give an example of how a data element would work in that scenario, part of the new capabilities we're deploying on RTR and on e-transfer is something called a risk list, which has certain data elements that have previously been associated with fraud. If we know a telephone number is previously associated with fraud and we can share that back into the system, that's something that a TSP could use to inform trying to filter through these bad actors. I talk always about how they're coming to me, but there are ways in which we could share back as well.

**Doly Begum:** If I may, I would ask Mr. Harroun the same question.

**The Chair:** Ms. Begum, I'm afraid we're quite a bit over, so we may have to circle back.

It's timely. I just looked down, for a moment, at an email from FIFA World that reads, “$4 million has been awarded thus far, Ben Carr. Click here for your exclusive reward.” When I clicked on FIFA World, let's just say it looks fraudulent. I'm glad I've been educated on the matter, but it's quite appropriate.

I don't see any of your logos there, so everyone is safe at the moment.

[*Translation*]

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

**Gabriel Ste-Marie:** Congratulations on your vigilance, Mr. Chair.

I'll continue my discussion with the representatives of the Mouvement des caisses Desjardins.

I'd like to hear your thoughts on the role of AI in fraud, but also in prevention.

**Frédéric Lapalme:** AI is the new thing, the flavour of the month and probably of the next decades. Fraudsters are already using it. I'll give you an example. In Quebec, the use of French has increased. It used to be a barrier that somewhat protected us. Unfortunately, that's no longer the case with text messages and emails. A chatbot can write a really good email.

When it comes to prevention and detection, as a financial institution, we need to use those tools. Again, it comes back to the privacy elements. That's important, but to be able to use AI, we need data. Financial institutions have a lot of data that can be used to protect their clients, their members, so my answer would be along the same lines.

**Gabriel Ste-Marie:** Let's move on to the topic of open banking.

Currently, when someone makes an unauthorized transaction, which is a fraud, the financial institution has to pay. However, with open banking, there's a risk the institution and the trading platform will pass each other the buck, or that fintechs won't even have the means to pay.

How can we ensure consumers don't lose out?

**Bernard Brun:** That's a very good question. We're entering another dimension where the focus is more on data portability. Open banking will also lead to more frequent transactions.

It's important to understand that this system already exists, but it takes the form of screen scraping. The first thing I'd say is it would be an excellent idea to adopt a regulatory framework, because that'll really make it possible to define responsibilities.

That said, we're really touching on the hot-button issue, meaning all the coordination that needs to be done. There has to be very clear coordination between jurisdictions, whether it be Quebec or other provinces and the federal government, to determine who's responsible and to what extent, especially in the context of open banking and consumer services, given the acceleration of transactions.

● (1625)

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

Mr. Chair, I'll give you the few seconds I have left. Thank you.

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

[*English*]

Mr. Falk, you have five minutes, sir.

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

Thank you, witnesses, for your presence at committee today.

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

Payments Canada was here a few meetings ago, and they talked about their RTR, real-time rail, system coming out later this fall, which will speed up transactions.

Currently, we don't have that system. We have a system that is slower. How much slower is it? What would a typical time for clearing be?

**Mark Hines:** E-transfer today is actually made up of a few components, including real-time components of e-transfer. The majority of our business payments and part of our retail payments are, in fact, real-time, and then the bulk of our system has delays between the user payment and the actual movement of the money. That exists today for fraud purposes, predominantly. The specific time of that window is mostly set by the financial institutions, and it can be anywhere from a couple of minutes up to half an hour. The real-time transactions will usually occur in a number of seconds, but usually under a minute.

**Ted Falk:** There is a bit of an offset today in the time that a transfer is made until it's received. It goes through the Interac system when a transfer is made.

I'm going to look at a case here. It was mentioned at one of our previous committee meetings.

Peter Squire, who's a realtor from Winnipeg, was defrauded on the phone in October 2022. In November of that year he made a transfer to the fraudster's account, an RBC branch in Toronto, and subsequently made a larger transfer there for a total of about $650,000. Somewhere along the line, the fraudster was able to establish an account at RBC and from there, transferred it to Citibank in Hong Kong.

