HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 156 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, April 8, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Monday, April 8, 2019

● (1640)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, I see we have quorum.

I apologize to the witnesses for all the difficulties with votes, but it is what it is and we're in the season that we are in.

Before I start, there has been some conversation about Mr. Dubé's motion. I'm going to allocate the princely amount of one minute to see whether there is an appetite to deal with Mr. Dubé's motion.

The first question I have is.... I shouldn't even ask this. I should say we're going to have this in open meeting as opposed to in camera; otherwise, we'll just waste more time.

Mr. Dubé, do you want to move your motion? We'll see whether we can get this done in one minute.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Hopefully I will need less than that. I've already presented it and explained why. It's on the record, so I'm happy to move to the vote.

The Chair: Ms. Sahota.

Ms. Ruby Sahota (Brampton North, Lib.): I would just like to state that I'm supportive of the motion; however, I do feel that the time frame is very loose. It allows up until June 21. I do think there is some urgency to the matter, because there are a lot of people who feel uncomfortable about the way the report was put out initially in December. I would urge that we perhaps state that it should be done at the minister's earliest convenience.

That's just a friendly amendment, so that we don't give such a lengthy deadline but do it as soon as possible.

The Chair: Mr. Dubé.

Mr. Matthew Dubé: Thank you. I appreciate that. Understanding that we have a busy committee, I would perhaps just amend it to say "at the minister's earliest convenience but no later than" the date that's in the motion, so we don't say that the earliest convenience is when some of us come back.

Ms. Ruby Sahota: Yes, I think that's a good amendment.

The Chair: Okay, do we have consensus on that?

Properly, I should have Ms. Sahota move an amendment and then we will vote on the amendment. Do you want to move your amendment?

Ms. Ruby Sahota: Yes, my amendment is, after the words "the Minister of Public Safety and Emergency Preparedness to appear", to say, "at his earliest convenience but no later than Friday, June 21, 2019."

The rest of it is the same.

The Chair: Okay. The vote is on the amendment.

(Amendment agreed to [*See Minutes of Proceedings*])

(Motion as amended agreed to [*See Minutes of Proceedings*])

The Chair: Excellent, thank you very much.

Now we'll turn to our witnesses. Notice the extraordinary level of co-operation among colleagues on the public safety committee, unfortunately not replicated anywhere else.

Our first witness is Ms. Terri O'Brien from the Interac Corporation, and the second witnesses are Mr. Ferrabee and Mr. Kyle from Payments Canada. I thank you for your patience.

I'm going to ask you for your opening statements.

I'll point out to colleagues that we are supposed to be voting again at 5:30. I assume that's when the bells go.

The Clerk of the Committee (Mr. Naaman Sugrue): There may be bells at 5:00.

The Chair: Okay, so let's at least get the statements done. We started the meeting. Thank goodness for that.

Do I have unanimous consent to proceed until we can no longer proceed?

Some hon. members: Agreed.

The Chair: Okay, that is probably 20 minutes.

Please proceed. Again, I apologize for these procedures, but they are what they are.

Ms. O'Brien, go ahead.

Ms. Terri O'Brien (Chief Risk Officer, Interac Corp.): Good afternoon, everyone. Thank you very much for the opportunity to address the committee.

My name is Terri O'Brien. I lead the risk management practice at Interac Corp.

For my opening remarks today, my goal is to provide insights and recommendations on cybersecurity from our unique position in the financial services landscape. Many of you know Interac already. Like millions of Canadians each day, you use our products and services to withdraw money and pay and transfer funds with security and convenience.

What you may not know is that Interac is 100% Canadian-owned and operated. What sets us apart is not only our Canadian roots, but the trust we have established with Canadians over our 35-year history. Last year, Canadians made 6.6 billion transactions, moving over $415 billion in value across our suite of products, including Interac debit and Interac e-Transfer.

Interac has been in the business of facilitating real-time payments between Canadians for decades, including our Interac e-Transfer product, which has been facilitating real-time payments since 2002. Of course, this includes real-time 24-7 fraud detection. With real-time payments comes the need for real-time security, prevention and detection capabilities, which we've built up over our history. Our real-time cyber and fraud capabilities help Canadians digitally transact with confidence across a variety of devices and platforms, including mobile devices. At the same time, we adhere to our core values that have been central to our history, including corporate responsibility, safety and soundness.

Security is a core element of everything we do, whether it's combatting fraud across our network or keeping the personal financial information of Canadians private. Therefore, cybersecurity is something we think about a lot.

As our economy and society have become increasingly digital, it is no secret that the pace of cybercrime has accelerated. As I'm sure you've heard in some testimony, and as we've read and seen in reports, around the world it has never been easier for people to access cybercrime goods and services. Fraud-as-a-service and cybercrime-as-a-service websites currently sell everything from credit card numbers to social media account credentials and denial-of-service attacks. All of that is available with a single click and for several hundred dollars.

In that regard, Interac was very pleased to see the government establish the Canadian Centre for Cyber Security last year and make new investments in cybersecurity in the most recent budget. We also support the creation of the centralized cybercrime unit under the RCMP.

Interac is in a unique position at the centre of the Canadian financial services landscape. We operate as a central payments and digital information exchange to facilitate the interoperability of payments and related information among our Canadian banks, credit unions, caisses populaires, payment processors, businesses and Canadian consumers. Because of this, we are in a unique position where we can detect cybercrime, including fraud and money laundering, as it moves throughout our system and between those institutions.

This is a unique role that Interac plays at the centre of the ecosystem. Whereas each financial institution can detect fraud and money laundering only within its own customer accounts, Interac can see the criminal activity across institutions.

In order to pick up on these patterns of criminal activity, we employ sophisticated tools that utilize machine learning and predictive behavioural modelling. When our systems detect high-risk or suspected fraudulent activity, actions are immediately taken, including suspending or blocking the transactions.

We also communicate directly with institutions across the financial system. We collaborate and share information to strengthen our collective resilience and security in the Canadian economy. A practical example of this for the committee is when we detect that financial criminals are utilizing many different accounts to target a specific bank, union or caisse populaire. In these circumstances, we alert the institution that is being targeted, while simultaneously working to block the activity and secure vulnerabilities at the various sending institutions.

Because cybercrime doesn't have business hours, neither do we. Our detection and prevention systems and staff operate 24-7, enabling us to counter cybercrime in near-real time.

We are constantly evolving our approach in order to keep Canadians safe when transacting over our networks. In 2018, our fraud risk mitigation practices prevented over $100 million in fraud losses, and we had over 4,300 malicious websites taken down.

We also work together today with the RCMP and local law enforcement to support and assist in their investigations of fraud and related criminal activity. Protecting Canadians' financial information amidst the changing payments landscape is a top priority for Interac.

● (1645)

Since the advent of mobile wallets, payments are now made through smart phones and other devices, as mobile payments are growing in popularity among Canadian consumers and businesses every day.

In order to secure the payments made via the Interac debit network on mobile devices, Interac became one of the first domestic debit networks globally to establish its own token service provider, or TSP. Our TSP ensures that personal identifiable information, including account numbers, is replaced with randomized information, or tokens, that is of no use to hackers or criminal activity.

Expanding the use of tokenization is one way we can enhance cybersecurity for the benefit of Canadians. Collaboration and coordination among private and public entities are also pivotal to addressing the volume of cyber-threats that exist today.

We see three specific areas of focus here that can greatly benefit Canadians. The first is information sharing with the new cybercrime unit in the RCMP. The second is a more targeted approach to detecting cybercriminals. The third is ongoing public education and awareness.

Interac believes there is an opportunity to reduce impediments that currently exist in order to enable more open sharing of known cyber-threats between Interac and the government through secure and trusted channels. This should include looking at legislative changes, as well as safe harbour provisions, to open up communication channels and address concerns around enforcement actions.

Second, when it comes to detecting cyber-threats, we see benefits in utilizing a more targeted approach as a key point of emphasis. The way threats are detected today is akin to a scattershot, in that all transactions must be scanned and analyzed with equal importance. A more efficient model would be one that focuses on lists of known cybercriminals and cyber-threats and those vectors and behaviours, utilizing information from government and law enforcement, as well as financial institutions and Interac.

