HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 171 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, July 15, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Monday, July 15, 2019

● (1330)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Folks, we're trying to get back on our timeline here. We are waiting for our other witness, but in the meantime, we will proceed with RCMP captain Mark Flynn.

You will make your presentation, and if the folks from the Communications Security Establishment come, we'll make arrangements for them to speak as well.

The meeting is now public, by the way.

For those who are presenters, the real issue here is that the members wish to ask questions. Therefore, shorter presentations are preferable to longer ones.

With that, Superintendent Flynn, I'll ask you to make your presentation.

Chief Superintendent Mark Flynn (Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police): You'll be happy to hear, as I understand the committee was informed, that I won't be making any opening remarks. I am present here today simply to address any questions you may have. As this, on its surface, does relate to an ongoing criminal investigative matter, it would be inappropriate for me to provide details of an investigation, particularly an investigation that is not being undertaken by the RCMP.

I welcome all questions. I am here to provide whatever assistance I can.

The Chair: Mr. Graham.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): It's a little harder to ask questions without an opening to work off.

The first question I have is this. If somebody calls the RCMP with a suspicion of data theft complaint, how does the RCMP treat that from the get-go?

C/Supt Mark Flynn: That will depend on the jurisdiction where it occurs. In the jurisdiction where we are, the police have jurisdiction, so they have the provincial and municipal responsibility. It would be forwarded to our intake process there, whether it be our telecoms office, the front desk of a detachment or a particular investigative unit that's identified for that.

In cases where we are not the police of jurisdiction, like in Ontario and Quebec where we are the federal police, we will become aware of these instances through our collaboration with our provincial and municipal partners. We will look at the information and determine whether or not there are any connections to other investigations that we have ongoing, and offer our assistance to the police of jurisdiction should they require it, although on many occasions this type of incident is very well handled. We have very competent provincial and municipal police forces that are able to handle these on their own.

Mr. David de Burgh Graham: At what point does something become federal? If something is provincial jurisdiction but affects multiple provinces, does each province have to deal with it separately or is the RCMP able to step in at that point?

C/Supt Mark Flynn: The RCMP doesn't automatically step in solely because it crosses multiple provinces. As occurs with traditional crimes, whether a theft ring on a border between two provinces, or homicides, the police forces in those jurisdictions are used to collaborating and do so very well.

When there's an incident that occurs from a cyber perspective, if it's going to have an impact on a Government of Canada system, a critical infrastructure operator or there are national security considerations to it, or if it's connected to a transnational, serious and organized crime group that already falls within the priority areas we're investigating, then that matter will be something we will step into.

From a cyber perspective, we have ongoing relationships and regular communication with most of the provinces and municipalities that have cyber capabilities within their investigative areas. We know that many of these incidents occur in multiple jurisdictions, whether they be domestic or international, so coordination and collaboration are really important.

That's why the national cybercrime coordination unit is being stood up as a national police service to aid in that collaboration, but prior to that being implemented, one of the responsibilities of my team in our headquarters unit is to have regular engagement, whether regular telephone conference calls or formal meetings where we discuss things that are happening in multiple jurisdictions to ensure that collaboration and deconfliction occurs, or on an ad hoc basis. When a significant incident occurs, our staff in the multiple police forces will be on the phone speaking to each other and identifying and ensuring that an appropriate and non-duplicating response is provided.

Mr. David de Burgh Graham: In the case of the incident we're here to discuss, which is obviously a major incident, is the RCMP being kept apprised of what's happening, even if it's not their investigation?

C/Supt Mark Flynn: I'd like to stay away from discussing this particular investigation, but I can tell you that investigations of this nature absolutely will lead to discussions occurring. That happens as a consequence of the fact that we do have those regular meetings, whether it be in cyber or other types of crime that are going on in different jurisdictions. These, obviously, on a scale of this nature, would lead to discussions.

I am not involved involved in any of those discussions at this time. It is not something I have knowledge about.

Mr. David de Burgh Graham: Understood.

Okay.

The Chair: Mr. Drouin, welcome to the committee.

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Thank you, Mr. Chair.

Mr. Flynn, thank you for being here. I know that you will not comment on the ongoing investigation, but as a member of Parliament who represents a lot of members who have been impacted—I have been impacted as well—I am looking more at the potential impacts of fraud.

I know that many Canadians get fraudulent calls from CRA. I myself called back somebody who pretended they were you guys. They wanted to collect some money for a particular person. They were demanding. They were really adamant. They gave a callback number, and I provided that callback number to the police. Is that something you would advise Canadians to do where obviously the RCMP, or your local police force, is the first point of contact?

● (1335)

C/Supt Mark Flynn: Absolutely. We actually have a program at the Canadian Anti-Fraud Centre and a close relationship with telecommunications service providers, who have been very helpful in addressing some of the challenges we've had around telemarketing and the mass fraud committed over the telephone. As we learn about numbers that are utilized for fraud, we are validating that, and the telecoms industry is blocking those numbers to reduce the victimization. We have adapted some of our practices to ensure that this occurs at a much more timely rate than it has historically.

Mr. Francis Drouin: Just from your experience, and learning from cases of fraud, we know that some of them may have my social insurance number. They may have my email address, as well as my civic address. It could be a very convincing case for them to pretend that they're either a government official or from some type of financial institution. What would you advise Canadians on the best way to protect themselves?

C/Supt Mark Flynn: With any mass fraud campaign, whether it be tied to an instance like this or just in general, people need to have a strong sense of skepticism and take action to protect themselves. There are many resources under the Government of Canada, with such organizations as the Canadian Anti-Fraud Centre and Get Cyber Safe, that provide a list of advice for Canadians. It simply comes down to protecting your information and having a good sense of doubt when somebody is calling you. If it's a bank calling, call your local branch and use your local number. Don't respond to the number they provide and don't immediately call back the number they provide. Go with your trusted sources to validate any questions that are coming in.

I have experienced calls similar to yours. I had a very convincing call from my own bank. I contacted my bank and they gave me the advice that it was not legitimate. It was interesting, because in the end it turned out to be legitimate, but we all felt very safe in the fact that the appropriate steps were taken. I would rather risk not getting a service than compromising my identity or my financial information.

Mr. Francis Drouin: Okay. Great.

Thank you.

The Chair: Mr. Paul-Hus, you have seven minutes.

[*Translation*]

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

Thank you, Mr. Flynn. I'll come back to you in a few moments.

The leader of the Conservative Party of Canada, Andrew Scheer, asked me to contact my fellow committee members to convene this meeting. He sent an open letter to the media on July 12, and I'd like to paraphrase a few paragraphs.

> Like the vast majority of Quebecers and all Canadians, I am worried about the the security of our information technology systems, identity theft and privacy protection.
>
> This is a very serious situation, and I understand the fear and anxiety of the victims, whose personal information, including their social insurance number, was stolen. They are worried about how this will affect them in the future. They will have to spend considerable time and energy dealing with this.
>
> It is reassuring to see that the leadership at Desjardins Group is taking the matter seriously and working hard to protect and reassure members. The federal government, too, has a responsibility and duty to support all victims of identity theft by learning from the past and strengthening cybersecurity in partnership with all stakeholders across the industry.…
>
> I want the victims of this data breach, as well as all Canadians, to know that we stand with them and that a future Conservative government would be committed to tackling the privacy challenges confronting Canadians.

[*English*]

The Chair: Well, we thank Mr. Scheer for that wonderful message.

[*Translation*]

Mr. Pierre Paul-Hus: We want to be very clear about what an important and serious issue this is—so important, in fact, that we felt it was necessary for the committee to meet on this sunny July 15.

Mr. Flynn, you answered the questions of my Liberal colleagues, but I find the RCMP's response to the situation rather weak. Allow me to explain. Some 2.9 million Desjardins account holders are very worried right now. About 2.5 million are Quebecers, and 300,000 are in Ontario and other parts of the country. For the past three weeks, constituents have been contacting our offices non-stop, and the government has yet to respond. The reason for today's emergency meeting is to figure out what the federal government can do to help affected Canadians.

You said the RCMP isn't really involved, but can't it do something given that it has its own cybersecurity unit, works with organizations like Interpol and has access to other resources? I don't want to interfere in a police investigation, but we heard that people's personal information was being sold abroad. Isn't there technology or techniques the RCMP can use to detect potential fraud?

● (1340)

[*English*]

C/Supt Mark Flynn: The RCMP's role, as I explained earlier, in many of these situations is to work with our provincial and municipal partners. It's important to recognize that our provincial and municipal partners are very skilled at responding to many of these incidents. It's not always the case that the RCMP has additional powers, authorities or capabilities to the ones they have when dealing with an incident that is singular in nature, where an individual is involved in a single event, as opposed to a broader one.

However, there's always a standing offer from the RCMP to our provincial and municipal partners, that should they require technical assistance, advice or guidance, we are available to them for that. It would be inappropriate for the RCMP to inject itself into the jurisdiction of another police force to run the investigation they are operating.

[*Translation*]

Mr. Pierre Paul-Hus: I understand what you're saying about the investigation probably being conducted by the Sûreté du Québec, but what the Conservatives and NDP want to know is this. What can the RCMP do about the personal information of 2.9 million people that was handed over to criminals? I don't want to discuss the investigation; I want to know whether you have resources. If you don't, we want to know. That's why we are here today. If personal data was sold on the international market, neither the Quebec provincial police nor Laval police is going to deal with it. I think it falls under RCMP jurisdiction.

[*English*]

C/Supt Mark Flynn: Again, outside the scope of this particular investigation, cybercriminals do commit the majority of their crimes to gain access to personal or financial information for the purposes of gaining access to financial institutions and the money that's housed in those locations. The RCMP work continuously with the international community to identify and pursue the individuals who are committing a great number of these crimes.

The RCMP are working closely right now with those international partners, as well as many of the large financial institutions in Canada and the Canadian Bankers Association, to ensure that we are targeting the individuals who are causing the most significant harm. Our federal policing prevention and engagement team has hosted sessions with both the financial institutions and the cybersecurity industry. We have a new advisory group that's helping us target those individuals.

As far as knowledge goes, it's only in the hands of those cybersecurity and financial institutions. We're trying to ensure that as we are putting the resources we have into investigations, we are targeting those individuals who are causing the most harm.

We do that, as well, internationally. As incidents occur, we speak to our international law enforcement partners. We identify the behaviours we have in our cases or in our Canadian law enforcement partners' cases, so that if there are connections or individuals who are in those other jurisdictions, we're using the mutual legal assistance treaty, and we're using police-to-police collaborative efforts that we have to ensure that, internationally, all of those efforts are put towards a problem.

Now, I want to stay away again—and I apologize for doing that—from this exact incident. I cannot express what is or is not being done in this particular incident.

[*Translation*]

Mr. Pierre Paul-Hus: Since the problem came to light, has the RCMP set up a special unit to help deal with it?

[*English*]

C/Supt Mark Flynn: I am unable to speak about this particular incident. It would be inappropriate for me to do so.

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

[*Translation*]

Mr. Dubé, you may go ahead for seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

Thank you for being here today, Mr. Flynn.

It's important that we talk about this situation because, as my colleague pointed out, people are worried. It's essential that we find out more about the federal government's capacity to take action and the means we have at our disposal, especially since the committee just wrapped up a study on cybersecurity in the financial sector before Parliament rose in June. I'll touch on some of the things the committee looked at in its study because they pertain to the matter at hand.

I'd like to follow up on some of your answers. First of all, it is rumoured that personal data was sold to criminal organizations outside Quebec and Canada. I know you can't comment on this case specifically, but at what point does the RCMP step in to assist the highly competent people at such organizations as the Sûreté du Québec when a case involves a criminal organization operating outside Canada that the RCMP is already monitoring?

● (1345)

[*English*]

C/Supt Mark Flynn: We have formal, regular engagement with our policing partners across the country. That occurs on a monthly basis in the cyber area, as well as biweekly in some other areas. However, when there are incidents such as this, as you described, there are immediate calls that go out to ensure that collaboration is occurring and that any of our international partners' information that's relevant could be utilized to aid in those investigations.

[*Translation*]

Mr. Matthew Dubé: Thank you.

You said local police forces, the Sûreté du Québec and the Ontario Provincial Police were very competent when it came to dealing with cybersecurity issues and had significant powers. Does the RCMP have special expertise or information that could help them?

The reason I ask is that the government touted the consolidation of the cybersecurity capacity of the Communications Security Establishment, or CSE, the RCMP and all the other agencies concerned as a way to ensure information was shared and everyone was on the same page. I'll be asking Mr. Boucher, of the Canadian Centre for Cyber Security, about this as well when we hear from him.

Do you engage municipal or provincial police, as the case may be, in the same way?

[*English*]

C/Supt Mark Flynn: Yes, we do. We work very closely, as I've stated, with our provincial and municipal police agencies. In fact, I take great pride in the fact that at some of those meetings that I described, where our federal policing prevention and engagement team brought together the private sector, financial institutions and cybersecurity, one of those policing partners actually stood up at the front of the room and thanked the RCMP for the collaboration they are seeing in the area of cyber, which is far better than anything they've ever seen in their career.

I take great pride in that because that has been a priority for me, my staff and our engagement folks, to ensure that we are not being competitive but are being collaborative and, in that collaboration, we are supporting each other. We are not superseding other police forces' authorities, but we're also ensuring that we can assist the others in that.

[*Translation*]

Mr. Matthew Dubé: Thank you. I don't mean to cut you off, but I have a limited amount of time.

When the committee was studying cybersecurity in the financial sector, we talked about the fact that people tend to think of state actors as being the threat. I won't name them, but I'm sure everyone has an idea of the countries that could pose a threat to Canada's cybersecurity.