You guys all play in the same sandbox. Is there no recourse for someone like Peter Squire?

**Mark Hines:** Once the money is moved, the loss has happened. That's precisely why my focus, both in my opening remarks and a few times today, is on how we need to focus on the prevention intelligence sharing. Once the money is moved and you're into recourse territory, there is room to optimize on the receive side.

I don't mean to be dismissive of it, but you've already missed the primary point, in my opinion. The opportunity is to stop it leaving the account in the first place because, for every one of these horrible stories, even if it has some form of happy ending, the amount of time that it takes today for that to happen has an outsized impact on folks.

That's precisely why we are saying to focus on the preventative aspect of it. Follow the models of other jurisdictions that are getting it right and are seeing the results of it.

**Ted Falk:** Do you, as Interac, flag certain transactions to your FIs, financial institutions, as potentially being fraudulent?

**Mark Hines:** Yes.

**Ted Falk:** At what frequency would that happen?

**Mark Hines:** On every e-transfer transaction today, we will score the transaction and deliver that score to a financial institution. They will then use that to make their decision on whether or not to process the transaction, to actually make the transaction. We do that today.

On the RTR and the upgraded e-transfer system, when we go live on the RTR, there will be four main elements. The scoring is one of them. An input to that scoring is what I've referred to as the risk list, which is the index of previously identified fraud. The key element on the RTR is this: The RTR side and the e-transfer side will benefit from each other's risk list. We've already taken a step in that data sharing to try to get ahead of this issue. The next one is something called confirmation of payee, which is that, before you make the payment, it will confirm whether the destination matches what you're intending to send. The last one is reporting, which is *post facto* intelligence.

● (1630)

**Ted Falk:** You're communicating with both ends of the transaction.

**Mark Hines:** Yes.

**Ted Falk:** Do you find that your communications are helpful? Do you have a degree of success in those communications that you have documented?

**Mark Hines:** Yes. Don't get me wrong. We have a lot of room to improve, but today we stop a lot of fraud already. In 2025, we stopped $99.8 million of fraud on our network. Our headline metric is measured in basis points, and it is 3.89 for our financial year 2025, which is on par with networks globally, like Zelle. We'd like to improve that. It's not the top end of those networks, but we already stop a lot today. What we're trying to do is steepen that response curve to reduce impacts on Canadians.

**The Chair:** Thank you, Mr. Falk.

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

**Karim Bardeesy (Taiaiako'n—Parkdale—High Park, Lib.):** I'll be sharing with Mr. Bains.

I have a couple of questions for Mr. Hines.

You have a very well-known brand, and your e-transfer product is a very well-known product. To what extent are scammers using or misusing the brand and logo, perhaps through digital social media platforms, such as on Meta's platforms, to impersonate as part of their scams? What kind of response do you usually have for that?

**Mark Hines:** Trust is our biggest strength. People use Interac because they trust us, and that's why fraud is such an important issue to us. It sounds very trite, but from a purely commercial perspective, if people don't feel comfortable using our platform, they won't use it as much.

With the RTR, competition is coming for us more than it has in the past, so that's why it matters. Being able to target the use of our marks on any platform that isn't authorized by us is part and parcel of why we're promoting this data sharing; it's that we can target it more effectively.

For us, it's no different from Wealthsimple's example, which is, again, another trusted brand. We suffer in the same way, and that feedback loop is really what we're looking for so that we can more effectively target it.

**Karim Bardeesy:** I have a question for the CRTC.

We heard testimony earlier that Meta is blocking news articles, news links, through their response to the Online News Act. To what extent does their implementation of news blocking demonstrate their technical ability to rapidly respond to suspicious links that they can identify with some specificity? What is your take on their inability to put news links back up, including those that might help respond to fraud?