Interac could play a pivotal role here, given our ability to detect criminal activity across our network and our connection to almost 300 financial institutions. Interac, at the centre of the ecosystem today, could represent a secure information exchange with the RCMP in the future, to allow both organizations to take a targeted approach in detecting and preventing crime, rather than scanning all transactions. We believe government can and should play a leadership role here by establishing and maintaining clear processes and lines of accountability.

Finally, at Interac we recognize there is a need to provide ongoing public information and education about cyber-threats and security best practices to support an increased knowledge of the current risks and how to keep Canadians safe. We regularly conduct proactive campaigns designed to educate and inform. We also participate in forums such as the Competition Bureau's public education working group to share our insights and results. We also collaborate actively with the RCMP and local law enforcement.

We look forward to further collaboration with the government on information sharing, targeted detection, and public education in the future.

To conclude, I would like to emphasize Interac's commitment to cybersecurity and our willingness to work together with the government, as we do today. We support recent initiatives and investments made by the federal government, and we believe that continued education and discussions like these can advance industry-wide solutions to help keep Canadians safe from cybercrime.

Thanks very much.

● (1650)

The Chair: Thank you, Ms. O'Brien.

Mr. Ferrabee, go ahead.

[*Translation*]

Mr. Justin Ferrabee (Chief Operating Officer, Payments Canada): Good afternoon.

My name is Justin Ferrabee. I'm the Chief Operating Officer of Payments Canada.

[*English*]

Thank you for inviting Payments Canada to contribute to the study.

Let me begin by reassuring the committee that security is Payments Canada's highest priority in all we do. It commands focus, resources and investment, above all other needs. This means that we design, review, modify, update and operate our systems as we monitor risks. We see security as a prerequisite for innovation in the payment space. We remain in a constant state of vigilance and respond decisively, as required, to ensure that we manage risk appropriately and that we remain secure.

Over the next few minutes, I'll share who we are and what we do, our collaborative approach to cybersecurity, and our recommendations for reducing the risk in the financial sector.

Payments Canada operates Canada's national clearing and settlement systems. While Payments Canada is a little-known entity to most Canadians, it plays an essential role in the economy and in the day-to-day operations of financial institutions and businesses across the country. Payments Canada's systems ensure that payments between financial institutions—the aggregation of all payments made in the economy—are safely and securely completed each and every day. The value transferred is over $50 trillion annually.

We are guided by our mandate and the public policy objectives of safety, security and efficiency of the Canadian clearing and settlement system. In consultation with members and stakeholders, we also maintain a framework of rules and standards that mitigate risk and facilitate the exchange of payments and the deployment of emerging payment products and services.

Given that cyber-threats evolve rapidly, Payments Canada is continually raising its defences. We have a cybersecurity action plan based on secure design principles and industry standards. The plan ensures that we are constantly watching for and closing gaps to maintain the resiliency of our operations.

Payments Canada operates within a network of financial institutions, regulators and other financial market infrastructures. We are held to the highest global security standards, including "Guidance on Cyber Resilience for Financial Market Infrastructures" from the Bank for International Settlements, the SWIFT customer security program, and the NIST cybersecurity framework.

We also work closely with the Bank of Canada to ensure that we meet the requirements for mitigating cyber-threats through internal and external assessments. Outside of these requirements, we establish rules and standards around the security of payment items and the connectivity of systems, to which our members must adhere.

From a wider, collaborative industry perspective, we work very closely with partners in the financial sector through cybersecurity industry groups such as the Canadian Financial Services Cybersecurity Governance Council, the Canadian Bankers Association cybersecurity specialist group, and the Financial Services Information Sharing and Analysis Center.

We also participate in and lead industry exercises for business continuity and cyber-resilience and share intelligence with partner agencies and organizations in the cyber community. These connections include the Canadian Centre for Cyber Security, Public Safety's critical infrastructure protection branch, RCMP's national critical infrastructure team, and the Canadian Cyber Threat Exchange. Further to these collaborations, we are actively engaged in the international cyber-risk community with our partners at the Bank of Canada.

Through all of these activities, we continually rank and benchmark ourselves internationally, and we are consistently in the top 1% of the global industry for safety and security.

Working closely with our financial institution members, the Bank of Canada and the Department of Finance, we are currently undertaking a major program to modernize Canada's payment systems to meet the growing demand for secure and innovative new payments products. Modernization will result in new payment infrastructure designed to strengthen the payment system.

Through our diligence and movement toward modern payment systems, we have identified gaps that exist outside our realm, which this study may be able to influence. There is a clear need for public-private coordination in responding to attacks against critical infrastructure and, with that, a single, clear point of contact in the public sector. These improvements will help us better share information, in a protected fashion, and help us manage and prevent future attacks. The release of the national cybersecurity strategy in 2018 and the recent developments with the Canadian Centre for Cyber Security will help in this area.

At the same time, the recovery of systemic cyber systems must be prioritized in the event of a widespread disruption. Policy that extends cybersecurity requirements to the supply chain of critical systems would help to improve the resilience of dependent components to the national infrastructure and the financial system as a whole.

● (1655)

Investments in policies and cybersecurity can also support digital supply chain risk. The modern supply chain often includes hundreds, or thousands, of software components that are embedded in critical systems sourced from companies and communities all around the world. It is a significant task to track and inventory all the ingredients of a system and make sure that those ingredients remain safe.

In the food safety world, we have labelling standards that inform customers about product ingredients and nutritional facts, but in the software world, we have no labelling standard to help consumers understand what components and what risks might exist within the software. Policy to support digital supply chain risk is necessary, and system labelling of software components should be studied for its benefits to the economy.

We also feel strongly that more could be done to address the cybersecurity skills shortage. There is already a gap in capable people and, given the increasing severity of threats, there is a need for policies and strategies to develop, attract and retain skilled workers. This would ensure that Canadian companies are able to safely grow and innovate as they expand their use of digital technologies.

Finally, we see a need to equip Canadians with the knowledge and awareness of good cyber hygiene to protect their personal and financial information online. For instance, right now millions of Canadians are seeking technologies and financial applications that mimic the services of open banking. In seeking such services, they aggregate account information across multiple platforms and thereby expose themselves to cyber-threats.

Payments Canada was pleased to see that several of these issues, and commitments to address them, were included in the 2019 federal budget, but we know that cyber-threats are not going away. They are evolving just as quickly, if not faster, than digitization and modernization across all industries. We must work together to build resilience in the face of these threats in a way that ensures that we do not hinder the pace of innovation.

While every organization has the responsibility to protect itself from cyber-attacks, doing so as a collective or a network is much more effective. Cybersecurity is an issue that affects the Canadian economy and our national security as a whole. Payments Canada is eager to contribute and support a network defence strategy.

Thank you.

● (1700)

The Chair: Thank you.

Colleagues, we have 12 minutes left. If we ran this down to five minutes before the vote, that would give you four minutes, then four minutes, and that would be about it.

I would seek your input as to whether we could come back and spend an hour with these folks, if they are available. Can we do that?

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): I won't be here.

The Chair: Okay, there are no votes, no motions. That's agreed. We'll come back for an hour. I just feel we're abusing these folks' time.

We'll be back here probably about 5:30.

With that, Ms. Sahota has four minutes, and then Monsieur Paul-Hus has four minutes.

Ms. Ruby Sahota: Thank you.

Ms. O'Brien, you spoke about malicious websites. How often are you seeing these malicious websites go up? How much of your capacity gets used up by taking down these malicious sites? Could you explain a little the awareness you are trying to raise for consumers so they're not duped?

Ms. Terri O'Brien: Last year, Interac experienced 4,300 of these phishing websites. We worked with a leader in the industry, a partner of ours, to take them down. It's a similar partner that works with many financial institutions. The larger financial institutions experience many more phishing incidents or fraudulent websites that are put up.

The websites are intended to collect personal, identifiable information—login credentials or other such means of identity—of Canadian consumers, so they can take over their bank accounts or other payment processing to extrapolate the money from their accounts. That's the intention of the websites. We are finding that they've been getting more sophisticated in recent years. I think folks would agree that they're getting better at stealing logos and branding and making it look like a legitimate website.