I realize you can't talk about it, but in this particular case, we are dealing with an individual—an individual who poses a threat because the stolen data can be sold and could end up in the hands of state actors. One of the things the committee heard was that individuals represent the greatest threat. Is that always the case? Does a lone criminal wanting to steal data pose a greater threat than certain countries we would tend to suspect?

● (1350)

[*English*]

C/Supt Mark Flynn: The threat comes from multiple directions, and I can't say which is greater, because, in our experience, we have seen a significant number of organized groups or individuals perpetrating the crimes across the Internet. The Internet is an enabler as much as it's a tool for us to use in leveraging and utilizing all the fantastic services that are out there.

[*Translation*]

Mr. Matthew Dubé: I have to cut you off because I'm almost out of time.

Has the presence of organized groups or countries with ill intentions seeking to buy personal data created some sort of marketplace? Do individuals like the alleged perpetrator in this case have an incentive, albeit a malicious one, to steal information and sell it to interested parties? Does the existence of these groups incentivize individuals who have the expertise to do things they wouldn't normally do?

[*English*]

C/Supt Mark Flynn: Yes, absolutely. We have seen a rise in what we refer to as cybercrime as a service to aid others who are less skilled at committing cyber offences, whether they are creating the malware, operating the infrastructure, or creating the processes by which somebody can monetize the information that is stolen. That is a key target area for the RCMP under our federal policing mandate, and we are targeting those key enabling services so that we can have the most significant impact on the individual crimes that are occurring, as opposed to chasing each individual crime.

[*Translation*]

Mr. Matthew Dubé: Thank you again for taking the time to meet with us today.

[*English*]

The Chair: Thank you, Mr. Dubé.

We have now been joined by Mr. André Boucher from the CSE, and I am going to give him an opportunity to make his statement.

I'll say to you what I said to Superintendent Flynn, that we are encouraging shorter statements rather than longer statements so that members will have more opportunity to ask questions.

Mr. Fortin, I see that you want to—

[*Translation*]

Mr. Rhéal Fortin (Rivière-du-Nord, BQ): If I may, Mr. Chair, I'd like to ask the witnesses questions. I'm not sure whether the agenda allows for that, but if so, I'd like a few moments.

[*English*]

The Chair: No, it's not, and I'm sorry, but you're not going to be able to speak to the witnesses.

[*Translation*]

Mr. Rhéal Fortin: No?

[*English*]

The Chair: No, not right now. Thank you. We're still in this hour cycle.

Mr. Boucher, as I said, shorter is better than longer. Thank you.

[*Translation*]

Mr. André Boucher (Assistant Deputy Minister, Operations, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair. As requested, I'll keep my presentation on the shorter side.

Mr. Chair and honourable members of the committee, my name is André Boucher, and I am the associate deputy minister of operations at the Canadian Centre for Cyber Security.

Thank you for the opportunity to appear before you this afternoon.

Let me begin with a brief overview of who we are.

The Canadian Centre for Cyber Security was launched on October 1, 2018 as part of the Communications Security Establishment. We are Canada's national authority on cybersecurity and we lead the government's response to cybersecurity events.

As Canada's national computer security incident response team, the cyber centre works in close collaboration with government departments, critical infrastructure, Canadian businesses and international partners to prepare for, respond to, mitigate and recover from cyber events. We do this by providing authoritative advice and support, and coordinating information sharing and incident response.

The cyber centre's partnerships with industry are key to this mission. Our goal is to promote the integration of cyber defence into the business model of industry partners to help strengthen Canada's overall resiliency to cyber threats. Despite these efforts and those of Canada's industry, cyber incidents do still happen.

This brings me to the topic we are here to discuss today. The cyber centre is not in a position to provide any details on this incident and does not comment on the cybersecurity practices of specific businesses or individuals. Any cyber breach, not just this specific instance, can be taken as an opportunity to revisit best practices and to refine systems, processes and safeguards.

In this case, media reporting and public statements indicate that the disclosure of personal information occurred as a result of the actions of an individual within the company—what is termed insider threat.

[*English*]

In our recent introduction to the cyber-threat environment, the cyber centre described the insider threat as individuals working within an organization who are particularly dangerous because of their access to internal networks that are protected by security parameters. For any malicious actor, access is key. The privileged access of insiders within an organization eliminates the need to employ other remote means and makes their job of collecting valuable information that much easier. More broadly, what this incident underscores is the human element of cybersecurity. The insider threat is only one example of this.

Cybercriminals have proven especially adept at exploiting human behaviour through social engineering to deceive targets into handing over valuable information. Fundamentally, the security of our systems depends on humans—users, administrators and security teams.

What can we do in a world of increasing cyber-threats? At the enterprise level, adopting a holistic approach to security is critical. This means starting with a culture of security and putting in place the right policies, procedures and cybersecurity practices. This ensures that when something goes wrong, as it almost inevitably will, there is a plan in place to address it.

Then we need to invest in knowing and empowering our people. Training and awareness for individuals and businesses are very important. Only with awareness can we continue to develop and instill good security practices, a fundamental step in securing Canada's cybe systems.

As well, we always need to identify and protect critical assets. Know where your key data lives; protect it; monitor the protection, and be ready to respond.

At the cyber centre, we'll continue to work with industry and to publish cybersecurity advice and guidance on our website. We regularly issue alerts and advisories on potential, imminent or actual cyber-threats, vulnerabilities or incidents affecting Canada's critical infrastructure.

Under, we hope, different circumstances, we'll continue to participate in conversations like this one, which help to keep the spotlight on these issues.

Ultimately, there is no silver bullet when it comes to cybersecurity. We cannot be complacent; there is too much at stake. While long-promised advances in technology may make the task easier, the need for skilled and trustworthy individuals will remain a constant.

Thank you, and I look forward to answering your questions.

● (1355)

The Chair: Thank you, Mr. Boucher.

Next is Monsieur Picard for seven minutes.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): I would like to preface my remarks by pointing out that the incident we are discussing today falls entirely within the parameters of the study we began in January on cybersecurity and financial crime.

As suggested by my fellow Liberal members, I put forward a motion that we study the issue. That shows how deeply concerned we are about cybersecurity in financial institutions. I'm delighted that Mr. Scheer commended our efforts in relation to the study. He fully supports my motion, and I'm glad that his party is joining the Liberal Party in its efforts to address the issue of cybersecurity in financial institutions, so thank you.

Mr. Flynn, I think it's important to speak to Canadians today to help people manage their expectations when something as serious as identity theft occurs.

The public wants the police to conduct a criminal investigation. Generally, people want something done about the loss of their personal information. They want their identity to be restored, without having to worry that five, 10 or 15 years down the road, they will once again be targeted. In terms of a criminal investigation, what are people's expectations?

[*English*]

C/Supt Mark Flynn: From a policing perspective, I believe that the public expectation is that police are going to pursue the person and anyone associated with that person who is involved in either the theft or the monetization of information—whether through cyber-threat, cyber-compromise, insider threat, or so on—and hold them to account and bring them into the judicial process to ensure that there are consequences, and that steps are taken to prevent this type of incident from occurring.

[*Translation*]

Mr. Michel Picard: It's very hard for people to understand just how difficult it is to prove that you are the person you say you are. How are people supposed to prove their identity? It's extremely challenging when three different people are out there using the same name and social insurance number.

● (1400)

[*English*]

C/Supt Mark Flynn: It's not an area of expertise for me, as a police officer, to confirm identity. I would go back to my earlier statement about using your local resources, whether it be financial institutions or other types of service. If you're able to use a local service to confirm it, that is your best way to deal with those companies when there are questions about your identity.

[*Translation*]

Mr. Michel Picard: To a certain extent, the criminal investigation is a way to ensure justice is served, provided that it leads to the perpetrators being nabbed, the evidence being used to successfully prosecute them and their being punished, mainly sent to prison.

That said, data on the black market represent virtual assets, ones that aren't housed in a physical location. Data can be located in many places. I'm not trying to alarm people, but it's important for them to understand that, even if the perpetrators are arrested, it doesn't necessarily mean that their data are no longer vulnerable and their identity can be restored.

[*English*]

C/Supt Mark Flynn: That is correct. It's important to point out that the only measure of success is not necessarily prosecution. In fact, in the cyber area many of those prosecutions will occur in other jurisdictions as we work collaboratively.

One of the approaches in the RCMP, and I know in some of our other police forces as well, is that we are bringing financial institutions and cybersecurity experts into our investigations. That is different from what we traditionally have done in our criminal investigative efforts. That has already borne fruit. It has already provided significant advantages. Those “partners”, as I refer to them, are able to see information that we as police officers might not know is important and we may not independently be able to identify that this could be used to provide protection for their customers. I know of at least one incident in a major investigation we've been undertaking where several financial institutions, through that collaboration, were able to identify and reduce potential harm to accounts that through that sharing were identified as compromised.

So I think the approach we are taking is providing benefits that are not solely measured by arrest and prosecutions.

[*Translation*]

Mr. Michel Picard: Mr. Boucher, your centre provides advice to other organizations. How can a business protect itself from its own staff? What advice do you have for businesses in that regard?

As we saw this winter, there is every reason to believe that banks, financial institutions and financial service companies have the best possible technology to protect their data from outside threats. What concerns us are threats from the inside. I don't think any software out there can protect against that risk. How do you advise organizations to safeguard against the human element when it comes to fraud?

Mr. André Boucher: Thank you for your question.

That ties in with my opening statement. A few tools are available, but what works best is going back to the basics—in other words, taking a holistic approach to security.

First, that means a well-established internal security regime for staff. It is important to understand exactly where the information that needs protecting resides, to know the individuals the organization works with and to constantly update the security regime. An individual's personal situation can easily change after they've been interviewed, so an organization should have those kinds of conversations with staff members on a regular basis. For individuals, a clear training and education program should be in place, one that includes refreshers, and the underlying processes should be clear.

IT teams have access to data loss prevention tools that can help to detect fraud. By the time fraudulent activity is detected, however, it's often too late. It is therefore important that organizations invest as early as possible in measures that build trust and confidence and that they work with reliable people.

[*English*]

The Chair: Thank you, Mr. Picard.

Mr. Motz, you have five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair.

Thank you, witnesses, for being here.

Mr. Boucher, I was intrigued by your opening comments on the Canadian Centre for Cyber Security being the national authority on cybersecurity and leading the government's response to cybersecurity events:

> As Canada's national...security incident response team, the Cyber Centre works in close collaboration with government departments, critical infrastructure, Canadian businesses, and international partners to prepare for, respond to, mitigate, and recover from cyber incidents.

That's fantastic. It also leads to this question by me: What standards or measures do we have in place now? We consider banking in Canada to be a critical infrastructure in this country. What standards are in place at this moment to ensure that those are met? Do we have incentives? Do we have penalties? Do we have anything in the way of ensuring that we have a uniform approach across the industry to make sure that Canadians are safe? It's Canadians we are here for and are serving in that capacity. I'm curious to know if we have a mandatory baseline that everybody needs to operate at. If we don't, how come? And how can we?

● (1405)

Mr. André Boucher: Thank you for your question. It's a vast question. I think you will have testimony this afternoon from experts from that specific sector of financial institutions.

I would say that from a cybersecurity perspective, the financial sector is quite mature, where we have both regulators in place and best practices that are part of the community. As cybersecurity-focused experts, we put a lot of effort into that collaboration in those best practices. We leave it to the regulators who are sector-specific to put in those minimum standards and guidelines that need to be in place, enforced and reviewed. We in fact appeal to the best and try to tease that up as much as possible for entire sectors, in this case the financial sector. The financial sector is one that's very mature. It's one where collaboration is established. It is where reputational risks are measured at their true value. Significant investments are made in that regard.

From a Canadian perspective, I would feel quite reassured that as a sector, there are both minimum standards and applications through the regulators that are in place and teams that are working at bringing the best out of enterprises so that they perform as well as possible.

Mr. Glen Motz: Approximately 2.9 million entities, individuals and Canadian businesses, are impacted by this particular occurrence, but millions of others across this country have also been victims of having their identities and credit card information stolen. They may not find solace in that particular statement that we have a mature banking industry in this country, because they continue to be victimized. I'm curious to know whether we are as vigorous in that way as we could or should be in pursuing the financial security of those institutions and of the people who put their trust in them.

Mr. André Boucher: I can assure you that we're quite vigorous in taking all the measures at our disposal, whether they be best practices in collaboration or measures that are enforced and in place.

The sad or unfortunate reality that we all have to compose with is that, as was pointed out earlier, when data gets lost and gets in the wild, we never get to recover it. It is not like a tangible asset that you can go and purge and bring home. It is a new reality for clients, it is a new reality for customers and it is a new reality for enterprises.

I would go back to the comment I made earlier that it just puts more fuel into the need to invest early, with early investments in having programs, in choosing our employees better, and in making sure we have a holistic approach to security to make sure we don't find ourselves trying to recover our losses.

Mr. Glen Motz: Okay. Thank you.

Chief Superintendent Flynn, as we've learned from this circumstance and from others, data is the hottest commodity on the dark web. We know that. People's names, addresses, dates of birth, social insurance numbers, IP addresses, email addresses—all those sorts of things are commodities that are traded at will on the web. I guess a couple of things come to mind for me. Can you help the Canadian public understand, number one, how that information is used by the criminal element, and number two, how they can then be vigilant? You answered Mr. Drouin partially with a response, but as the law enforcement agency in this country, what red flags or alarms could you make the Canadian public aware of that they need to be vigilant about if they've been compromised, and even before they become compromised?

The Chair: Mr. Motz asks an important question. Unfortunately, he's left you no time to answer it. I would invite you to work an answer into a response to another member. We have three hours' worth of hearings here, and if I don't keep this on track, we'll get lost.

Ms. Dabrusin, you have five minutes, please.

● (1410)

[*Translation*]

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

When we did our study on financial institutions and cybersecurity, we heard that banks had extensive security measures in place—something people may be questioning now. We also heard people being talked about as though they were cardboard boxes.