**Scott Hutton (Vice-President, Consumer, Analytics and Strategy, Canadian Radio-television and Telecommunications Commission):** We've been engaging with Meta on the news front for a number of years, and we currently have an open proceeding in front of us. When we did ask them questions, from what we understand, it is very much a light-handed approach. They are looking at bona fide news sites, and these are what they are blocking access to. It's a very limited approach that they are taking.

Certainly, they are making an effort for their own purposes not to distribute that news, but that's what they are doing. They are identifying the limited number, hundreds as opposed to potentially hundreds of thousands, of fraudsters out there.

**Karim Bardeesy:** Thank you.

Maybe this is more of a comment than a question, and then I'll hand it over to Mr. Bains.

One of the tools that we as MPs have to communicate with the public is our monthly householders and newsletters. Sometimes print products are an untapped resource in the fight against things like fraud and in informing constituents, especially those who are a little less technologically literate. Maybe it's a consideration for the kinds of products that might come from your very trusted resources that we could start putting in our householders.

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

Thank you, Mr. Chair

Thank you to our witnesses for joining us today.

I'm going back to a previous witness who came here representing the Canadian Association of Retired Persons. As we know, that community is probably one of our most vulnerable. They are Canadians who ultimately built this nation, and we need to make sure that we're protecting them.

During their commentary, they talked a lot about the fact that CRTC could do more with protection. I know you've recognized the blocked calls and some of the other measures you've taken, but they talked about gaps. I'm interested to know this. During your work, are you seeing gaps in some protections that you could close and that you're working towards? Maybe you could talk a bit about that.

● (1635)

**Steven Harroun:** Obviously, I come from a different perspective at this table. I'm responsible for a civil legislative regime. There's not much I can do about true fraud, true crime or true criminal behaviour. Where I've taken my approach within my sector and the compliance enforcement sector at the CRTC is that compliance is number one, which is ensuring legitimate companies comply with the telemarketing rules, the anti-spam rules, etc.

In that same vein, if I can't deal with it through a compliance measure, I do have the tools at my disposal sitting in the communications regulator, where I can ask the TSPs to do certain things. That is where we get to the policy measures I spoke to you about. One of the examples I gave was billions of calls being stopped using AI technology to identify fraud calls. Being able to do that means that phone never rang, so Canadians have never picked that up and they've never fallen victim to that scam, which is fantastic.

One of the things I mentioned earlier was education. I wouldn't dismiss the power of education, especially when it comes to our seniors and our vulnerable communities, whether that's new immigrants who don't speak English or French as a first language or low-income individuals. Education is about helping them understand the scams, which is all I can do in a civil regime. I can let them know that these scams exist and tell them what to look for and how to protect themselves. Pause, and consider whether this is legitimate: Is this too good to be true? Is this too bad to be true? Verify before you click on that link and before you claim your $4 million. It is about that verification piece.

For me, as the regulator of a civil regime, education is critical, because the more Canadians are aware of scams, the less likely they are to become victims.

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

Colleagues, that's all the time we have. The vote will open up in just about two minutes. What I'm going to do is suspend and give everyone the opportunity to vote. If folks stay in the room and don't go too far and everybody confirms that they voted, we can get right into the business ahead of us. We do have two hours beyond what we have now to complete the tasks at hand, but the quicker we get to it, the quicker we can get out of here.

I want to thank our witnesses for making themselves available today. This has been a very important study and an eye-opening one.

As Ms. Begum referred to earlier, one of the things I always appreciate about opportunities like this is that it goes beyond partisan lines. There is a desire on the part of all members from all parties who represent Canadians across the country to tackle this issue. It's one that all of our constituents are victims of and one that we're rightly seized with at the moment, and we couldn't be seized with it if not for the expert advice and guidance we get from individuals such as yourselves.

On that note, I want to thank you very much for making yourselves available.

Colleagues, I'm going to suspend. It will be up to your teams to make sure that you vote. I'll see you again in a couple of minutes.

[*Proceedings continue in camera*]