We do participate heavily in public education in this regard. It's very important to know that your financial institution isn't going to send you links and emails to click through to these malicious websites. There are ways that we educate the public to double-check that they are, in fact, on their own financial institution's website or Interac's website, and not on a spoofed website.

Ms. Ruby Sahota: You also spoke a bit about mobile wallets, and Interac has been operating on the tap system for a while now. Has this led to an increase in fraudulent incidences? Are we forgoing safety for the sake of convenience? Could you shed some light on that?

Ms. Terri O'Brien: I would say no, actually. The mobile technology is more secure. It is akin to the tap technology, so it uses the EMV card technology. It's quite a layered security. I also mentioned tokenization. What's actually stored on the phones is a token, not the actual card number. It leverages the tap technology, which is quite secure. We have almost eliminated fraud in the Interac debit business. A lot of that has to do with chip and PIN. The residual, which is really at one basis point—it's as low as it could possibly be—stems from exploits in the U.S., where there are still terminals with a magnetic stripe, but effectively, in Canada, that technology is extremely secure.

Ms. Ruby Sahota: We heard a little bit about the token service provider from witnesses from Mastercard when they were here. I'd never heard about it before. It seems that—and correct me if I'm wrong in my understanding—this system isn't used consistently. Why is Interac not switching over to the token system completely so that personal information is eliminated?

● (1705)

Ms. Terri O'Brien: Interac has developed and deployed our own token service provider. It's correct in that we are not using any other provider, whether it's Mastercard or otherwise. We have our own token service provider. We deploy our own technology because it is so secure and because we can manage and maintain the security around it.

The Chair: Thank you, Ms. Sahota.

[*Translation*]

Mr. Paul-Hus, you have the floor for four minutes.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

I want to thank everyone for being here. We're sorry about the disruption resulting from the votes in the House.

In the case of Interac, if I make a transfer, the recipient will have 30 days to accept the funds. Where is the money from my bank account stored on a virtual level? How does this work?

[*English*]

Ms. Terri O'Brien: That's a very good question. I think the question is directed toward our Interac e-Transfer product, which has several different options. Auto-deposit is an immediate, real-time transaction. The one that you described is called our question and answer type of transaction. That's where the recipient would like a security question answered to deposit the e-transfer transaction. In that case, since a person may not be on their email on a daily basis, they are given 30 days to accept the transfer. What happens, however, for the person sending the transaction is that the money is taken from their account. It's a good-funds model, so the funds are available. It's held by the sending financial institution in a suspense account, and then, once the security question is answered, the funds are released. At all times they are secure.

[*Translation*]

Mr. Pierre Paul-Hus: I gather that, if I do business with the Royal Bank, the money doesn't go to Interac. The money will remain in a Royal Bank account.

There's often a concern. Once the transfer is made, we have no more contact. We wait for the recipient to accept the funds. However, if the person doesn't receive the money, we worry about where the money has ended up. So the issuing bank has it.

I'm trying to understand the technical system. From a virtual standpoint, could another person intercept the transfer? Could a hacker intercept a transfer? What could be done in that type of situation?

[*English*]

Ms. Terri O'Brien: The answer is no. It's a highly secure, closed-loop, private network. While Interac operates the infrastructure, Interac also has the operating regulations and governance through which the transactions transfer from each financial institution. What we are facilitating is the financial institution that wants to employ the question and answer or Q and A type service. At no time, though, could the transaction be intercepted in transit. It is securely held at one financial institution and then, once released, the payment across the Interac infrastructure is securely facilitated into the receiving institution.

[*Translation*]

Mr. Pierre Paul-Hus: You're saying that the transfer process is perfectly secure. There's no way to interfere with it.

[*English*]

Ms. Terri O'Brien: That's correct.

We have a fully secured, closed-loop private network among the almost 300 financial institutions, credit unions and caisses populaires across Canada.

[*Translation*]

Mr. Pierre Paul-Hus: You spoke a bit about the government. What current legislation should be amended and made more effective for you? Certainly some legislative measures aren't effective and should be improved.

[*English*]

Ms. Terri O'Brien: That's a wonderful question.

We actively work with the RCMP and law enforcement today on the exchange of some information, although it often requires a production order. We would suggest that certain privacy and other safe harbour legislation could be opened that would allow a much more targeted approach among the trusted channels that we have today, whereby we could effectively focus and manage the cybercrime in a much more targeted way.

We find that our communications today are quite effective, but they are unspecific and constrained in many ways. We think there definitely are legislative options that would allow for more open sharing of that information, which would benefit—

The Chair: Thank you, Mr. Paul-Hus.

With that, I'm going to suspend, and we'll resume as soon as possible for another hour. There will be no motions or anything else.

Again, I thank you for your patience.

● (1705)

(Pause)

● (1725)

The Chair: We are back on. I see quorum.

Mr. Motz, you have never been more popular in your entire life.

We're going to go with four minutes, then four minutes, and then we'll go to five-minute rounds. Mr. Dubé would normally be up next, but I don't see Mr. Dubé, so I'm going to go to Mr. Picard. When Mr. Dubé arrives, we'll go back to Mr. Dubé.

Again, thank you for your patience.

Mr. Picard, you have four minutes.

Mr. Michel Picard (Montarville, Lib.): Thank you.

Ms. O'Brien, you talked about cybercrime and fraud. What is the nature of the fraud you detected on your system, to which you've reacted in the past?

Ms. Terri O'Brien: The fraud is constantly changing, and it also moves around based on vulnerabilities at the different financial institutions. The most common fraud that we see is what we call account takeover fraud. In the earlier example, we were speaking about some of the phishing exams, a person's credentials or personal, identifiable information that allows criminals to overtake their bank account. Then they start a systemic practice of draining the funds from that bank account, sometimes to different receiving institutions, and pulling the money out of the financial system.

At Interac, we are in a unique position where we can see that fraud cross institutions across our network into different financial institutions on the receiving end. What we've developed is a fraud detection system that patterns that behaviour and is able to detect it. Then it either blocks the transactions or holds them for further review.

Mr. Michel Picard: When you block a transaction, that means that someone somewhere has the information of the cardholder. By having that, they may then have access to their bank account and therefore start digging for more than just the money—personal information that can be used for identity theft and so on. Your action may block a transaction, but part of the damage is done already, and we don't yet have any control over what kind of information has been stolen at this point.

● (1730)

Ms. Terri O'Brien: Not always. I won't outline all of the behavioural models, but I will say—noting that 99.9% of transactions flow through, and that's just indicative of our volume—that when a transaction actually gets blocked, it is a known fraudulent transaction. There are certain vectors and information we have where certain transactions are known, usually through information sharing that we actively participate in between Interac and the financial institutions, both sending and receiving. Sometimes that happens with the RCMP and law enforcement as well. It's that reciprocal sharing of information that is really critical to allowing us to block known fraudulent transactions. In the cases of the blocks, the customers are not impacted.

Mr. Michel Picard: We're still stuck with four-digit PINs, which provide maybe 10,000 combinations. Is that sufficient nowadays?

Ms. Terri O'Brien: I'd say yes. The chip and PIN, both the chip technology with the EMV-layered security and the PIN that is known only to the user, have been very effective. We've almost eradicated fraud on Interac debit. It's well below one basis point of fraud. As I mentioned earlier, it's just the remaining mag stripe terminals in the U.S.

I think it's also effective because of public education. There has been a lot of public education so that you don't share your PIN. Even in widely streamed media, in television shows, they've talked about how sometimes even spouses don't share PINs with each other. It's been very effective public education to keep your PIN secure and secret.

Mr. Michel Picard: You said that you have a private network among banks, but when I buy something at the store, do I make my transaction through a totally private, closed network? If that's not the case, do I have to go on the web or somewhere to make that so I'm totally secure?

Ms. Terri O'Brien: You are totally secure. The PIN pads you make your transaction on, those are all issued by acquirers and payment processors, and they are part of the closed loop network. Every point in the network is secured.

Mr. Michel Picard: How about going—

The Chair: Thank you, Mr. Picard.

Ms. Terri O'Brien: It doesn't go across an open Internet.

The Chair: I know you were on a roll there.