What can people do to better protect themselves? Can you give us any helpful information or details? Is there a place where members of the public can turn for information on how to better protect themselves—a website or a telephone line, perhaps? Is there anything you can tell us, Mr. Boucher?

Mr. André Boucher: Thank you for your question.

We have an extensive program. On our website, cyber.gc.ca, people can find information on how to protect themselves. Of course, people have to be aware when they are online. That is the most basic rule of cybersecurity. People have to know not only how to use the Internet, but also what they are sharing with others online. We are constantly running campaigns to educate people on using their devices securely and being smart about who they choose to share confidential information with.

Having the best protection and keeping it up to date is the first step, but making smart choices is another. People should visit only the sites of companies they consider to be reliable and reputable. Once they've done those two things, people need to choose what information they agree to share with the company. It's a three-step approach, and it is all available in the information and guidance we provide to people.

Ms. Julie Dabrusin: I see.

I also saw a lot of information about passwords. For instance, it mentioned people who use the same password for all of their online accounts.

Can you share some things people can do to protect themselves when it comes to their passwords? That's an important element.

Mr. André Boucher: Yes. I always look for opportunities to promote our website, so on our website, we talk specifically about how long and complex passwords should be. We also provide some tips. I encourage people to explore our website for themselves. It is often said that people should change their passwords regularly, but the problem with that is having to memorize a bunch of ever-changing passwords. The guideline has evolved over time. Nowadays, it is recommended that people choose at least one strong password, using certain parameters, which are available online, based on password length and/or complexity, depending on the available options. If it's possible to have a password containing up to 15 characters, people should try to choose a password that uses all 15 characters. If the password can have only eight characters, that's pretty bad, but people should at least choose a more complex password.

Constantly changing one's passwords is of minimal benefit if it means people have to write them down somewhere or use the same one for many different sites. What we want people to do is be diligent about choosing their passwords: choose something that is unique and as strong as the provider's parameters allow. People can use the same password, but if a data breach occurs, they have to act fast, changing their password and taking additional security measures. It's important to do a combination of things.

Ms. Julie Dabrusin: The other problem is that once people have a password that works well, they use it for all their online accounts. Some sites tell users that their passwords have to be longer, more complex or what have you, but they never remind people not to use the same password all the time or to use a different password than they do for other accounts. Would you mind talking about that as well?

Mr. André Boucher: Now you're asking me to be very pragmatic.

Ms. Julie Dabrusin: Yes, but this is pragmatic stuff.

Mr. André Boucher: What I would advise people, other than being very pragmatic, is to base their passwords on their level of uncertainty when it comes to the various online services they are using. For instance, for online banking, people should use a number of distinct passwords that are as complex as possible. However, for their online account with their local curling club, say, people may wish to be a little less rigorous and use the same password a few times, even though that isn't what I would recommend.

Ms. Julie Dabrusin: What can banks do to better educate the people using their services?

Mr. André Boucher: I believe most, if not all, banks require a minimum level of sophistication when it comes to the passwords they accept. They already have a certain standard in place to protect themselves from clients who are less diligent than they should be in selecting a password.

[*English*]

The Chair: Thank you, Ms. Dabrusin.

Mr. Clarke, welcome to the committee. You have five minutes, please.

[*Translation*]

Mr. Alupa Clarke (Beauport—Limoilou, CPC): Thank you, Mr. Chair. I'm very pleased to be here today.

Thank you, gentlemen, for being here and giving up your time to reassure Canadians and answer our questions.

One of the cornerstones of the social contract that exists across this land is the protection of citizens, not just the protection they offer one another, but also the protection provided to them by the government. For the past three weeks, constituents in all of our ridings have been profoundly concerned. Two days after the data breach was made public, people started coming to my office. When I would knock on people's doors, that's all they would talk about. That tells me people are genuinely concerned and feel that the government has done nothing in response.

The question my constituents want you to answer, Mr. Boucher, is very simple. Can the Canadian Centre for Cyber Security indeed ensure the 2.9 million Canadians affected by this data breach are properly protected, yes or no?

Does your centre have the tools to respond to the situation and ensure the victims of identity theft are protected?

● (1415)

Mr. André Boucher: It's fair to say that the Canadian Centre for Cyber Security has the resources to deal with all aspects of cybersecurity. The case we are talking about today involves an insider threat and stolen information. Strictly speaking, it's not a cybersecurity issue.

Mr. Alupa Clarke: I'm not talking about what's already happened. I'm talking about what's going to happen next. That's what worries people. I want to know whether the Canadian Centre for Cyber Security has the capacity to deal with international or national fraudsters who send text messages or whatever it may be.

Does your centre have the capacity to deal with that?

Mr. André Boucher: I'm not trying to evade the question, but the issue actually comes down to legislation or fraud. It's not a cybersecurity problem. That's not to say, however, that, if we see something happening, we aren't going to respond.

The first thing we do every day is talk to our partners, including the RCMP, to share what we know and update them on anything new. We make sure that whoever is responsible for the matter does something with the information we provide. The national team is the best there is and won't let anything fall by the wayside. The members of the team endeavour to fix any problems and do everything they can to keep Canadians' information safe.

Mr. Alupa Clarke: I'm going to take advantage of your cybersecurity expertise.

Is Canada's current social insurance number regime appropriate in a modern age dominated by the Internet? We are at the point now where people shop on their cell phones and pay for their purchases at the cash in mere seconds. Is our system of social insurance numbers adequate in the world we live in?

Mr. André Boucher: Thank you for your question. You don't ask easy ones, Mr. Clarke.

I'm not an expert in social insurance numbers or their use, but I can talk about identifiers. No matter what identifiers are used, whether they involve complex or simple cryptology, information management is always an issue and the potential for data theft always exists. It's a very complex issue, and I'm going to let the experts in social insurance numbers speak to your specific question.

The bigger problem, as I see it, is how identifiers are managed. They are key pieces of information, and learning how to manage them properly in the large security systems I was talking about earlier is crucial.

Mr. Alupa Clarke: Superintendent, my next question is along the same lines as that of my fellow member, Mr. Motz.

Whether they've approached me on the street, come to my office or answered the door when I was canvassing, everyone has asked me the same question. They want to know what crimes these fraudsters are going to commit down the road. They want to know what to expect. What crimes will the 2.9 million victims of this massive data breach be the target of in the future?

In addition, how long will it be before those crimes are committed? The media are reporting all kinds of things. We are hearing that it will take five or 10 years before the fraudsters do anything—that they'll wait until the dust has settled.

[*English*]

The Chair: Again, that's an important question. You have about 15 seconds to respond to it.

C/Supt Mark Flynn: The reality is that whenever personal information, passwords, etc., are released on the Internet, they are there forever. People need to be cautious and vigilant about that, and use the services that are available, like credit monitoring, etc., to ensure that triggers are put in place to notify them when someone's trying to use that information, to help prevent an actual fraud from occurring.

I'm trying to respect the timeline.

● (1420)

The Chair: Thank you, Mr. Clarke.

Mr. Graham, you have five minutes.

[*Translation*]

Mr. David de Burgh Graham: About 15 years ago, I was in an IRC channel—I'm not sure whether you're familiar with that forum—and someone was selling credit card numbers, along with the three-digit code on the back and the billing address. Everything was ready to go. The person was offering to sell them to people. I felt that was wrong and I wanted to call the police or some other authority, but no one replied or knew what to do.

If someone saw something similar happening on the Internet today, is there someplace they could call to report it?

[*English*]

C/Supt Mark Flynn: The RCMP operates the Canadian Anti-Fraud Centre in partnership with the Ontario Provincial Police and the Competition Bureau. That is one of your best places to go to report fraudulent activity, whether it be the telephone numbers that people are calling from, or an individual identity theft or fraud that occurred. They collate that information. They share that information. Police investigations are launched based on the collation of that. That would be the first place you should call, as well as your local police force.

Local police forces—whether they be the RCMP or, in Ontario and Quebec, another police force—need to hear about the crimes that are occurring. There are connections between organized crime involved in fraud and other criminal activities.

[*Translation*]

Mr. David de Burgh Graham: What powers does the Canadian Centre for Cyber Security have? What can the centre do?

Mr. André Boucher: Do you mean generally or in this specific case?

Mr. David de Burgh Graham: I mean generally. At the centre, do you accept comments from people on the outside, or do you work only with businesses? Explain how it works, if you don't mind.

Mr. André Boucher: As I explained earlier, the Canadian Centre for Cyber Security is responsible for providing advice. It prepares and protects information of national interest. It is responsible for incident management and response, including mitigation strategies. Every step is undertaken in coordination with the centre's partners, as per its mandate. When a fraud-related issue arises, the national team is called in. It is made up of centres that have already been appointed. We make sure all stakeholders have access to the available information so we can move forward. Work on the case continues, and if more information becomes available, it is shared with the person responsible.

Here's where the value of this business model lies. If something changes while the case is under way—for instance, if it ceases to be an investigation—the Canadian Centre for Cyber Security takes over until the victim receives or, rather, until the case is closed.

Mr. David de Burgh Graham: Earlier, we were talking about passwords. Nowadays, we see two-factor authentication being used a lot more for bank accounts. Could the same thing be done for social insurance numbers?

Mr. André Boucher: I'm going to say the same thing I did earlier. I'm not an expert in social insurance numbers, but we strongly advise people to use two factors whenever possible. It's not perfect, but it improves the security of their information.

Mr. Michel Picard: I'd like to revisit the issue of a unique identifier.

Other models exist. On other committees, we've talked about the popular Estonian model, I believe. It's a system that's in line with our discussions on open banking. All the information is centralized and people can access it using a unique identification number.

At the end of the day, no matter what you call it, a social insurance number is a unique identification number, so it's important to understand the system's limitations. It's all well and good to have the ultimate ultra-modern system, but if a single unique identifier is assigned to an individual, the information will always be vulnerable if someone gets a hold of it.

Mr. André Boucher: Absolutely. I can't name them today, but a number of countries around the world have endeavoured to adopt a system that relies on a national unique identification number. Some have been successful, and others, less so. As you said, the number becomes an essential piece of information and the slightest vulnerability puts the data at risk.

Mr. Michel Picard: Does your centre manage its employees' personal information itself?

Mr. André Boucher: Yes, absolutely, using all the measures I mentioned earlier.

Mr. Michel Picard: How do you protect against an employee who wakes up in a foul mood one day and decides to help the other side?

Mr. André Boucher: We have an extensive security program in place from the get-go, starting with the selection of personnel. Of course, a culture of security prevails throughout the organization, one that encompasses personnel security, physical security and computer system security.

The processes are in place. The system is evergreen, meaning that it's constantly updated. We don't rest on our laurels, so to speak. We review the system on a regular basis. It's an extensive and complex process, but the investment is worth it.

● (1425)

Mr. Michel Picard: Is your approach used elsewhere in the market? Has another organization established a culture of security similar to yours?

Mr. André Boucher: Our approach is modern, but we don't have a monopoly on security programs. Documentation is available. Public Safety Canada put out a publication on developing appropriate security programs. It's an excellent reference that refers to the same models we use.

Mr. Michel Picard: Thank you, Mr. Boucher.

[*English*]

The Chair: Thank you, Mr. Picard.

Mr. Dubé, you have three minutes.

Mr. Fortin, we'll have a few minutes left. Do you wish to ask a couple of minutes of questions?

Mr. Rhéal Fortin: Yes, please.

The Chair: Go ahead, Mr. Dubé.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

Mr. Boucher, I didn't get a chance to ask you questions earlier.

My first question is about something your colleague Scott Jones said when he appeared before the committee as part of the other study we've been referring to a lot today. He said it was important that institutions and businesses report data breaches and thefts that affect them.

In its recommendation, the committee remained rather vague. Should it be mandatory to report such breaches to police in order to minimize the impact on the public and catch those responsible?

That brings me to two other questions. They're for you, Mr. Flynn.

Since the information remains online forever, should police treat these threats in the same way they do physical ones? If a murderer or someone else poses a physical threat, I imagine police investigations are conducted with a certain level of urgency. Should the same apply to cyberthreats? Desjardins contacted Quebec provincial police in December, if I'm not mistaken.

My last question is about background checks and ongoing security checks. Given how savvy individuals are these days, should these checks become the norm?

You can have the rest of my time to answer.

Mr. André Boucher: Regarding your question about reporting incidents, I would just point out that we recommend organizations invest before an incident occurs. The organization has to have a security program in place, one that can detect threats and so forth. We always recommend that people report incidents and share them with their community because there are usually commonalities that everyone can learn from.

As the country's cybersecurity centre, we work to gather that information across all communities and to find commonalities in order to issue advice and guidance that could lead to enhanced security nationally. Yes, incidents should definitely be reported.

[*English*]

C/Supt Mark Flynn: With respect to the physical versus the cyber harm, I agree with you. It's a very difficult thing to understand. We struggle in policing to determine where we are going to apply our resources, because we always look at where we're going to be able to have the most significant impact in reducing harm.

If you look at fraud, fraud is a very large and significant threat in Canada and globally. It is difficult to measure $400,000 worth of fraud or $2 million worth of fraud against a physical threat or a homicide, or an assault against an individual. We struggle with that, but I can tell you that we're aware of it and are examining how we measure that risk and how we prioritize.

[*Translation*]

Mr. Matthew Dubé: Wouldn't it be appropriate to acknowledge that this kind of incident has a lifelong impact on a person and to respond with that in mind?

[*English*]

C/Supt Mark Flynn: Yes, it's absolutely a consideration.

The Chair: Thank you, Mr. Dubé.

[*Translation*]

Mr. Fortin, you have two minutes. Go ahead.

Mr. Rhéal Fortin: I have a quick question for Mr. Flynn. I say quick, because I have just two minutes and I also have a question for Mr. Boucher.

Two years ago, 19 million Canadians were the victims of fraud as a result of a data breach at Equifax. Similar data were stolen in that case. Last year, some 90,000 CIBC and BMO customers were targeted. This year, it's Desjardins members.

Can you tell us whether, further to these events, crime involving the use of the stolen data has increased?

[*English*]

C/Supt Mark Flynn: The specific data from those compromises...?

[*Translation*]

Mr. Rhéal Fortin: Yes, but I'm talking about this type of crime.

● (1430)

[*English*]

C/Supt Mark Flynn: We are seeing fraudsters utilizing information that is compromised in operations. The RCMP had a successful investigation into Leakedsource.com, which was reselling some of the information from the large compromises that were made public. There was a guilty plea in that case.

It is not an unusual circumstance that somebody is reselling that. We are seeing that occur.

[*Translation*]

Mr. Rhéal Fortin: All right, but has there been an increase in crime involving data stolen as a result of these breaches? Has the crime rate gone up?

[*English*]

C/Supt Mark Flynn: I haven't taken note specifically of the rate of crime, but it is certainly a type of crime that we are seeing.

[*Translation*]

Mr. Rhéal Fortin: I see.

My second question is for Mr. Boucher.

Mr. Boucher, in your brief, you give three recommendations to deal with increasing cyberthreats. The second is to invest in training and awareness so that people have the tools to respond. Has the federal government earmarked funding to work with the Quebec government to improve the security of Quebecers' information?

Mr. André Boucher: I can speak for my organization. We have a national responsibility, and that includes working with our Quebec partners. We invest in education and training, and we also make our services available to Quebec businesses.

Mr. Rhéal Fortin: Sorry, I don't mean to rush you, but as you know, two minutes isn't much time.

Are any investments planned, and if so, how much? Has the federal government made so many millions available to work with Quebec on a training program or other cybercrime initiative, for example?

Mr. André Boucher: I don't have that information with me today.

Mr. Rhéal Fortin: I see.

Thank you.

[*English*]

The Chair: Unfortunately, you're not going to be able to answer that question.

Before I suspend I just want to go to point three of your presentation, Mr. Boucher, where it says, “Identify and protect critical assets. Know where your key data lives. Protect it and monitor the protection. Be ready to respond”. In other words, zero trust, which is what we've heard for the last six months.

Is that the standard by which any financial institution, let alone Desjardins, should be held?

Mr. André Boucher: I think every large enterprise has to measure its own key assets and the value of those assets and make a risk-based decision on how much they're going to invest to protect those assets. Starting from a position of zero trust is the reality of the complex environment we live in today. Don't assume your system is going to work on its own. It takes a holistic investment in a security program—in the right people, the right processes and the right technology. The sum of these things will....

The Chair: That's a consensus standard among the cyber community, if your will, your point number three—zero trust.

Mr. André Boucher: It is a consensus that you have to invest in all of these aspects.

The Chair: Thank you, Mr. Boucher.

With that, we're going to suspend.

We are scheduled to hear government officials and are actually making some decent progress here. I am assuming, and I don't know quite correctly whether, if I suspend for two or three minutes, we can re-empanel with the government witnesses and keep on moving. Is that agreeable to colleagues?

Okay. With that, we will suspend and re-empanel with the government witnesses. Thank you.

● (1430)

(Pause)

● (1435)

The Chair: We are back on. I want to thank the officials for their flexibility and ask them to indulge the committee with further potential flexibility as we are awaiting the arrival of representatives of Desjardins.

I'm going to ask the various representatives of Canada Revenue, the Department of Finance, the Department of Employment and Social Development, and the Office of the Superintendent of Financial Institutions for brief statements. If, in fact, the representatives of Desjardins are under some time constraints and do arrive, at the end of those statements, I'm going to suspend for a moment, ask you folks to take your seats in the back of the room, and deal with Desjardins for a period of time. After that I'll ask you to come back, and the members will have questions, if that's an acceptable way. Even if it's not an acceptable way to proceed, that's how we're going to proceed, so with that, I'll simply go in this order of Revenue Canada or Department of Finance, whoever wants to make their statement first.

Ms. Annette Ryan (Associate Assistant Deputy Minister, Financial Sector Policy Branch, Department of Finance): Thank you, Mr. Chair. I will go first, if that's all right.

[*Translation*]

My name is Annette Ryan. I am the associate assistant deputy minister of the financial sector policy branch within the Department of Finance. I am joined by Robert Sample, director general of the financial stability and capital markets division, as well as Judy Cameron, managing director of the Office of the Superintendent of Financial Institutions Canada, and her colleague. We are pleased to appear before you today.

● (1440)

[*English*]

My remarks today will address two areas that, I believe, are pertinent to the issues before you. Specifically I will clarify the roles of government departments and agencies and private sector actors within the federal financial sector framework and update the committee on efforts being undertaken by the Department of Finance, federal regulatory agencies and banks in support of cybersecurity and data protection.

Protecting the privacy and security of Canadians' personal and financial data is an objective shared by both levels of government and the private sector, and it is one that's crucial for maintaining continued trust in Canada's banking system.

I'll address the roles within the federal government and then discuss provincial government and private sector roles.

The Department of Finance along with federal financial sector oversight agencies has responsibility for the laws and regulations that govern Canada's federally regulated banking system. We collectively set expectations and oversee implementation to ensure that operational risks related to cybersecurity and privacy are properly managed by the financial institutions that we regulate.

The Minister of Finance has overarching responsibility for the stability and integrity of Canada's financial system. Cybersecurity is a primary aspect of financial cyber-stability as it ensures the sector remains resilient in the face of cyber-threats and attacks

In turn, Public Safety has recognized the financial services industry as being a critically important sector within its wider national critical infrastructure strategy.

The Department of Finance works closely with a range of partners responsible for financial regulation and cybersecurity both domestically and internationally to ensure that the sector is adopting appropriate cyber-resiliency and data protection practices and that the specific needs of the financial sector are considered within economy-wide policies and statutes that relate to cybersecurity and data security.

I'll describe the general responsibilities among financial regulators. The Office of the Superintendent of Financial Institutions is the prudential regulator of federally regulated financial institutions, including banks. OSFI develops standards and rules for managing cyber-risks as is consistent with its wider oversight of operational risks that institutions must manage.

The Bank of Canada monitors financial market infrastructures, such as payment systems, to enhance resilience to cyber-threats, and the bank coordinates sector-wide responses to systemic-level operational incidents.

Other federal agencies have responsibilities for laws of general application in respect of privacy. The Office of the Privacy Commissioner of Canada oversees the banks' compliance with Canada's private sector privacy legislation, the Personal Information Protection and Electronic Documents Act, known as PIPEDA. PIPEDA sets out requirements that businesses must follow when collecting, using or disclosing personal data in the course of commercial activities. These include putting in place appropriate security safeguards to protect personal data against loss, theft or unauthorized disclosure.

The Department of Innovation, Science and Economic Development has overall policy responsibility for PIPEDA. In November of 2018 the Government of Canada implemented amendments to PIPEDA related to data breach reporting requirements and associated monetary penalties for failing to report.

As you've just heard, other federal departments and agencies, including Public Safety, the Canadian Centre for Cyber Security and the RCMP, share responsibilities with respect to broader Government of Canada cybersecurity initiatives.

[*Translation*]

It is important to note that supervisory responsibility for the financial sector in Canada is divided between federal and provincial governments. Provinces are responsible for the supervision of securities dealers, mutual fund and investment advisers, provincial credit unions and provincially incorporated trust, loan and insurance companies.

Accordingly, federal and provincial financial sector authorities have protocols in place for information sharing, particularly where matters of financial stability are concerned. Financial institutions, themselves, of course, are most immediately responsible for maintaining cyber and data security on a day-to-day basis, directly managing operational risks through an extensive series of protective and preventative measures, both individually and through industry-level co-operation.

These are supported by policies and standards that are continually updated to address the evolving threat landscape and remain in line with industry best practices.

● (1445)

[*English*]

Cyber-attacks are a serious and ongoing threat. I will focus on some of the steps being taken by the Government of Canada, the financial sector, regulatory agencies and the banks to ensure cybersecurity in the financial sector.

In budget 2018, the federal government invested over half a billion dollars in cybersecurity, and in October of 2018, it established the Canadian Centre for Cyber Security, which serves as a single window of technical expertise and advice to Canadians, governments and businesses. The centre defends against cyber-threat actors that target Canadian businesses, including federally or provincially regulated financial institutions, for their customer data, financial information and payment systems. Efforts to address cybercrime have been further bolstered by the newly created national cybercrime coordination unit within the RCMP, which provides a national cybercrime reporting mechanism for Canadians, including incidents related to data breaches or financial fraud.

More recently, in budget 2019, the government proposed legislation and funding to protect critical cyber systems in the Canadian financial, telecommunications, energy and transport sectors.

[*Translation*]

Our colleagues at the Treasury Board Secretariat continue their work with provincial governments, financial institutions and federal partners toward a pan-Canadian trust framework for digital identity with the goal of strengthening digital ID protection in the context of cyberthreats.

[*English*]

On the regulatory side, earlier this year OSFI published new expectations on technology and cybersecurity breach reporting via the technology and cybersecurity incident reporting advisory. This is intended to help OSFI identify areas where banks can take steps to proactively prevent cyber incidents, or in cases where incidents have occurred, to improve their cyber-resiliency.

While the first objective is to prevent data breaches, the reality is that these events happen and are not localized to the financial sector. Having said this, when cyber events occur at a federally regulated financial institution, control and oversight mechanisms are in place to manage them.

To summarize, cybersecurity is an area of critical importance for the Department of Finance. We are actively working with partners across government and in the private sector to ensure that Canadians are well-protected from cyber incidents and that when incidents do occur, they're managed in a way that mitigates the impact on consumers and the financial sector as a whole.

Thank you for your time. I'm happy to take questions.

[*Translation*]

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

We now move on to Ms. Boisjoly.

Ms. Elise Boisjoly (Assistant Deputy Minister, Integrity Services Branch, Department of Employment and Social Development): Thank you very much, Mr. Chair.

My name is Elise Boisjoly, and I am the assistant deputy minister of the integrity services branch at Employment and Social Development Canada. I am joined by Anik Dupont, who is responsible for the social insurance number program.

Thank you for the opportunity to join you today. My remarks will focus on the social insurance number, or SIN, program. Specifically, I will clarify what the social insurance number is and provide information on its issuance and use; inform the committee on privacy protection related to the SIN; and provide information on our approach in the case of data breach.

What is the SIN? The SIN is a file identifier used by the Government of Canada to coordinate the administration of federal benefits and services and the revenue system. The SIN is required for every person working in insurable or pensionable employment in Canada and to file income tax returns.

It is issued prior to your first job, when you first arrive in Canada or even at birth. During the last fiscal year, over 1.6 million SINs were issued.

The SIN is used, among other things, to deliver over $120 billion in benefits and collect over $300 billion in taxes. It facilitates information sharing to enable the provision of benefits and services to Canadians throughout their life such as child care benefits, student loans, employment insurance, pensions and even death benefits. As such, the SIN is assigned to an individual for life.

The SIN is not a national identifier and cannot be used to obtain identification. In fact, it is not even used by all programs and services within the federal government; only a certain number use it. The SIN alone is never sufficient to access a government program or benefit or to obtain credit or services in the private sector. Additional information is always required.

● (1450)

[*English*]

While data breaches are becoming increasingly commonplace, the Government of Canada follows strong and established procedures to protect the personal information of individuals. My colleague mentioned the Privacy Act and the Personal Information Protection and Electronic Documents Act, which is being administered by Innovation, Science and Economic Development Canada. They provide the legal framework for the collection, retention, use, disclosure and disposition of personal information in the administration of programs by government institutions and the private sector, respectively.

As my colleague mentioned, on November 1, 2018, a new amendment to the Personal Information Protection and Electronic Documents Act came into force, which requires organizations that experience a data breach and that have reason to believe there's a real risk of significant harm to notify the Office of the Privacy Commissioner, the affected individuals and associated organizations as soon as it's feasible. Violating this provision may result in a fine of up to $100,000 per offence.

At Employment and Social Development Canada, we have internal monitoring strategies, privacy policies, directives and information tools for privacy management, as well as a departmental code of conduct and mandatory training for employees on protecting personal information. We believe that any security breach affecting social insurance numbers is very serious and, in fact, we ourselves are not immune to such a situation. For example, in 2012, the personal information of Canada student loan borrowers was potentially compromised. The breach was a catalyst for further improvements to information management practices within the department.

Preventing social insurance number fraud starts with education and awareness. This is why our website and communication materials include information that can help Canadians better understand the steps they should take to protect their social insurance numbers. Canadians can visit the department websites, call us or visit us at one of our Service Canada centres to learn how best to protect themselves. It is important to note that protecting the information of Canadians is a shared responsibility among the government, the private sector and individuals. We strongly discourage Canadians from giving out their social insurance numbers unless they are sure that doing so is legally required or necessary. Canadians should also actively monitor their financial information, including by contacting Canada's credit bureau.

[*Translation*]

A loss of a social insurance number does not necessarily mean that a fraud has occurred or will occur.

However, should Canadians notice any fraudulent activity related to their social insurance number, they must act quickly to minimize the potential impact by reporting any incidents to the police, contacting the Privacy Commissioner and the Canadian Anti-Fraud Centre, and informing Service Canada. In cases where there is evidence of the social insurance number being used for fraudulent purposes, Service Canada works closely with those affected.

Despite ever larger data breaches, the number of Canadians who have had their social insurance number replaced by Service Canada due to fraud has remained consistent at approximately 60 per year since 2014.