Mr. Michel Picard: No, I know. Thank you.

Ms. Terri O'Brien: They're good questions. Thank you.

The Chair: Mr. Cannings, welcome to the committee. I see you're not Mr. Dubé.

Mr. Richard Cannings (South Okanagan—West Kootenay, NDP): No, not the last time I checked.

The Chair: We had held four minutes for Mr. Dubé as the next questioner, but you may want to catch your breath and we can come back to you.

Mr. Richard Cannings: I would like to catch my breath and figure out what exactly we're talking about.

The Chair: Well, we're trying to figure out the same thing.

Mr. Motz, you have five minutes.

Mr. Glen Motz: Thank you, Mr. Chair.

First of all, thank you to both of the organizations for being here today.

I'll start with you, Ms. O'Brien. Canadians wonder—and I think I know the answer to this, but you can shed some light for us—if an Interac e-Transfer is traceable.

Ms. Terri O'Brien: Could you expand on the question? In what regard do you mean traceable?

Mr. Glen Motz: We're talking about cybersecurity today, so if we have an issue with an e-transfer, is that e-transfer a traceable transaction, if it is to a bad actor?

Ms. Terri O'Brien: Part of my testimony today was about encouraging open collaboration and more information sharing and safe harbour provisions with the RCMP. The transactions are traceable. However, in today's environment, if the RCMP is looking at a bad actor, as you suggest, they will keep certain information around that bad actor secret. They will sometimes issue a production order, in which case we will share the information we have, as required by law, and then they will continue their investigation into that bad actor.

We have some information that is shared among ourselves at Interac, the financial institutions and law enforcement, wherein we can have indicators that inform our behavioural models, but how the RCMP does its tracing of bad actors is shared to us as they are able to do so.

● (1735)

Mr. Glen Motz: Thank you for that.

In your opening remarks, you spoke about having a proactive sharing system, I think you called it.

Can you describe for us, in an ideal world, what the ideal sharing would be between your organization or the industry in general and law enforcement, to protect consumers? What would that look like?

Ms. Terri O'Brien: Sure. I'm happy to crystal-ball some great ideas in that space. We would absolutely love.... The cybercrime unit, particularly in government and the RCMP, as well as law enforcement, will regularly monitor some of the online or dark web or deep web marketplaces. Those marketplaces come up and go down quite frequently as they are trying to hide some of the marketplaces and some of the identifiable features of them.

In an open sharing environment, we would know that very quickly, and therefore we would have an ability—as to your earlier question—to trace bad actors as they come up in these online marketplaces in a closer to real-time fashion. If that information was openly shared with us, we could do a lot more to block or monitor potentially fraudulent transactions.

Mr. Glen Motz: Payments Canada, would you care to weigh in on that question? In an ideal world, what do you see as being a vehicle or a way in which we can share information between the financial institutions or the financial industry and law enforcement to protect consumers better than we do now?

Mr. Justin Ferrabee: I'll have our CISO, Martin Kyle, respond to that, because we're active in that.

Mr. Martin Kyle (Chief Information Security Officer, Payments Canada): There are many sharing organizations and groups already in place. In our comments, we talked a little bit about an information sharing group with the Canadian Bankers Association, for example. We talked about information sharing with a non-profit, the Canadian Cyber Threat Exchange, which was represented here by a witness, I believe. We have information sharing with the Canadian Centre for Cyber Security and with the RCMP. All of these various sharing groups allow us to get more information about existing threats and learn how to detect those threats on our systems, and then allow us to respond to those threats.

Mr. Glen Motz: You said in your opening remarks that Payments Canada transfers more than $200 billion daily through your various networks. If that's the case, how do you keep those large sums of money safe during your transfers? What does that look like?

Mr. Martin Kyle: As you know, our number one priority is the security of those transfers. We enable the safety of our systems by reducing our attack surface, as we in the trade call it. We have a very small, close-knit group of members whom we support and allow into that network. That network is very segregated from other networks, and that small attack surface allows us to pay very close attention to what happens on it in identifying threats, monitoring the activities and responding to the things that occur there in real time.

The Chair: Thank you, Mr. Motz.

Mr. Cannings, have you caught your breath, or should I go to Ms. Dabrusin?

Mr. Richard Cannings: I'll wing it here.

The Chair: Okay, you have four minutes.

Mr. Richard Cannings: Thank you.

As you understand, it's a bit of a surprise for me to be here. I just got off a plane and voted, and then they took me down here. So unfortunately I have not been able to hear your testimony. I had no idea what was going on before in this study either.

A question pops into my mind about payments with chip cards. You may have covered this, and my apologies if that's the case. Canada was an early adopter, at least compared to the United States. I'm just wondering about two things. Is that an issue, that Canada has widely used chip cards and Americans have not? I'm not sure if that's changing. Is there an issue between the two countries on the security status of those systems? Should we be more worried in the United States than we are here, or vice versa?

● (1740)

Ms. Terri O'Brien: That's a very good question. We have almost eradicated fraud in Canada on the debit card with chip and PIN. It's a very effective technology and secondary control, and only the person knows the PIN. The EMV technology on the card has been very effective to date.

We do have risk in that the U.S. has not adopted EMV technology. Industry pressure is increasing for them to do so. More of their point-of-sale terminals are being enabled. They have offered chip and signature in some point-of-sale terminals, but they haven't fully migrated to a chip and PIN environment.

It's a good example where a consortium of the industry, together with payments processors in the centre of the industry and settlement partners, can combat fraud when coming together on solutions.

The risk to Canadians in the U.S. is certainly lower, but it does continue with the magnetic stripe.

Mr. Richard Cannings: Where I interact with it, it's more the inconvenience of trying to buy gas in the United States and they demand a swipe and a postal code; of course, Canadian postal codes don't work down there.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): I can explain it to you.

Mr. Richard Cannings: I don't know. In Texas, they have trouble with it.

I was just going to ask you about skimming devices and chips. Is that not an issue at all?

Ms. Terri O'Brien: It's much less of an issue with the chip and PIN. Skimming devices still exist, though they have to have cameras to try to capture the PIN, but it's not a very elegant fraudulent solution because your hand could be in the way. So the risk is really negligible in Canada. The skimming devices that take the mag stripe continue to be a risk in the U.S. The mag stripe is easily copied.

Mr. Richard Cannings: That certainly does it for me.

Thank you.

The Chair: If you need any hacking help, Mr. Graham is here to help.

Ms. Dabrusin, you have five minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

My first question is probably more for Payments Canada. I was looking at a letter I received from someone who lives in my community. We're in that hybrid moment where people still sometimes write paper cheques, and now they can deposit them by taking a picture and sending that in. But then that cheque stays floating around with that person. They have all this personal information with your signature that you're counting on someone to deal with properly, although they might be just a private individual who doesn't have a way of dealing with it.

Has this ever come up as an issue that's been raised with you, and if so, do you have any tips for people about that and what they can do to protect their personal information?

Mr. Justin Ferrabee: I can speak for Payments Canada. We're at the infrastructure layer. We would write the rules around how that works, and we run the systems that do the cheque imaging and enable the digital image. But all the security and all the services provided to a consumer would be through their bank. We would support the bank, support our members in that, but it's at the policy level of the bank.

Ms. Julie Dabrusin: Okay.

Ms. Terri O'Brien: To add from my many years in banking, the technology has come a long way and the cheque imaging is quite good now. Of course, consumers are encouraged to destroy the cheque afterwards. However, duplicate cheque detection has come a long way as well. If you ever try to deposit it twice, it won't allow you to do so.

Ms. Julie Dabrusin: Thank you.

To Payments Canada, you talked about labelling within the digital supply chain and how to create proper labelling. Does anybody do any labelling in the world? Do you know of a standard out there?

Mr. Martin Kyle: No. In fact, that's why we put it—

Ms. Terri O'Brien: I know one.

Ms. Julie Dabrusin: Do you?

Ms. Terri O'Brien: I do, yes.

Mr. Martin Kyle: Go ahead, please.

Ms. Terri O'Brien: I've been looking at the model. It's actually quite good. SWIFT has adopted a model wherein they publish the security standings of all their counterparties, as they call them, not from a creditor's standpoint but just as a counterparty to the system. It's a good model that we quite like.