That being said, we understand that many Canadians have signed a petition asking Service Canada to issue new social insurance numbers for those impacted by this data breach. The main reason we do not automatically issue a new social insurance number in these circumstances is simple: getting a new social insurance number will not protect individuals from fraud. The former social insurance number continues to exist and is linked to the individual. If a fraudster uses someone else's former social insurance number and their identity is not fully verified, credit lenders may still ask the victim of fraud to pay the debts.

In addition, it would be the individual's responsibility to provide their new social insurance number to each of their financial institutions, creditors, pension providers, employers—current and past—and any other organizations. Failing to properly do so could put individuals at risk of not receiving benefits or leave the door open to subsequent fraud or identity theft.

It would also mean doubling the monitoring. Individuals would still need to monitor their accounts and credit reports for both social insurance numbers on a regular and ongoing basis. Having multiple social insurance numbers increases the risk of potential fraud.

Active monitoring through credit bureaus as well as regular reviewing of banking and credit card statements remain the best protection against fraud.

In closing, protecting the integrity of the social insurance number is critical to us, and I can assure you that we will continue to take all necessary action to do so, including reading this committee's report and considering advice from this committee and others on how to best improve.

Thank you for your time. I'd be happy to answer your questions.

● (1455)

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Ms. Boisjoly.

Would anyone else like to speak before we go to questions?

Mr. Guénette, you have the floor.

Mr. Maxime Guénette (Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency): Thank you, Mr. Chair.

Good afternoon to all committee members.

[*English*]

My name is Maxime Guénette. I'm assistant commissioner of the public affairs branch and chief privacy officer at the Canada Revenue Agency. With me today is my colleague Gillian Pranke, deputy assistant commissioner of the assessment, benefit and service branch at the CRA.

The CRA is an organization that touches the lives of virtually all Canadians. We're one of the largest holders of personal information at the Government of Canada. We process more than 28 million individual income tax returns annually. It's therefore critical that the CRA has an extensive privacy framework in place to manage and protect personal information for all Canadians.

[*Translation*]

Integrity in the workplace is the cornerstone of agency culture. The agency supports its people in doing the right thing by providing clear guidelines and tools to ensure privacy, security and the protection of personal information, our programs and our data.

The agency is subject to the Privacy Act and associated Treasury Board policies and directives for the management and protection of Canadians' personal information. Section 241 of the Income Tax Act also imposes confidentiality requirements on its employees and others with access to taxpayer information.

The agency also adheres to the policy on government security and direction provided by lead security agencies like the Communications Security Establishment and the Canadian Centre for Cyber Security.

In April 2013, the agency appointed its first chief privacy officer, who is also responsible for the access to information and privacy functions within the agency.

[*English*]

Part of my role as the chief privacy officer is to ensure that the CRA's respect for the privacy of the information it holds is reinforced and strengthened by overseeing decisions related to privacy, including assessing the privacy impacts of our programs; championing privacy rights within the agency, including managing internal privacy breaches when they occur; and reporting to CRA senior management on the state of privacy management at the agency.

Our responsibility for sound privacy management goes beyond appointing a chief privacy officer, though. It's a responsibility that all employees share.

Protecting the CRA's integrity includes ensuring that we have the proper systems in place to safeguard sensitive information from external threats. Agency networks and workstations are equipped with malware and virus detection and removal software, which are updated daily and protect the CRA environment from the increasing threat of malicious code and viruses.

[*Translation*]

At the agency employee level, computers are secured with a suite of security products ranging from anti-virus software to host intrusion software.

External services are conducted on secure platforms and protected by firewalls and intrusion prevention tools to detect and prevent unauthorized access to agency systems.

During online transactions we ensure that all sensitive information is encrypted when it is transmitted between a taxpayer's computer and our Web servers. Regardless of how Canadians choose to interact with the agency, they must complete a two-step authentication process before gaining access to their account.

These steps are crucial to making sure that access to personal information is only available to authorized individuals. The process includes validation of a number of personal and confidential data points, including a person's social insurance number, their month and year of birth, and information from the previous year's income tax return.

[*English*]

The CRA will shortly also be implementing a new personal identification number for taxpayers who choose to use it when calling the individual inquiries line. In addition, the CRA is currently examining additional security procedures to safeguard the information of taxpayers. As cybercrime and phishing scams become more sophisticated and commonplace, the CRA is being proactive in warning the public about fraudulent communications claiming to be from the CRA.

One very simple way in which taxpayers can safeguard against fraudulent activity is to sign up for My Account, or for businesses to sign up for My Business Account, so that they can use the CRA's secure portals to access and manage their tax affairs easily and securely. When an individual is signed up for My Account, they can also sign up for online mail in order to receive account alerts informing them of possible scams or other fraudulent activity that may affect them.

CRA is proud of its reputation as a leading-edge organization committed to excellence in administering Canada's tax system. However, inappropriate fraudulent activity can occur in the workplace. CRA has incorporated a broad array of checks and balances to ensure that those who access taxpayer information are strictly limited to employees required to do so as part of their job and to detect misconduct when it does occur.

● (1500)

[*Translation*]

Monitoring of employees' access to taxpayer information is centralized, ensuring an independent process that enables the agency to detect and, if necessary, address any suspect transactions in our systems. This provides assurance that authorized users are accessing only the applications and data they are allowed to access based on strict business rules.

[*English*]

In 2017 the CRA implemented a new enterprise fraud management solution, which complements existing security controls and further reduces the risk of unauthorized access and privacy breaches. This solution enables proactive monitoring and detection of unauthorized access by CRA employees. Any allegations or suspicions of employee misconduct are taken very seriously and are thoroughly investigated. When wrongdoing or misconduct is founded, appropriate measures are taken, up to and including termination of employment. If criminal activity is suspected, the matter is referred to the proper authorities.

[*Translation*]

Upon hire, agency employees are required to read and acknowledge the agency's code of integrity and professional conduct and the values and ethics code for the public sector.

The code clearly outlines the expected standard of conduct, including the obligation to protect taxpayer information in accordance with section 241 of the Income Tax Act. Unauthorized access to taxpayer information is considered to be serious misconduct, as reflected in the agency's directive on discipline.

[*English*]

The code ensures that current and former employees are aware that the obligation to protect taxpayer information continues even after they leave the CRA. All employees are asked to review and affirm their obligations under the CRA's code of integrity every year.

In the event a privacy breach does occur, it is assessed in accordance with TBS policy and procedures to document and evaluate all potential risks to the affected individual. In such a case, the CRA offers support to the affected individual through a dedicated agency representative so that the client has the opportunity to ask questions and find information as well as, on a case-by-case basis, get access to free credit protection services.

On the rare occasion when a taxpayer's information is confirmed to have been compromised, the CRA will act to resolve all outstanding issues. This includes reviewing all fraudulent activity that may have occurred in the account, including fraudulent refund payments.

[*Translation*]

We at the agency are deeply committed to safeguarding the trust Canadians place in our organization, and to meeting their expectations that we have the right checks and balances in place to secure the information entrusted to us. We have worked hard to earn the public's trust, because it is the foundation of our self-assessment tax system.

[*English*]

A good reputation takes years to establish. We safeguard it by remaining vigilant in our efforts to protect taxpayers from security breaches and to protect Canada's tax administration system from misconduct and criminal wrongdoing.

Thank you, Mr. Chairman. I'd be pleased to answer any questions you may have.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Guénette.

If there is no one else, we will begin the question period.

Mr. Drouin, you have seven minutes.

Mr. Francis Drouin: Thank you very much, Mr. Chair.

I thank all witnesses for appearing before the committee on short notice.

I should mention that I am one of the victims of the data breach at Desjardins, as are many of my constituents.

Ms. Boisjoly, you referred to the online petition asking that the social insurance numbers of those affected be changed. Can you explain to the committee why that would not be done and why it would only complicate things without providing better security for Canadians?

Ms. Elise Boisjoly: I briefly mentioned that in my presentation and I thank you for giving me the opportunity to talk about it at greater length.

First, an information leak does not necessarily mean that fraud or identity theft has occurred. Second, we do not automatically change social insurance numbers after a leak like this because it doesn't really solve the problem or automatically remove all risk of fraud.

Let me explain that first point a little more. If you do not change the social insurance number linked to a certain credit number and if a credit agency uses the old credit number, the person involved will not necessarily be able to get credit. In addition, if a lender does not properly check the identity of that person, and a fraudster borrows money using his name, the lender could ask him to pay the debt. So there can be other cases of fraud if lenders do not correctly check people's identity.

The second reason is that it can create serious problems of access to benefits and services. As I said in my presentation, victims of data breaches must warn everyone, financial institutions, credit agencies, past and future employers, and the managers of pension schemes to which they belonged with their old social insurance numbers, and make the necessary changes. Often, people no longer remember those to whom they have given their social insurance number, especially at the beginning of their careers. That can prevent people from receiving a pension, for example, because it is no longer possible to establish a link between an individual and the benefits to which they are entitled.

At federal level, we would certainly advise the Canadian Revenue Agency and all organizations involved. But changes could be made manually and there may be errors. This could complicate the calculation of pensions or employment insurance benefits. If someone forgets an employer and makes errors, the calculation of employment insurance benefits or the old age pension could be wrong.

● (1505)

Mr. Francis Drouin: In other words, changing our social insurance number does not necessarily protect our personal information.

Why is another social insurance number issued in cases where fraud has been proven?

Ms. Elise Boisjoly: When fraud has been proven, we look at the type of fraud and discuss the matter with the person involved. Often people decide not to change their social insurance numbers. They register, or have someone register them, at a credit checking agency. By so doing, they will be better protected than they would be if they changed their social insurance number. Often, having been informed, people decide not to change their social insurance number. In a very small number of cases, 60 per year since 2014, people insist on making a change when fraud has been confirmed. At that point, we allow a new social insurance number to be issued, but we will also explain that it will not necessarily solve the problem.

Mr. Francis Drouin: Here is a more practical question.

Like everyone in the same situation as myself, I see a risk of fraud. How then can I advise the authorities, whether at Revenue Canada or Service Canada, that my social insurance number may perhaps be used fraudulently? Can I call Service Canada to advise them of that? Is there an internal process that allows the public to do that?

Ms. Elise Boisjoly: Absolutely. Let me make two points about that.

First, since this leak was made public, we have received between 1,400 and 1,500 requests directly from members of the public. They have called us to find out how to better protect their personal data and we have given them a lot of information about doing so. They will often take the steps that we advise them to take, such as looking at the credit agency reports and checking their bank transactions.

Second, if they notice a suspicious activity, they must follow the very clear procedures to give us that information. If suspicious transactions are detected, we ask them to contact Service Canada, which will be able to take the steps needed to help them.

Mr. Francis Drouin: Okay.

The website lists 29 cases in which Canadians are allowed to give out their social insurance numbers. To banking institutions and other entities, for example.

What does Service Canada do so that Canadians know when they should give out their social insurance number and when they should not? What recourse is possible when an organization asks for a social insurance number when it should not do so?

● (1510)

Ms. Elise Boisjoly: Our website, our call centres and the Service Canada centres tell Canadians who they may give their social insurance numbers to. When we issue social insurance numbers, we actually tell people who they should and should not give it to. A certain number of organizations are authorized to ask for social insurance numbers, for example when a bank or creditor pays interest, which the Canada Revenue Agency needs to know.

If someone not on that list asks for a social insurance number, people can refuse and ask to provide another form of information. For example, a long time ago, landlords often asked tenants for social insurance numbers in order to check their credit. They can simply provide a credit report rather than give out their social insurance number. The person asking the question must—

[*English*]

The Chair: Thank you.

It's helpful if the witnesses look at the chair from time to time so that I can signal them.

Ms. Elise Boisjoly: Thank you very much.

These glasses just—

[*Translation*]

The Chair: Mr. Paul-Hus, you have seven minutes, please.

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

My thanks to you all for being here today.

Listening to you is like being in *The Twelve Tasks of Asterix*. Let us put ourselves in people's shoes. Their concern is that they have no real idea of what will happen. We asked to meet with you so that we could have some information on the subject. We know that the social insurance number is one measure but is there anything else that should be done in the future to change the system? Could we do as other countries have done, such as providing more digital identification, whether it is by means of fingerprints or something else?

Ms. Boisjoly, you say that there about 60 cases per year, but look, 2.9 million people had their data stolen. Are you expecting a major increase in the number of requested changes of social insurance numbers following these identity thefts?

I also have a question for you, Mr. Guénette.

The people following what is currently happening want to know what is being done. You proposed a good solution, and solutions are what people need. You mentioned people going on the Government of Canada site and opening their financial records. If I understand correctly, by opening your records, you can receive alerts or warnings.

It has now been three weeks. We are here today as the result of an emergency request. Why was there no communication with the public, immediately or within a week following the thefts, to let people know what the Government of Canada can do to help? That's what we need to know.

I am all ears, Ms. Boisjoly.

Ms. Elise Boisjoly: Thank you.

To answer your first question on new measures, every situation like this gives us the opportunity to review our security and privacy protection measures. All of our colleagues and myself certainly focus on that when there are incidents of this kind. The colleagues who have gone before us spoke a lot about the evolution of cybersecurity. They said that we always have to be ready. We are certainly always focused on that.

My colleague mentioned the Treasury Board, whose mandate includes identity management. They are focusing on ways in which we can better solve the problems associated with digital identity, specifically by conducting pilot projects with the provinces. We participate in those forums, and we are thinking of ways to move the discussion on digital identity forward.

Second, in terms of the number of identity thefts, we have been advised of many in the last 14 or 15 years. Probably millions of people have already been affected and, despite that, the number asking for a new social insurance number remains rather low. So I cannot answer your question, because I am not aware of the future, but I can say that there have been a lot of thefts and that the number seems constant, around 60 per year.

Mr. Maxime Guénette: Thank you for the question, Mr. Paul-Hus.

As Ms. Boisjoly said, there is never a bad time to remind people about the things they can do. At tax time, we conducted advertising campaigns and communication initiatives online and on social media to remind people about the services at their disposal. However, more can always be done. We are always looking for opportunities to communicate more in this respect. So—

● (1515)

Mr. Pierre Paul-Hus: Okay, but the case before us is about managing a crisis. We are here to find out whether a federal organization can lend a hand to Desjardins, who are taking their own steps to rectify the situation as best they can. Currently, I see some inter-agency measures but really no proactive measures to help Canadians, aside from a message that has already been sent out.

In your opinion, why does the government seem to be so passive? Why is it saying nothing? Is it because nothing can be done? Is there no solution?

We are looking for solutions because people are concerned. If you are telling us that current agencies do not have the means or the tools to help them, we are going to look for other solutions.

Are solutions like the one Desjardins proposed, the Equifax services, quite effective in your experience and as you assess this situation? We are looking to reassure people with things that are true. We don't want to say just anything.

Mr. Maxime Guénette: Currently, because the investigation is still in progress, there is a lot of information…

Mr. Pierre Paul-Hus: The investigation has nothing to do with it because we know how the data breach happened. We also have an idea of where the data was sent, but, at the moment, that is not what we are interested in. We know that someone, somewhere on the planet, has our information and is in a position to harm us by stealing our identity. So we want to know whether our agencies can become proactively involved or, if not, what can be done.

You have a solution in my case, so that is already something that the public could be told about. It is important to do that quickly because people are not in a very good mood during their holidays. Then we will have to see if something else can be done.

The issue of the social insurance number has come up everywhere. A number of suggestions have been made. You are responsible for that file and you are saying that nothing can be done, at least not in that way. These are the answers that people need to hear. But the fact remains that we have to leave here telling people what the government can do to help, first Desjardins and second, the 2.9 million people who have been affected. We are hearing a lot about internal protocols, but, for the Canadians listening to us, that does not mean a lot. This is why I want to hear clear answers. I know that you are giving them when you can, but basically, when we leave here, we will need to know what can be done.

Mr. Maxime Guénette: I can assure you that very proactive discussions are going on between the various departments involved.

As far as the revenue agency is concerned, as I said in my remarks, the social insurance number, the address and the date of birth are some of the pieces of information people need in order to identify themselves to the agency. We also need information on tax returns from previous years, which was not in the information stolen from Desjardins, according to the discussions we have had. However, once again, the investigation is still in progress. So these questions—

Mr. Pierre Paul-Hus: As I told you, that really changes nothing.

How much time do I have left, Mr. Chair?

[*English*]

The Chair: You have about 10 seconds.

[*Translation*]

Mr. Pierre Paul-Hus: What is the first thing people should do if their identity is stolen? Call the police?

Ms. Elise Boisjoly: Yes.

Mr. Maxime Guénette: Certainly.

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

Mr. Dubé, you have seven minutes.

Mr. Matthew Dubé: Thank you, Mr. Chair.

Thank you all for taking the time to come here today.

Ms. Boisjoly, I was struck by one point in your reply to Mr. Drouin. You said that a personal data breach does not lead to identity theft. That is basically what brings us here today. Canadians want to avoid identity theft, of course; it's their main concern. I have some questions about it.

You said that people should report suspicious activities associated with a social insurance number. I am a federal lawmaker and I don't know what a suspicious activity associated with a social insurance number is. I have never been a victim of fraud, thank heavens, and the same goes for the people around me, touch wood. However, I do know people who have been victims. They find out when they receive a bill for a cellphone they do not have, or for a Canadian Tire credit card that they never applied for. They end up with debts and obligations that are not theirs.

Can you tell me exactly what a suspicious activity associated with a social insurance number is?

Ms. Elise Boisjoly: Thank you for your question.

You have certainly identified some suspicious activities, as you say. We ask people to protect themselves as best they can by working with a credit bureau so that transactions are monitored as closely as possible. They should look at their bank and credit card transactions. If they see actions in their name that they did not make, we asked them to contact the bureau—

● (1520)

Mr. Matthew Dubé: I am sorry for interrupting you, but my time is limited and I only have one round.

The suspicious activities or problematic transactions that we may be able to see on our credit card statements can be associated with all kinds of things. It may be someone who has stolen our mail and obtained our address. That is information that is probably easier to obtain. You rightly mentioned that, in terms of the situation we are discussing today, the person has complementary information. In principle, with all the information that has been stolen, that person could easily call Revenue Canada and obtain a new password. If you have someone's entire file, you have all the information you need.

Ms. Elise Boisjoly: Yes, and that is the most important point. We are talking about a number of identifiers. Each one of the organizations is responsible for checking people's identity.

My colleague said that there must also be a line from the tax return. With employment insurance, there is an access code and you are asked to provide the two figures in that access code. When we are checking identities, we must make sure that we ask questions about identities that are secret and shared only with the people we know. That allows us to better verify people's identity and to provide them with the service. For example, you would not be able to call Service Canada and obtain employment insurance benefits with the information that has been made public at the moment.

Mr. Matthew Dubé: As for getting a new social insurance number, I have a little difficulty understanding. Basically, the argument is that it becomes complicated for people. In principle, a social insurance number is issued for reasons of efficiency. A unique identifier makes transactions with government agencies easier.

Forgive me if this analogy may not be an exact one. If I see a problem with my credit card today, the bank or the company that issued it is still able to transfer a balance or to link the legitimate transactions on my credit card that has been used fraudulently and the new one it sent to me.

Why would a financial institution be able to do that, while you are not able to say that someone's social insurance number has been compromised and to give them a new number? A former employer, for example, might have to take care of questions about that person's pension. Knowing that is the same person, why are you not able to link the previous social insurance number to a new one? You may perhaps have to do some additional checking, given that the number has been compromised. But I am still having a little difficulty understanding why you can't do it.

Ms. Elise Boisjoly: When you started, you said that the first reason we do not automatically give out social insurance numbers is that it can make life difficult for people. The first reason is actually that it would not really prevent fraud. This is a very important point. People have to continue to check their previous social insurance number because there are still—

Mr. Matthew Dubé: I am sorry to interrupt you, but, if I lose my credit card, it does not necessarily mean that it has been stolen. It may have fallen down a sewer somewhere, meaning that it will never be seen or used again. I would still call my bank, Visa or whomever, to ask them to cancel the card. I would still keep checking and I would have some peace of mind, knowing that I am protected.

Why not use the same logic for victims of breaches of personal data, especially ones that are all over the news? To make sure they are protected, people want to dot all the i's and cross all the t's that they can. They change their credit cards and everything, as they do when they lose their wallets. Why not proceed in the same way?

Ms. Elise Boisjoly: A social insurance number is not like a credit card, which is a bank's only way of identifying that person. It is an identifier used by employers for as long as people are in the workforce. It is also used for various programs and services.

At the moment, no computer system links all those systems so that social insurance numbers can be updated by employers and by the various groups and programs. That task would be done manually. That is why we do not know all the employers. In the federal government, it would be done manually. As I said, we have only done it a few times. There is a risk of errors. I am just mentioning this to the committee.

● (1525)

Mr. Matthew Dubé: I have less than a minute left.

At the risk of tangling ourselves up in technical details, I would like to understand this better. If an employer wants to use a social insurance number, how does that work? Surely, things come together in some way when you move up the ladder.

I have one final question, which goes back to what Mr. Paul-Hus rightly said.

Let me take Quebec as an example. When there is flooding, police forces and the Government of Quebec hold public consultations on the spot so that people can attend.

Mr. Guénette, I respect what you said, but perhaps advertising campaigns or posts on social media are not enough.

Given the extent of this theft, this breach, have you considered organizing consultations in person in the key places in Québec, the major centres of Longueuil, Montreal and elsewhere?

[*English*]

The Chair: Again, Mr. Dubé has asked an important question but has not left any time for an answer, so you'll have to work it in somewhere else.

Usually you're so good, Mr. Dubé.

[*Translation*]

Welcome to the committee, Ms. Lapointe. You have seven minutes.

Ms. Linda Lapointe (Rivière-des-Mille-Îles, Lib.): Thank you very much, Mr. Chair.

Good afternoon to you all and thank you for joining us.

I do not normally sit on this committee, but I gladly agreed to replace one of its permanent members.

I have had discussions with a number of my constituents in Rivière-des-Mille-Îles, which is to the north of Montreal and includes Deux-Montagnes, Saint-Eustache, Boisbriand and Rosemère. They are very concerned. This is something that has come up all the time since the House adjourned on June 21. That is why I agreed to be here today without hesitation, even though I am not familiar with all the studies that this committee has done.

Ms. Ryan, earlier, you began by saying that the Department of Finance establishes the legislation and regulations that govern the Canadian banking system. You then said that oversight of the Canadian financial sector is shared between the federal and provincial governments.

Let us look specifically at Quebec. The provinces are responsible for real estate brokers, and mutual funds and investment representatives, and so on. Desjardins is a provincial cooperative institution. Just now, I mentioned my constituents, but my entire family and myself are also among the 2.9 million people affected. This concerns us a great deal and we are wondering what will be the future impact of this theft on our lives.

Have you had any requests from Desjardins? Mr. Guénette said that there are ongoing discussions between departments, but have people from Desjardins been in communication with you to get additional information?

[*English*]

Ms. Annette Ryan: To the extent that Desjardins is largely provincially regulated, their first point of contact with a government regulator would be with the Autorité des marchés financiers in Quebec. When I spoke of the system of banking rules and regulations in place federally, that applies to the institutions that have elected to be federally regulated.

To the extent that Desjardins is largely provincially regulated, many of the operational requirements put in place in advance of this incident would have been worked through with the Autorité des marchés financiers.

My colleague from OSFI can speak to how that is put in place at the federal level. In this incident the institution stepped forward and took a number of responsible measures very quickly to be transparent about the leak. That is consistent with both provincial law and federal law in terms of privacy, and the federal and provincial privacy commissioners have struck a joint investigation to look into this incident, but many of the provisions for not just the conduct of the financial regulation of Desjardins but also the consumer protections are provincial in this case. We can speak to the federal system, but I would direct many of the questions you may have to those responsible at the provincial level.

● (1530)

[*Translation*]

Ms. Linda Lapointe: I have one other question. Are credit bureaus in federal jurisdiction?

[*English*]

Ms. Annette Ryan: It's largely provincial, and in this case it is provincial.

[*Translation*]

Ms. Linda Lapointe: Okay.

Have people from Equifax been in communication with you?

[*English*]

Ms. Annette Ryan: Equifax would not be in touch with us or the department, and they are largely regulated for consumer issues at the provincial level for this.

[*Translation*]

Ms. Linda Lapointe: Thank you.

I have used half of my time and so I am now going to turn to you, Mr. Guénette.

You talked earlier about the external rules on preventing identity theft, but you have not spoken a lot about the internal rules. I would like to know about the internal rules in the Canada Revenue Agency. After all, we are here today because data was stolen from the inside.

How do things work at the Canada Revenue Agency? Do the employees have to be at certain levels in order to have access to the systems? You talked about centralizing or detecting problems by intervening if necessary. You said that there are strict rules and I would like you to tell me a little more about them. Can people work with their own electronic equipment when they are in front of Canada Revenue Agency screens? I would like to know more about that.

Mr. Maxime Guénette: Thank you for your question.

Of course, we have security rules at several levels. First, we screen the staff that we hire. People with more specific access have “Secret” security clearance instead of a lower level of clearance. A whole host of physical security measures are in place. People working in call centres, who have access to screens showing taxpayer information, may not have their personal phones with them. We have measures in that regard.

As for access to taxpayers' data, those data are on separate servers that are not connected to the Internet. There is a mechanism by which the employees' access to the data is reviewed annually, or each time they change jobs. Managers verify the access those employees have on a regular basis.

As for the workload, in my introductory remarks, I talked about the administrative rules. When we give employees their workload, our business fraud management system checks by using algorithms in real time. The system applies several dozen rules. For example, if employees check their own tax accounts, an alert is automatically issued and the system sees it immediately. If employees work on tasks that they have not been assigned, the system will immediately send an alert to the manager, who would then be able to ask an employee what he or she was doing in the system. Screen shots are captured per minute, which allows us to see which pages employees are consulting or which changes they have made. The system was implemented in 2017 and it is very advanced. It allows us to have controls in place.

In terms of preventing data breaches, employees are unable to copy information onto CDs, DVDs or USB keys. The system does not allow it.

Ms. Linda Lapointe: Thank you.

The Chair: Thank you, Ms. Lapointe.

[*English*]

We'll have Mr. Motz and Mr. Clarke.

Mr. Glen Motz: Thank you, Chair.

Again, thank you to the departmental officials for being here.

I have just two quick questions for the Department of Finance. You say that your first objective is to prevent data breaches. We know the reality is that these happen and are not localized to the financial sector.

Ms. Ryan, you said that when cybe events occur at a federally regulated institution, which is what we're talking about, control and oversight mechanisms are in place to manage them. Can you explain to Canadians in practical terms what that actually means when you play that out?

● (1535)

Ms. Judy Cameron (Senior Director, Regulatory Affairs and Strategic Policy, Office of the Superintendent of Financial Institutions): I'll take that question.

I represent the Office of the Superintendent of Financial Institutions. Our mandate is to supervise financial institutions and set rules for them so as to protect the interests of depositors and creditors. Broadly speaking we're looking at safety and soundness, but we also make sure they comply with all federal rules. For example, we expect them to have systems in place to comply with privacy laws.

We set expectations around what institutions should be doing, such as complying with privacy laws. We also expect them to do cyber self-assessments to assess their own internal protections against cyber events. Then we supervise them to make sure they are complying with the expectations we have set out to make sure that they have good compliance management systems in place.