That allows each of the participants in the ecosystem.... If you're a financial institution or a caisse populaire and you see a lowered security level that's not quite at the standards, you can mitigate or limit your risk to that partnering financial institution. They've implemented some really interesting things in the past year.

● (1745)

Ms. Julie Dabrusin: Knowing that there's one standard out there, somebody who's doing it, what's the government's role in that? Is it that government adopts a form of labelling and then requires it for our financial institutions, or is it something that we leave to another sector?

Mr. Martin Kyle: I can respond to that.

The attestation program to which Terri referred has been a set-up by the SWIFT organization, to allow the counterparties to publish their attestations to other counterparties. If one organization feels like the other counterparty that they're doing business with is too risky, because of their attestation they have the opportunity as a business owner to de-risk themselves or to demand that certain requirements be met before they continue doing business with that organization.

Mr. Justin Ferrabee: I just want to come back to the labelling of ingredients. The attestation is a version of it, but it's an early version. There is no precedent for identifying all of the components in the value chain and disclosing and managing that. There are multiple parts to this. It's not actually being done anywhere else that we know of.

Ms. Julie Dabrusin: Part of what I'm thinking is that, from what we've heard, more and more of this is crossing borders. It's not something that lies entirely within Canada, as far as how it's being done is concerned. I'm trying to figure out which body, which organization is best set up so that we can co-operate with it as the Canadian government. We can encourage other international governments to participate, but where should that lie?

Ms. Terri O'Brien: It's a great question. SWIFT is a global organization that has started early days in that. I would absolutely suggest that Interac would be an appropriate place as well. We currently run our operating regulations and minimum standards, whether they're security standards or participant standards, for all the FIs in our ecosystem.

We have a very robust governance policy and operating regulations in market today. We're looking at how we can enhance those in-market regulations every day. The participants eagerly participate in the marketplace and adhere to those regulations because what it gets them is reciprocity of payments and access to the ecosystem.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you, Ms. Dabrusin.

Mr. Motz, you have five minutes.

Mr. Glen Motz: Thank you, Chair.

One of the things I'm sure you heard or read about is that Canada is dealing with whether to accept Huawei as part of our critical infrastructure moving forward. With 5G on the horizon, the question I have for both of your organizations is whether your platforms are prepared to use servers that are built, in whole or in part, by foreign entities that are likely subject to extrajudicial directions from a foreign government.

Ms. Terri O'Brien: I can answer only for Interac, but I can firmly say that we are not. We are not prepared to allow data outside of our Canadian constitution and Canadian roots. Our incorporation—we became a corporation about a year ago—is quite strongly grounded in Canada. All of our data is to reside in Canada. We are also to use Canadian vendors and Canadian suppliers in the delivery of any of our services, but we build our own technologies. To your question about foreign service providers, we are quite anchored in our Canadian roots.

Mr. Glen Motz: Before I get Payments Canada to respond to the question I asked previously, I just want to follow up with your comment. If you don't have a server from someone like this, what happens if the infrastructure on which you transfer your data has the ability to have switches that can be hacked by a foreign entity? How does that play into your security programs?

Ms. Terri O'Brien: All our infrastructure and data are resident in Canada and owned and operated by Interac.

To your question about a foreign entity as a hacker, our experience is that most hackers are foreign entities. We haven't seen a lot of domestic Canadian hackers.

● (1750)

Mr. Glen Motz: They access the information through the back door; they're not hacking the system. We're talking about certain foreign actors who, because of the technology that's in place, could potentially intercept communication that happens on a daily basis, and we don't even know it's being siphoned off.

Ms. Terri O'Brien: We do vulnerability scan controls and have intensive security scans. We use only Canadian networks, Canadian telecom providers, and have Canadian data centres in multiple provinces. We run our transactions only through our Canadian data centres, so I don't anticipate that.

Mr. Glen Motz: Okay. Thank you.

Payments Canada, what is your response to the first question?

Mr. Justin Ferrabee: As you can appreciate, we wouldn't discuss specific capabilities or principles or how we manage our infrastructure.

What you're raising is a very acute thing we're aware of and are concerned about. Part of the motivation for the tracking of supply chain ingredients is to know that, because we would have providers of a service who would have technology and they may not know exactly where it has all come from, so we wouldn't know.

We have to imagine that it is not safe or secure, and we have to prepare ourselves for that—and we are. We are aware of these risks, but without that kind of knowledge, even if they were to attest that this is true, it might not be true. We can't afford to take those risks, so we plan as if it's not and we try to make it so.

The Chair: You have a little more than a minute.

Mr. Glen Motz: A previous witness at committee some time ago —and I asked this the other week—called Canadians "innocent", which I thought was a very polite way of saying that we don't have a clue about our own cybersecurity.

From the perspective of both of you, what needs to change in Canada to get the consumer to get it, to be more vigilant in their own cybersecurity, and thus their own privacy? What role do we have as legislators to make sure we encourage them?

Ms. Terri O'Brien: While I am not privy to the comment, the "innocent" comment seems to be directed more at general public knowledge.

Mr. Glen Motz: Yes.

Ms. Terri O'Brien: Our resiliency in Canada, particularly with the financial institutions, is quite strong on a global scale.

To your question about Canadian consumers, I would agree. I think public education is immensely important. Certainly this time of year, with the level of CRA scams that come out, from both phone calls and emails that people receive—and I'm sure all of you are well versed in that—Canadians do get pulled into those scams. They don't have enough education or awareness to understand when they should hang up the phone or delete the email, and also to up the system security on their home computers, and how important that is.

The Chair: Thank you, Mr. Motz.

Mr. Graham, you have five minutes, please.

Mr. David de Burgh Graham: Thank you. I hope it's enough.

Mr. Cannings, I'll just tell you how the things we talked about earlier work. The postal code in your constituency office is V2A 5B7. If you're trying to use your postal code, you'd have the numbers from that: two, five and seven, plus zero, zero.

In the U.S., your postal code for the purpose of your card is 25700. Now you know how it works.

Mr. Richard Cannings: Okay. Next time I'm in Texas I'll remember that.

Mr. David de Burgh Graham: Have a safe trip, and keep in mind that your postal code is a public record. Everybody knows how it works now, so there you go.

The Chair: It might be fraud, but that's another thing.

Some hon. members: Oh, oh!

Mr. David de Burgh Graham: To come back to the matter at hand, we're talking about foreign-built devices. There is one thing I'm curious about, and this applies to both organizations. When you have third party software, or hardware for that matter, do you always get the source code, audit it and compile it yourself?

Mr. Martin Kyle: We do risk assessments on all the software and projects we deploy. Those risk assessments include an inventory of the libraries that are included in the applications that we develop, as well as any defects associated with those libraries.

The digital supply chain comes from all around the world. This microphone probably comes from many different countries around the world, so the risks that are represented in the components that make up this piece of equipment need to be assessed. They need to be assessed for vulnerabilities that could allow adversarial groups to enter this piece of equipment, or a piece of software.

We make sure that when we deploy something, it goes through a rigorous risk assessment process where we evaluate things as much as possible.

● (1755)

Mr. David de Burgh Graham: The question at the core is, do you have access to the source code of what you're using, or is the risk assessment "We don't need it in this case because we trust this company"?

Mr. Martin Kyle: We ensure that we do audits on the organizations that provide source code to us. We certainly have access to some of the source code. We build some source code. Where we don't have access to the source code, we go through a rigorous risk assessment process with the company that provides it to us.

Mr. David de Burgh Graham: Terri, is it the same story?

Ms. Terri O'Brien: No, actually. All of our high-risk and transaction-based systems are proprietary code bases. Proprietary code means that we have a large development team that builds the code themselves. We put it through quite rigorous security standards and vulnerability scanning. We have a managed detection and response, layered security protocols that are quite robust and a private, closed-loop network.

We do, of course, have the source code, because we have a team that writes the source code, and we have very robust security layers. We're constantly reviewing our security posture as well.

Mr. David de Burgh Graham: What does Interac know about a transaction? If I go to the store and buy something, what do you know about the transaction?

Ms. Terri O'Brien: I can share with the committee that all the data meets the minimum required standards in order to process the transaction, and any personal, identifiable information that is required to process the transaction to your bank account and not somebody else's bank account is fully secured.

Mr. David de Burgh Graham: How about what the transaction is actually for?

Ms. Terri O'Brien: Do you mean the intended use and purpose of the transaction in terms of the merchant where it's being purchased?

Mr. David de Burgh Graham: If you go to the gas station and buy gas and a bar of chocolate, does Interac know that you bought gas and a bar of chocolate, or that you went to the gas station?

Ms. Terri O'Brien: I can't share all the data elements that are collected, but I believe the transaction is about the money movement itself. It's not about the goods and services that you're looking to purchase.

Mr. Richard Cannings: Be careful what you're buying.

Mr. David de Burgh Graham: This applies to both of you. Do you have member institutions that do a poor job of living up to your standards? I know that in the case of Payments Canada membership is statutorily required for some organizations. Interac is probably the same thing. Do you have lagger organizations you're always chasing that are not keeping up with your standards? You don't have to identify them, but do they exist?

Mr. Martin Kyle: I would say that all the organizations that participate with Payments Canada have high security standards, and they all meet a very rigorous bar for safety and security.

Ms. Terri O'Brien: I would say absolutely the same. As the centre of the ecosystem, Interac spends a good amount of time with all of our participants—and we have many more participants—in giving them lead time and testing time when we're raising security standards, which we always are. We actively work with them to make sure they can make the new standards.

Mr. David de Burgh Graham: Thank you.

The Chair: Thank you, Mr. Graham.

Mr. Cannings, you have three minutes if you wish to use them.

Mr. Richard Cannings: You caught me off guard here.

The Chair: I can go back to somebody else.

Mr. Richard Cannings: Okay. Sorry, normally in my committee I never get a second chance.

The Chair: I'll go back to myself and ask about what I'm interested in.

I have my Visa card here with CIBC, and I have my debit card. On a security basis only, I would be given to understand from your testimony, Ms. O'Brien, that this is far safer than this.

Ms. Terri O'Brien: Yes. I would agree with that statement.

The Chair: Why? Is it because you have 300 organizations in this, and you are a closed loop? There are many more thousands of organizations in this.

What is the essential—

Mr. David de Burgh Graham: John, be careful not to show the numbers; we're televised.

The Chair: I've already been hacked on this. This one can't be hacked.

Mr. Michel Picard: He has no money anyway.

The Chair: Yes, that's right.

What is it in the structure that makes the one safer than the other?

Ms. Terri O'Brien: I think there are many factors. As I alluded to earlier, Interac has a very strong governance and operating regulations structure that is layered. It's not just about the security of a closed-loop network. It's about the participant's level of security, the issuers and acquirers, like the PIN pad level of security, as well as varying degrees of transaction types and limit structures, which is different from some of our credit card partners that we have in Canada, which may have a higher risk appetite.

They have different types of participants in their marketplaces, and different types of fraud monitoring, so I can't speak to the level of fraud monitoring, or their risk appetite. I just know that it's higher than ours in some regards, in their limits on certain different types of cards. As you may well know as a consumer, many cards have much higher limits. Those are more attractive targets for cybercrime than debit cards.

● (1800)

The Chair: So, it's not a function of how the system is set up or the security that's built into it; it's a function of how much risk we want to take in order to be able to do volumes of business.

Ms. Terri O'Brien: I think it's a function of both. It's a layered approach. It's a function of the security of the participants, of the operating regulations, of the limit structure, of the fraud risk monitoring—for sure, that's pivotal and key in that ecosystem.

The Chair: Thank you.

I have one other question, with respect to the sharing that's going on among the various institutions. Not all institutions will have the same degree of interest—that's not quite right. They're all interested, but they will have different agendas. Particularly, the government will have one agenda; the security people will have another agenda; the financial institutions will have another agenda and whoever else is in that.

Are you satisfied that, with the various agendas that are going on and your feeding in that data, security is actually enhanced at the end of the day?

Ms. Terri O'Brien: I would say yes, absolutely. It is further enhanced with every amount of information sharing that we have.

Of course, we participate, as Justin and Martin said, in a lot of central forums, in information sharing through some committees, and the CCTX has been a great addition in recent years. But the actual event sharing in the moment of a particular theme or threat vector that is in the marketplace at any given time is really pivotal to detecting it and preventing that fraud. Then it benefits the entire ecosystem. We at Interac will speak with individual financial institutions on a daily basis, because those threat factors continuously change. It's been quite effective.

The Chair: I'm assuming Payments Canada would adopt the same answer. Is that correct? Okay.

I have a final question for Payments Canada. I've never quite understood why, when I'm paying a bill online, the money clearly comes out of my bank account but is not credited to the vendor for a day or two or three. It puzzles me that it's not an instantaneous transaction. Do you have an answer to that?

Mr. Justin Ferrabee: Yes. As an infrastructure layer, we don't interact with consumers at the bill payment level, but part of our modernization program includes the creation of a real-time payment rail, which would do exactly that—eliminate the lag in deposits, cheque holds, bill payments and the like. So, if you keep your fingers crossed, you'll see one coming soon.

The Chair: Okay. Well, I'll lie awake at night waiting for that.

Some hon. members: Oh, oh!

The Chair: We have Mr. Cannings, and then Mr. Eglinski.

Mr. Richard Cannings: I'm just going to follow up on what Mr. McKay was asking, about comparing the credit card and the Interac model.

I had Mastercard representatives in my office last week telling me about their system. As I recall, Mastercard and Visa are more of an intermediary between banks, vendors and individuals, whereas Interac has sort of a direct line into your bank account. I'm just wondering if that adds more risk to a transaction, having that direct line into your bank account, whereas the other ones seem to be having more layers where security could kick in. Maybe it's the other way around. I don't use Interac a lot, and it's not because of this, but I'm just curious as to this direct access to your bank account. What sort of security questions come into that?

Ms. Terri O'Brien: I actually think it reduces the risk to have the closed-loop private network. For clarity, the direct connection is called an API, or an application programming interface that we have to the financial institution, through which all transactions flow. The sending institution—your bank, for example—would vet that you have the funds available and then send it in real time across our payment infrastructure to the receiving institution, and we would be able to facilitate those transfers. I do believe the direct connection reduces risk. We can monitor and manage the system appropriately.

● (1805)

Mr. Richard Cannings: Mr. McKay also mentioned bill payments, for instance. Is that similar? When I'm paying a bill, I don't think Interac is involved, but when I'm paying a bill through my bank, is it a similar process?

Ms. Terri O'Brien: Interac does do some of those transactions, and we're looking at it. Certainly, e-transfers are easy to understand. If you're paying a service provider, a plumber in your home, you may choose to use Interac e-Transfer, and those are real-time payments today.

The bill payment interface that you may use with, say, Rogers, to pay your cable bill, for example.... Today those payments are held at the financial institutions and then remitted through a batch process. We're actively working with them on how to make those payments real-time, because we have real-time capabilities already, but today, those are batch-processed payments at each of the Canadian financial institutions. It's just a legacy thing.

The Chair: Thank you, Mr. Cannings.

Now we have Mr. Eglinski.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you.

This is for Interac. Earlier, you stated that you kept all your stuff within Canadian servers and stuff like that, but you do provide international service to foreign cardholders. Is that correct?

Ms. Terri O'Brien: We do have some international remittance on our Interac debit product. I think somebody had an example. If you were in the United States and you wanted to withdraw money through your Interac bank card, you could use a third party ATM. We do have an ability for you to withdraw funds when you're in another country.

Mr. Jim Eglinski: Someone from a foreign country cannot use your system. Do you maintain a relationship with foreign banks in such a case?

Ms. Terri O'Brien: No, we do not maintain foreign banking relationships.

If you, as a Canadian consumer with a Canadian bank account, choose to withdraw funds if you're visiting Texas, for example, you can withdraw funds in Texas through your Interac debit card. But no, we do not maintain foreign banking relationships.

Mr. Jim Eglinski: I was wondering about security.

I'll turn it over to my friend, who had a question for you.