Mr. Glen Motz: Basically, it's just oversight. Now, in this particular circumstance, it's oversight of what's happened to make sure that—

Ms. Judy Cameron: It's oversight of their systems to prevent this, really.

Mr. Glen Motz: Okay, so that's one question. The other question is for Ms. Ryan, or whoever might....

I'm just going to read the summary that you gave. You said that "cybersecurity is an area of critical importance for the Department of Finance. We are actively working with partners across government and the private sector to ensure that Canadians are well-protected from cybe -incidents and that when incidents do occur, they're managed in a way that mitigates the impact on consumers and the financial sector as a whole."

What does that actually look like to impacted consumers, to consumers at large, to the financial institution, to the banking industry, to various government departments? You can say that, but what does it actually look like?

Ms. Annette Ryan: I think that the number of federal partners you have had as witnesses today speaks to that.

The investments in the cyber centre were part of the first line of defence in strengthening the ability to prevent cyber incidents, and they are focused, as André Boucher spoke to, on the appropriate response to a cyber event. In this case there was a specific type of cyber event, a breach by an employee, so many of those defences that have been built by the cyber centre were not triggered in this case, but the resources of the cyber centre are complemented by new resources for the RCMP. You heard the RCMP speak about the national cybercrime centre and their efforts at the Canadian Anti-Fraud Centre.

We also realize that a cyber event or a data event does play out on the privacy side. Therefore, measures such as the new requirements for businesses to notify customers that there has been a breach are a key part of a citizen's ability to be vigilant about their own finances and to know that important information about them has been put into play. A monitoring service like Equifax is important because it helps put that person into the mix to know when something that's being done in their name is not right.

Mr. Glen Motz: I have just one quick follow-up question to that. If I were one of the 2.9 million Canadians impacted by this circumstance, or one of the millions in this country who have already been impacted by data breaches of various varieties, I would want assistance in getting my life back, like them. Right now there is a lot of talk about what that looks like, but in practical terms, Canadians want to know how to get their lives back. They want to mitigate the risks and the impacts that a breach like this has on their personal lives, on their financial futures and on those of their families.

I'm curious; it seems that the Department of Finance has a role to play in having a location from which Canadians can find the information they need, follow a template, call numbers, or whatever it may be to help get their lives in order, because this is, and will be, devastating to those whom these criminals are going to take advantage of.

As government, we have a responsibility to ensure that we protect Canadians as well as we can. This is not going to go away.

● (1540)

The Chair: I'm going to have to leave it there. I thank you for your witness.

Colleagues, I need some guidance here. Our next witnesses are outside, and, as you know, are under some time constraints. I propose suspending. The question, colleagues, is do you want to suspend and release these witnesses, or do you want to suspend and ask these witnesses to remain so that we can have our final rounds of questioning?

Mr. David de Burgh Graham: If they're willing to stay, I'd like to ask my questions.

Mr. Alupa Clarke: I would like to intervene with these witnesses, please.

The Chair: With that, I'm going to suspend. I'm going to ask the witnesses to leave the room, but to stay nearby, and after we finish with the next witness to come back—

[*Translation*]

Mr. Rhéal Fortin: Mr. Chair, I have some questions for the witnesses, but I will leave it up to you to decide on a good time for me to ask them.

[*English*]

The Chair: We'll look forward to that, Mr. Fortin.

With that, we'll suspend for a couple of minutes while we bring in our next panel. Thank you.

● (1540)

(Pause)

● (1540)

The Chair: Colleagues, I'd ask you to take your seats.

I ask the next set of witnesses to come forward—Mr. Brun, Mr. Cormier, and Monsieur Berthiaume.

I would ask that the cameras leave, please. That's all of the cameras, including the CBC camera. Thank you.

I want to thank you and your colleagues for coming, Mr. Cormier. Apparently you're fairly popular these days.

We have encouraged witnesses to make brief statements, with the emphasis on their being brief, because there is an appetite on the part of members to ask questions. I'm informed of various times by which, I believe, you, Mr. Cormier, have to leave—and what time is that?

Mr. Guy Cormier (President and Chief Executive Officer, Desjardins Group): We're supposed to leave around 4:30, but maybe we can add—

The Chair: I'd encourage you to stretch that if you would.

Mr. Guy Cormier: Probably an hour would be okay.

● (1545)

The Chair: Okay. I think we can live with an hour. Possibly your colleagues can stay after you leave.

The issue is that this has been an emergency meeting and people have literally come from all over Canada to hear what you have to say.

With that, I'll ask you to make whatever remarks you have and then we'll turn it over to questions.

Mr. Guy Cormier: Thank you very much.

[*Translation*]

Good afternoon, Mr. Chair and members of the Standing Committee on Public Safety and National Security. I'm joined this afternoon by Denis Berthiaume, Senior Executive Vice-President and Chief Operating Officer, and Bernard Brun, Vice-President, Government Relations, Desjardins Group.

First, I want to say that, at Desjardins, we were ambivalent about this exceptional committee meeting.

On the one hand, this meeting may seem premature, since we're in the process of managing this situation and the police investigations are ongoing. It's far too early to assess the situation. As such, we intend to tell you everything that we know, but in a way that won't interfere with the ongoing investigations.

On the other hand, we see this special meeting as an opportunity to inform legislators and the public about the security of personal information and the need to rethink the concept of digital identity in Canada. In my reflection process, this point prevailed.

First, I'll state the obvious. What happened at Desjardins has happened elsewhere and could happen again in any private company or public organization whose mission involves personal information management. We can think of several banks around the world, such as the American bank Chase, Sun Trust, the Korea Credit Bureau, or a number of government entities in Canada and the United States, to name a few, that have been the victims of malicious employees.

Desjardins is a leading financial institution and one of the largest cooperative financial groups in the world, with more than $300 billion in assets. In 2015, Bloomberg ranked the Desjardins Group as the strongest financial institution in North America, ahead of all Canadian banks. In other words, even the best aren't immune, and we believe that this message must be heard.

Personally, I've been working at the Desjardins Group for 27 years. I chose this organization at the start of my career because the financial institution has managed, after nearly 120 years, to successfully combine the economic and social aspects of our society.

The malicious actions of one employee led to this deplorable situation. That employee has now been dismissed. He violated all the rules of our cooperative. In this situation, we acted as quickly as possible and as transparently as possible, with the sole objective of protecting the interests of our members. That was our priority.

On June 20, a few days after learning of the extent of the situation, we went public and shared all the information available, in conjunction with the police forces. At that time, we also announced the measures implemented to address the privacy breach.

We've taken all the necessary measures to address the situation. We quickly implemented additional monitoring and protection measures to protect the personal and financial information of our members and clients. We informed all the relevant authorities, including the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Autorité des marchés financiers, the Office of the Superintendent of Financial Institutions, and the Quebec and federal departments of finance.

We've implemented additional measures to confirm the identity of individuals when they contact us. We're constantly monitoring all our members' accounts. The procedures for confirming the identity of our members and clients when they call the Desjardins caisses, Desjardins Business centres and our AccèsD call centre have also been the focus of additional measures.

We contacted the affected members through the AccèsD private messaging system and by personalized letter, to inform them of the situation and of the steps that they needed to take.

We've also added extra measures to help with the activation of the Equifax monitoring package. The affected members can now register in four ways. They can register on the Equifax website, through the AccèsD telephone service, through the AccèsD web and mobile application, and directly in our Desjardins caisses by speaking with their advisor.

We're actively working with the different police forces. Lastly, we're working with external experts to continue to protect our members' personal information.

I can confirm that we acted diligently. After we received information from the Laval police service, we conducted an internal investigation and quickly traced the source of the breach to a single employee. The employee was suspended and then dismissed.

At this time, our main priority is to reassure, assist, support and protect each and every member affected by the situation.

● (1550)

Again this morning, we announced new protection measures for all our members. In this digital age, we at Desjardins believe that all our members must be protected.

As I was saying, Desjardins announced this morning that, from now on, all members of our cooperative will be protected from unauthorized financial transactions and identity theft. Membership is automatic and free of charge, regardless of whether they've been affected by the data breach. Since this morning, Desjardins has been protecting all its individual and corporate members. This sets a precedent in the financial services world in Canada. We're the first institution to take this step. In this situation, Desjardins is acting with rigour, a sense of duty and the willingness to honour its special relationship with its members.

We've entered an age where data is a resource on par with water, wood and the raw material needed to run entire sectors of our economy. Data is now the raw material for a whole innovative economy that will lead to tremendous productivity gains and make life easier for Canadians.

Canada is a few months away from the implementation of 5G mobile connectivity, which will increase the flow of data tenfold. According to experts, this ultra-fast connectivity will lead to futuristic applications related to artificial intelligence. Canada is already among the world leaders in this area with its three hubs, Montreal, Toronto and Edmonton. In addition, as we speak, the Department of Finance Canada is in the process of conducting a consultation on open banking, which would help open up the transactional sector. Several European countries have already made the shift.

I'll humbly ask you, the legislators, the following questions.

Is Canada currently well equipped to manage these promising technological developments, which also involve new risks? Should our identification systems be adapted to the digital age to ensure the protection of privacy and to better deal with cybercriminals? This issue is the whole notion of digital identity, which I referred to a few minutes ago.

I want to respectfully point out that these are real issues raised by the situation at Desjardins.

In closing, I want to make a proposal. I'd like to invite the committee to recommend to the Government of Canada the creation of an ad hoc multi-stakeholder working group to advise the government on how to regulate the management of personal data and digital identities. We believe that a group that listens to Canadians' concerns should at least include representatives of governments, the financial services and insurance sector, and the telecommunications sector, along with jurists and experts, or any other group that the government deems it appropriate to involve in the reflection process.

The mandate of this committee should consist of advising the government on legislation and regulations; ensuring the protection of the public; encouraging innovative technological development for the benefit of Canadians and communities; and ensuring the strategic monitoring of best practices around the world, so that Canada is always up to date.

I personally believe that Canada can't pursue excellence in digital technology and artificial intelligence without having the same ambition for data and personal information management. We must all learn from the current situation at the Desjardins Group.

Thank you.

The Chair: Thank you, Mr. Cormier.

Mr. Picard, you have seven minutes.

Mr. Michel Picard: Welcome, Mr. Brun, Mr. Cormier and Mr. Berthiaume. Thank you for participating in this exercise. Your presence is greatly appreciated.

Mr. Cormier, I'll start by reassuring you that, last January or even earlier, the Standing Committee on Public Safety and National Security and the Standing Committee on Access to Information, Privacy and Ethics began to address issues related to the unique identifier. We looked at models from abroad, including Estonia's model, which raises a number of other issues.

Before I ask you some more practical questions, I want to point out that the unique identifier is one of the cybersecurity issues. When someone gets their hands on the unique identifier, we'll be faced with the same issue.

I'm pleased to hear that you're offering protection to all your members. However, financial institutions tend to charge their clients to protect the clients' data from identity theft. The financial institutions themselves make the offer. Do you have the same philosophy?

To have my salary deposited into my bank account and to make transactions, automatic withdrawals and Interac payments, I must give my name, address and social insurance number to the institution that I'm dealing with. However, I must use a third party to protect this information. Why do I need to rely on someone other than the entity to which I give the information?

● (1555)

Mr. Guy Cormier: To answer the first part of your question, we made the decision this morning to set up a protection program for all our individual and corporate members. The corporate component sometimes isn't covered by other institutions or even by Equifax. We've decided to offer this service free of charge to our members as long as they stay at Desjardins. We won't charge them anything. I want to quickly reiterate that the program covers all unauthorized financial transactions involving a person's account, deposits and money. If a transaction hasn't been authorized, we'll reimburse the person. That's one thing.

Second, if a person is unfortunately a victim of identity theft, we'll provide assistance, not a list of the steps to take. We'll call on our experts to provide assistance, and the experts may even participate in conference calls to help the person recover their identity.

Third, we'll provide coverage of up to $50,000 to reimburse members for expenses that they may have incurred, such as lost wages, child care costs or the cost of obtaining documents.

This concept of free service is extremely important to us. If you're a member of the cooperative, you have access to the program.

We humbly propose that a committee be established to, among other things, address the issue of whether privacy should be managed by third party companies. I think that the status quo isn't an option.

Mr. Michel Picard: There are two issues involved in what I consider the temporary solution of dealing with a third party. You're asking people to deal with a third party to protect their personal information. Two years ago, this third party was also the victim of hacking. We conducted a study on the matter here.

How liable would you be if your clients' personal information were hacked from the entity that you trust, such as Equifax?

Mr. Guy Cormier: That's a relevant question. In Canada, Equifax is the firm with a market share of over 70% in data and information protection and management.

When the incident occurred, we decided to turn to the Canadian company that offered this service to Canadians. We worked with the company. However, in the days that followed, we noticed some issues. We quickly took our own steps to resolve the issues concerning member registration on the Equifax website. We went through this. We saw the need to improve the procedures and methods, and we took charge of the matter.

Now, should one, two or three private companies in Canada manage all this? We must think about it.

Mr. Michel Picard: Identity theft is unique in that the data is active and will always remain on the market, unless the person using it dies. The data is virtually present all over the world. It can be used on the black market after 24 hours, as in cases of debit or credit card fraud.

The identity theft issue isn't about the security of the client's data at their own financial institution. I'm sure that your systems are up to date in terms of protection from external hacking and that you're fulfilling your responsibility to your clients by meeting the expectations of Quebecers and Canadians. If an issue arises in the account, you'll reimburse the criminally misappropriated money.

The identity theft issue is as follows. Let's say that a person goes to a bank tomorrow morning. The person says that his name is Guy Cormier and that he needs a mortgage to purchase a house. The mortgage would be at the other bank and not at Desjardins.

Identity theft causes damage in other areas. One example is the real estate flips in Saint-Lambert, in the South Shore, where people took out fake mortgages under fake identities. There were a baker's dozen, and that was only in Quebec. After that, it will be Canada and Europe. Identity theft has an impact, and it isn't limited to the Desjardins Group financial system.