Ms. Terri O'Brien: Sure.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Mr. Eglinski.

I was away for a few minutes. I don't know whether the question has already been asked, but I don't think so.

How many direct attacks on systems do you experience each day or month?

Can you tell us where the attacks come from? Are the attacks carried out by individuals, by people in Canada or abroad? Are any attacks carried out by specific countries?

Both witnesses can respond.

[*English*]

Mr. Martin Kyle: As you can appreciate, we don't describe the details of our specific security capabilities or security incidents or events. Suffice it to say, the financial industry receives attacks all the time from everywhere.

[*Translation*]

Mr. Pierre Paul-Hus: Without providing the details of your organizations, can you tell us what type of attacks are carried out? Are the attacks carried out by isolated individuals or organizations? Can we have this type of information?

[*English*]

Ms. Terri O'Brien: It might be important for the committee to make a distinction between attempts and attacks.

I would say that all financial institutions, payment ecosystem providers and settlements providers are going to sustain attempts. At Interac, we have a managed detection and response, so that when there is an attempt to infiltrate our systems, we can see it. We're actively monitoring it and we're preventing it to make sure that it doesn't happen.

I'd say attacks are relatively few. What I do know of them, from some of our partners and through some of these forums where they're reported, is that in recent years they are sophisticated. I don't think we're seeing a lot of the one-off you described. They are more sophisticated attempts that are coming through.

[*Translation*]

Mr. Pierre Paul-Hus: Do you have an obligation to disclose to the banks? You're an intermediary between the different banks. When the threats are more significant, do you have a time frame, a number of hours in which you must inform the banks and the government?

When it comes to the government, I don't think that there's an obligation to disclose. However, in terms of your business partners, is there an obligation to disclose?

● (1810)

[*English*]

Ms. Terri O'Brien: We don't have an obligation to disclose among the various financial institutions. That's not a legislative requirement, but we do have trusted channels through which we do share some of that information for the betterment, safety and soundness of the ecosystem. We will share information on a very specific basis with the related FI.

[*Translation*]

Mr. Pierre Paul-Hus: You clearly referred to sophisticated operations, which require significant resources. Can you give us an idea of where the threats are coming from?

[*English*]

Ms. Terri O'Brien: I think the new cyber unit of the RCMP is probably best placed to pinpoint where in the world they're coming from. There are certainly various countries where we have seen attempts and attacks, but it does migrate around. It is global and it is sophisticated.

[*Translation*]

The Chair: Thank you, Mr. Paul-Hus.

[*English*]

You have five minutes, Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thanks very much, Chair.

Thank you for being with us.

I want to pick up where my colleague Monsieur Paul-Hus left off. I also serve on the Standing Committee on National Defence. This is one of those areas where, when we talk about critical infrastructure, there is some overlap.

Without getting into the details, as you pointed out, or giving us information that should not be disclosed, how concerned are you, generally speaking, about a state-to-state attack, and how much do you consider yourselves to be part of our core infrastructure? I'll maybe add to that question. What if your service does go down for a prolonged period through an attack? What would be the implications for the country?

Mr. Martin Kyle: First of all, as you've heard, we are safe. Security is our most important priority. We support our members, the financial institutions in Canada, in their security programs, and they support us in ours. Attacks and threats come from all sides. We must maintain a constant state of vigilance, and our members must do so as well. We rely on every Canadian citizen to be responsible for their own security. We also believe that together we can improve and increase the security of the country as a whole.

Mr. Sven Spengemann: Are you in any capacity at all working with analysts or staff of the Department of National Defence in protecting yourselves? Is there a collaboration on such issues as AI, quantum, things that would affect other parts of our critical infrastructure as well if they came at us?

Mr. Martin Kyle: Absolutely.

Mr. Sven Spengemann: Are you able to elaborate in a bit more detail?

Mr. Martin Kyle: No.

Mr. Sven Spengemann: Okay.

Are sufficient funding levels in place, in your assessment, to do that kind of work? Are there trajectories where we need to invest more, be it talent, structural work or thinking about it differently, as we go into AI and those kinds of questions?

Mr. Justin Ferrabee: We're very confident with what we have now. There is always opportunity and a need to continue to invest and improve. We are very confident and feel as though we have been responding well, as have our partners in government and elsewhere. There are also needs that emerge as we go, as you've heard. The bar is always rising, so the need to continue to invest, and potentially grow investment, is there.

Mr. Sven Spengemann: Is the degree of centralization of the clearance system that we see in Canada typical of other developed democracies—the G7 and the Five Eyes—or is there an argument to decentralize the clearing system so that any given attack will be able to do less damage if successful?

Mr. Justin Ferrabee: Our central clearing system is very similar to those of other G7 countries and other advanced financial infrastructures. We are always looking at opportunities to continue to strengthen the security. We are confident in the position we have right now, and we will always be looking. We've done a lot of research, which has been public, on distributed ledgers and their application. The low surface area and the high trust among parties are factors that diminish the need for a distributed ledger of some kind or some other new technology in that way, but we're always looking at it and investing in innovation.

● (1815)

Mr. Sven Spengemann: That's very helpful. Thanks very much.

The final question I have is strictly a personal interest question.

What percentage of consumer transactions in Canada, in your estimation, are done on a non-electronic, i.e., cash basis? What kinds of trend lines do we see? Is that data that you have?

Mr. Justin Ferrabee: We publish a report every year called "Canadian Payment Methods and Trends", which refers to that. You will see cash diminishing. We believe it will continue to decline, but it will never go away. It's below 50% now, and declining at a rate of somewhere between 5% and 7% a year.

Mr. Sven Spengemann: Thank you very much, Mr. Chair.

The Chair: Well, I must be in the declining minority, then.

We have Mr. Picard and Mr. Graham.

Mr. Michel Picard: Can I withdraw money from an ATM machine in London or Paris?

Ms. Terri O'Brien: I think in Europe there are some restrictions, but, yes, there are certainly ATMs that you could withdraw money from in Paris.

Mr. Michel Picard: Can I withdraw money from St. Petersburg or Moscow?

Ms. Terri O'Brien: No, that would violate sanctions rules.

Mr. Michel Picard: There's nothing available on the Russian side, using my Interac card.

Ms. Terri O'Brien: No. We would absolutely adhere to all sanctions rules in Canada.

Mr. Michel Picard: Okay. I'm done.

The Chair: That was quick.

Mr. Graham.

Mr. David de Burgh Graham: I'm going to build on an earlier question from Ms. Dabrusin on cheques, and perhaps the obsolescence of the cheque as we know it.

Is it time to dump account numbers, addresses and signatures on our cheques and switch to...? I don't know if we can have a paper version of a token, but is there is any way of doing that?

Ms. Terri O'Brien: Yes. Absolutely.

We're innovating new payment transmission technologies every day. The cheque continues, I would say, mostly in the small business space and a little bit in the retail consumer space, but not as much. There's really no need for a paper cheque anymore.

Mr. Justin Ferrabee: We would say that we're seeing a rapid decline at the consumer level. There are still some people who rely on it, and there are some circumstances where that's the only method of payment that is going to work, for a host of reasons. Where we see the biggest need is in the small business area, and usually it's for managing information, because currently information doesn't flow cleanly across the system in terms of to, from and all the notations, and they get a copy of the cheque so they can see it.

Until we can rectify or remedy that, we see a strong hold on cheques. We're making a number of moves to improve the information that travels with payments by publishing standards. One of the most current global standards for information is the ISO 20022 standard, which includes vast amounts of information to travel with your payment, which would allow a small business person to see more, including invoice and all kinds of other information that goes with that.

Our expectation is that the decline of the cheque will come with the introduction of more robust information to travel with the payment.

Mr. David de Burgh Graham: The cheques will continue to exist. Are you going to de-information that piece of paper?

Mr. Justin Ferrabee: No. We're going to replace it.

Mr. David de Burgh Graham: You're going to replace it completely. Okay.

[*Translation*]

Mr. Picard, do you have anything to add?

[*English*]

Mr. Michel Picard: I'll go back to Russia.

Mr. David de Burgh Graham: The Russians are coming.

Mr. Michel Picard: Part of the transaction, I guess.... It might be a bit complicated to know every member of your group, but if I withdraw money in Europe, those banks are part of your network somehow. I don't know how it works. Do you know, or is it possible to know whether banks outside Russia, in Europe and elsewhere, which are maybe owned by Russian interests, are part of your network?

Ms. Terri O'Brien: They're definitely not part of our network. I'd say the financial ecosystem in Canada has gotten quite mature and robust in our sanctions screening and in understanding transfer agencies and those types of things. We definitely secure the network.

We do very few transactions outside of Canada, so it's not a problem that we encounter or that we see.

Mr. Michel Picard: Now I'm done.

The Chair: Okay.

Mr. Eglinski, do you want to ask any further questions?

Mr. Jim Eglinski: I think I'm good.

The Chair: Mr. Paul-Hus.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

We've met with Mastercard representatives. Mastercard has red teams, which are known as “ethical hackers” in French. I know that there have been discussions about the term, and I don't know how you translate it. These people work internally and really try to break and outsmart the system to see whether it has any flaws. Do you have any similar teams in your company?

● (1820)

[*English*]

Ms. Terri O'Brien: We do. We have a very robust IT security team, which uses a number of tools that allow us to proactively scan the system for vulnerabilities and manage detection and response capabilities as well. We actively scan our systems on a daily basis and keep quite current.

[*Translation*]

Mr. Pierre Paul-Hus: You have internal information technology teams. You carry out scans. However, you don't really hire hackers, who will try to find the flaws in your system.

[*English*]

Ms. Terri O'Brien: We have a very large IT security team. We don't call them “white hat hackers”. We call them IT security. We have a large IT security team that's constantly testing—we call it penetration testing—and scanning the system. I think it's fundamentally the same. “Red team” and “white hat hacker” are kind of buzzwords these days.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

Mr. Justin Ferrabee: I can answer for Payments Canada. As you can appreciate, we don't speak specifics about the techniques we use, but we're well aware of those techniques, as well as other ones, and we employ those that are most suited for ensuring the safety and security of the system.

[*Translation*]

Mr. Pierre Paul-Hus: Lastly, the goal of our study is to look at the banking and financial system as a whole in terms of cybersecurity. As partners of the banking system, in your opinion, what are the main vulnerabilities with regard to cybersecurity?

[*English*]

Ms. Terri O'Brien: We see two vulnerabilities that I spoke to earlier in my remarks. One is a lack of ability of government, RCMP and law enforcement to openly share information. The criminal activity changes quickly. It is a real-time fraudulent environment, so the ability to access that information more quickly would enable us to have stronger defences than we already have today.

Two is public education, which you all seem quite aware of. Public education on what they should and should not do would go a long way to securing the system and the ecosystem.

[*Translation*]

Mr. Pierre Paul-Hus: Yes, we know.

[*English*]

Mr. Justin Ferrabee: It's an ecosystem, and there are many actors in it and varying degrees of capability and risk. We know we are stronger when we work together, and the answer to identifying vulnerabilities is to work together in identifying them and to each play our part in resolving and managing them. That's where we put our time and effort, and we believe our counterparts do as well. We support our members and anybody in the financial institutions in that coordination, and we're confident that's the best strategy.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Mr. Spengemann and Mr. Graham are going to share five minutes.

Mr. Sven Spengemann: Thank you, Mr. Chair.

Again, I fully appreciate the levels of confidentiality you need to preserve, but in the mind of this committee or the Canadian public, we sometimes get the perception that there's a qualitative difference between a state-led, state-directed or state-owned attack and what comes out of the private sector or the underground world. Is there qualitatively an appreciable difference in those attacks? Does a nation-state have greater capacity to do us harm, or is that misplaced, in the sense that if we are fighting effectively against attacks that come out of the “private sector”, we are as equipped to fight off a state-led attack or a series of coordinated attacks?

Mr. Martin Kyle: Certainly, nation-states have more resources than most criminal organizations, but unfortunately we've seen that some exploits that have been leaked from nation-states have ended up in the hands of criminal actors, which creates a threat environment that's constantly evolving. While we monitor these things and focus on the safety of the national payment system, we recognize that continued investment and focus are required to address all these threats.

Mr. Sven Spengemann: Both fronts are equal, and if you do it well, you're able to stave them off no matter where they come from.

Mr. Martin Kyle: That's correct.

Mr. Sven Spengemann: Okay, that's helpful. Thanks.

The Chair: Mr. Graham.

Mr. David de Burgh Graham: Just to build on that a little, the intent of a state actor in the financial system would not be to take the money. That's not their purpose. It's to see who is trading money with whom, to get the metadata, as we like to talk about, and be in a position to undermine the system when they push a button if they need to.

Would that be an accurate assessment of state actors in the system?

Mr. Martin Kyle: There are a number of motivations for various state actors. We've seen in the past that some state actors use financial systems to get around sanctions. Some state actors are motivated for other reasons. There are a myriad reasons for any threat against the financial system, and we need to be aware of all those reasons and take proactive countermeasures against those threats.

● (1825)

Mr. David de Burgh Graham: If a foreign country wanted to undermine our financial structure, its intention would not be to take data; it would be to shut down our system. I assume we are doing our utmost to prevent that from happening as well.

Mr. Justin Ferrabee: We would not be specific on any incident we are aware of. We assure you that we think about that and take action to prevent that, and that our colleagues in other organizations around us do the same. This is not an unknown for us, or something we're not aware of. We're very clearly focused on that.

Ms. Terri O'Brien: Yes, and our respective resiliency programs.... I can speak only for Interac, but we're at 99.9% uptime. You can achieve that uptime only if you have a resiliency strategy that includes very robust infrastructure to deliver on that, even during times of degradation of service or any attack that may attempt to disrupt the service.

Mr. David de Burgh Graham: On another topic, in the EMV technology, what does EMV stand for? I forget what the “E” is, but “M” is Mastercard and “V” is Visa. Is that correct?

Ms. Terri O'Brien: You know, the acronym's been around for a decade or so now, so—

The Chair: It's a music store.

Mr. David de Burgh Graham: HMV, that's a different thing.

Is there a qualitative difference between the credit card and debit card systems in anything we're talking about? What are the differences between the two networks and systems? Not that you have a biased position, but does one have an advantage over the other?

Ms. Terri O'Brien: I spoke to this a bit earlier. I can only speak to the closed-loop network that we have, but we really have a layered security strategy in fraud monitoring and a robust security and risk strategy. It's multiple different controls and security standards that we have on our network.

The Mastercard and Visa networks are largely based out of the U. S., and then operate on a global basis, so they have a different set of standards that they're going to meet, a differently layered security structure that they're required to meet and a different risk appetite. I can't speak as much to theirs. I can only speak to the safety and soundness that ours provides to Canadians.

The Chair: Thank you, Mr. Graham.

Just before I let you go, Wayne Gretzky famously said that you don't talk about where the puck is; you talk about where the puck is going. Some of the big developments in your industry are Apple, Amazon and various others. Would either one of you allow Apple into your systems?

Ms. Terri O'Brien: I can share from an Interac perspective that we were the first to market with Apple in putting the Interac debit card in the Apple wallet. That was the TSP technology that we spoke about earlier. We also have the same Interac debit card in the Google wallet, in the Samsung wallet. Canadians do want to be able to tap their phones in the same way they tap their cards. We have found the abstraction and tokenization of that data to be extremely secure and to be a really good security protocol. Leveraging the EMV technology has created a really secure product that has very little fraud associated with it.

The Chair: Canadian consumers using any one of those lines can be as secure as with a direct use of a Canadian bank product, then.

Ms. Terri O'Brien: It's akin to direct use of your Interac debit card.

The Chair: Right.

Payments Canada, go ahead.

Mr. Justin Ferrabee: We don't interact at the point of sale and would have no reason to interact with Apple as a payment provider. Our staff would likely use it, but it's not something that's in our systems or anything. It's not a point of interaction for us.

The Chair: Okay.

Thank you for that, and again I want to thank you for your patience. We have stressed your patience, but it is what it is. Thank you for a very interesting and useful testimony.

Ms. Terri O'Brien: Thank you for having us.

The Chair: With that, we're adjourned.