The protection that you're offering is appreciated and necessary. However, if I may say so, the protection is limited to the client's financial situation within their institution.

● (1600)

Mr. Guy Cormier: Basically, the thought process behind the new measure announced this morning is that we're in the digital age. There will be fewer and fewer paper transactions in the coming years. This data becomes raw material for our economy. Given the importance of the data, at Desjardins, we've taken on the responsibility of offering protection to all our members.

I said that there were three pillars. The first pillar is the financial aspect that you're referring to. If Desjardins members see an unauthorized transaction in their transactions accounts, Desjardins will fully reimburse them. This answers the first part of your question on the financial transactions aspect.

In terms of other types of identity theft involving credit card transactions made elsewhere, such as cellphone purchases or car rentals, people can contact Desjardins and they'll be taken care of. Second, if they need help with recovering their identity, not from a financial perspective, but in relation to other aspects of their private lives, Desjardins will support them. If we need to call government agencies or private firms, or help them prepare notarized documents or a presentation, we'll do so. We're no longer talking about the financial aspect. We'll help the people with the other steps that they may need to take.

[*English*]

The Chair: Thank you, Monsieur Picard.

[*Translation*]

Mr. Paul-Hus, you have seven minutes.

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

Thank you for joining us, Mr. Cormier.

We fully understand that this situation is very emotional and complicated for Desjardins. Mr. Cormier, you said that it was premature to hold a committee meeting. I want to point out to everyone again that the Conservatives requested this meeting, with the NDP's support, to see how the federal government could help Desjardins and the nearly three million affected members.

The objective isn't to investigate the situation or to find out how the data was stolen. The police are in charge of that aspect. For my part, I hope that the individual will be punished to the full extent of the law. I hope that the law is strong enough to send him to prison for a long time, but that's another matter.

We've met with officials from various departments, including the Department of Finance and the Canada Revenue Agency. These are large departments. However, it's difficult to know whether the Government of Canada can be useful in this situation.

I want to know whether you've received effective support from the government. If not, what could the government do to help you?

Mr. Guy Cormier: There are two or three parts to my response. When this incident occurred, we contacted several federal and provincial government agencies. We spoke with the different departments of finance. I want to tell you that the departments were very helpful and supportive. Bernard Brun can confirm that very clear and open discussions were held.

I've noticed that both the federal and provincial government authorities want to reassure the public. You have no idea how important this is to us. Sometimes, we see what's being written and said. I understand that people have concerns and questions. As MPs, you must hear about many of them from the people in your constituencies.

I can see that the federal and provincial government officials want to reassure people and give them the proper information. This is very helpful to Desjardins. People must be told to contact us so that we can introduce them to the programs that we announced this morning. Whenever we meet with people in our caisses or client contact centres, we're in direct contact with them and we reassure them.

We don't want to trivialize the situation. However, according to several studies and several experts who are currently assisting us, there's a clear difference between a data breach and what happens in a real data theft. This isn't a “one-to-one” case. The proportions are very small.

By adding the protection that we announced this morning, we're telling all our members, including businesses, not to worry. If any issues arise, they should call Desjardins. We'll assist them.

● (1605)

Mr. Pierre Paul-Hus: Since the incident, you've offered the affected members a free five-year Equifax membership. Is the new protection announced this morning a lifetime membership, or is it new internal protection?

Mr. Guy Cormier: Exactly. There's new internal protection. As I said, it's the first pillar. If people see an unauthorized transaction posted to their account, they must notify Desjardins. We'll then review the transaction with them and give them a full reimbursement. I must point out that there's no limit, whether the amount is $10,000 or $100,000.

Second, if they're victims of identity theft, they must contact us. We'll assist them and hold conference calls. We even offer a period of psychological support, through our life insurance companies, to people who are going through this highly emotional situation.

Third, it's the new $50,000 protection for people who must incur personal expenses to recover their identity. Desjardins will cover these expenses. This is extremely important.

I want to reiterate that people who are victims of the data breach must continue to actively register for Equifax services, since this gives them access to the alert service. The alert service could notify them of an unauthorized transaction in the following weeks or months, and this service isn't included in the Desjardins package. The Desjardins Group strongly recommends that members who are victims of the breach register for Equifax services.

Mr. Pierre Paul-Hus: I'm a Desjardins member, but also a Royal Bank client—

Mr. Guy Cormier: Thank you.

Mr. Pierre Paul-Hus: The Royal Bank has a system that I didn't know about. I learned about it from an employee last weekend. The Royal Bank site has a link to the TransUnion site. When I click on the link, my credit report and credit rating appear. It's completely free.

Will Desjardins provide a similar service?

Mr. Guy Cormier: I'll let Mr. Berthiaume answer that. He'll undoubtedly be very happy to do so.

Mr. Denis Berthiaume (Senior Executive Vice-President and Chief Operating Officer, Desjardins Group): We provide the same type of service with TransUnion. On the web and on mobile devices, you can access your credit rating in real time. With regard to the alert system, I think that we've explained it well. We work with Equifax, but we're also considering the possibility of providing an alert system with TransUnion.

Mr. Pierre Paul-Hus: You've done an extraordinary job of putting all this in place. Congratulations.

I now want to talk about Canadians who are afraid that their data, which has been sent somewhere in the world, will be used to make transactions or for any other purpose. You can't be responsible for everyone. You have a responsibility to your members, and 90% of Quebecers are Desjardins members. However, you can't know whether data sent abroad comes from this particular breach.

In other words, if my stolen data is sent abroad, will you still cover me, even though the data could have been sent from another source?

Mr. Guy Cormier: The current situation at Desjardins was not our only reason for making this morning's proposal, but we certainly sped up the process. At the beginning of each year, we do some planning. Based on security, our new products and our new offers, we consider what we should offer our members according to their needs.

Mr. Pierre Paul-Hus: I'll interrupt you, because I made things unnecessarily complicated. What I meant was that even though a data breach occurred on your side, another organization may be sending my information elsewhere. In this case, wouldn't the government have some level of responsibility? You seem to be taking care of everyone's issues. At some point, shouldn't we suggest that the Government of Canada help all Canadians?

Mr. Denis Berthiaume: Look, right now, the important thing is to reassure the members and to offer protection to everyone. We won't start determining whether data sent abroad comes from the data breach at Desjardins or from an information leak in another organization. We want to cover and reassure our members.

To answer your question, if fraud occurs in a Desjardins account, we'll cover the member concerned. As is the case with other financial institutions, in the event of attempted fraud, whether the account is a current transactions account, a credit card account or another type of account, we don't hold the members liable.

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

Mr. Dubé, you have seven minutes.

Mr. Matthew Dubé: Thank you, Mr. Chair.

Mr. Cormier, Mr. Brun and Mr. Berthiaume, thank you for being here. You're welcome here. I think that you've fully understood our objective, which is to share information to restore the confidence of people who are extremely worried. You said it well. Like you, we're hearing from these people. This is all the more beneficial to us, since we've just completed a study. We've opened the door for members of the next Parliament with respect to cybersecurity in the financial sector. As such, we're particularly interested in this matter.

Since it hasn't been mentioned yet, I'd say that, as Quebec MPs, we're not here to conduct a witch hunt. Based on the number of activities that we're involved in, we can clearly see that Desjardins is a local partner in the community. We want to work together, and I think that your recommendation today reflects that. Thank you very much.

I want to touch on a few points, in the hope that you can answer some questions. I understand the constraints that you're operating under. The first thing is very simple. It seems silly, but it concerns Equifax's French services. A few people have reported difficulties with obtaining services in French. Have you worked with Equifax to ensure that your members, the vast majority of whom are French-speaking, receive service in French?

● (1610)

Mr. Denis Berthiaume: Yes. First, we wanted to proceed quickly with Equifax, and I think that was the intent of the process. The people at Equifax have been very helpful. They've even adjusted their service offer to accommodate us in several ways. We've worked very well together.

Now, over time, we've learned about the limits of the French-language capacity at Equifax. As a result, we've introduced a number of additional measures. The president mentioned the four initiatives that have been implemented.

First, people can go online or use their cellphones to register directly for Equifax services. We'll take care of referring them to the services, establishing the link with Equifax and providing the authentication.

Second, people can obtain a French-language service by contacting our AccèsD call centres. Wait times are very reasonable. We act as a bridge, in a way, between our members and Equifax to improve the experience. We've been implementing this approach over the past few days and weeks. We believe that this approach has been successful.

Mr. Matthew Dubé: It's not necessarily specific to what we want to review, and it doesn't fall within the mandate of the committee. However, you'll appreciate that I still wanted to get the facts straight. Thank you.

I want to focus on regulations. We heard a bit about them from the government officials who spoke before you. Are the regulations becoming cumbersome when it comes to achieving your objectives and ensuring the security of your members' data? In your particular situation, you're subject to both Quebec and federal government regulations. Compared to traditional financial institutions and large banks, you're in a somewhat unique situation. You'll forgive me for perhaps not using the correct terminology, but I think that you understand what I mean. Can this different situation cause problems?

Simply put, would it be in our interest to ensure a better alignment between the Quebec government and the federal government requirements, so that you don't need to turn left and right to comply with two different regulatory entities?

Mr. Bernard Brun (Vice-President, Government Relations, Desjardins Group): Thank you for your question.

It's extremely relevant because we operate in a bijurisdictional system. That said, overall, Desjardins is perfectly comfortable in the current framework. Obviously, with technological exchanges, the interconnectedness within the financial system is becoming more and more apparent. In this regard, we mustn't act in isolation.

Mr. Cormier pointed out earlier that we worked well together. We were able to speak with all the federal and provincial government stakeholders. We strongly encourage them to work together. We can see the collaborative efforts, but we urge the governments themselves to hold discussions.

With regard to the fact that an entity such as the Desjardins Group operates on both sides, I don't see this as an issue. However, we clearly need support in this area. We can feel it and we're focusing on it. This relates to our suggestion regarding the creation of a multi-stakeholder committee with people from different governments. This will enable us to move forward and adopt effective policies that will affect everyone.

Mr. Matthew Dubé: Thank you.

It may be more difficult to answer my next question, as the police investigation is still ongoing.

Given the growing cyber security expertise, especially among people who work in that field, do you think it would be appropriate to recommend ongoing background or behaviour checks for employees who have access to sensitive information and can use the information belonging to other users, other employees?

I am not saying that you have failed in that area, but everyone is starting to recognize the existence of people whose expertise is growing. Their expertise is being used, but it can also have more harmful consequences.

● (1615)

Mr. Guy Cormier: My colleague can talk about our practices, and then I will complement his comments based on my perspective.

Mr. Denis Berthiaume: The first thing is that rigorous security investigations are constantly being conducted at Desjardins. Investigations are indeed related to the job level. That is an important element.

Regarding the situation before us, we could wonder whether anything could have been detected. I would like to point out that internal fraud by a malicious employee is the most difficult risk to protect against. That is recognized across industry, and there are many examples of it.

In addition to security investigations, security mechanisms were in place. Obviously, we are talking about a malicious employee who found a way to circumvent all the rules and used a scheme to extract data. That said, I want to reassure you that security mechanisms are in place.

Mr. Guy Cormier: With time, will we be able to go further in terms of the situation we are going through? As I was saying, in the digital age, people handle personal data not only in financial institutions, but also in all kinds of businesses. Today, when someone wants to enrol their child in daycare, they must provide their social insurance number, and that number can remain on the table for five, 10 or 15 minutes, during the enrolment process. That is the reality in Canada.

I think that any business where employees handle personal information must ensure they have been screened.

[*English*]

The Chair: We're going to have to leave it there.

[*Translation*]

Thank you, Mr. Dubé.

Ms. Lapointe, go ahead.

Ms. Linda Lapointe: Thank you very much, Mr. Chair. I will share my time.

Gentlemen, thank you very much for being here.

I have been a member of Desjardins since around 1980. Like my colleague was saying, Desjardins is omnipresent. My riding is Rivière-des-Mille-Îles, and it includes Deux-Montagnes, Saint-Eustache, Boisbriand and Rosemère. There is a caisse Desjardins in Deux-Montagnes and one in Thérèse-De Blainville. Those are two major institutions in the region. There are two RCMs and two caisses Desjardins.

Mr. Guy Cormier: There is Mr. Bélanger.

Ms. Linda Lapointe: Yes.

You said that internal fraud is the most difficult type of fraud to detect and protect against. Earlier today, officials from the Department of Finance and the Canada Revenue Agency talked to us.

How do things work internally at Desjardins? How could have supervisors detected that malicious employee? It is clear that he managed to get into the system. Are there access levels and screenshots? Does the system issue alerts when it identifies something unusual? Are your employees allowed to have their cellphone with them when they work with data?

I am sure you will re-evaluate the existing measures. You talked about a lone malicious employee, but what will you do to protect yourselves against other malicious employees? What are your rules? How does it work?

Mr. Guy Cormier: Mr. Berthiaume, can you talk about operations?

Mr. Denis Berthiaume: Yes.

Regarding operations, I first want to say that no one, when they turn on their computer in the morning, has access to all the data. That is not how things work. At Desjardins, jobs are categorized according to the data required to do the work. That's the first thing.

Moreover, our organization has implemented a number of internal security and control mechanisms, but we do not want to discuss those publicly, as even our employees are unaware of those mechanisms. So I cannot describe them in any great detail.

Concerning this particular situation, a police investigation is under way, and that makes the issue highly sensitive. Quite frankly, we don't want to hinder the ongoing police investigation in any way.

As I just said, we cannot provide details on our security mechanisms, as they are important for helping us prevent this from happening again. The situation involves a single employee, but I can tell you that our security mechanisms detect external or other elements of fraud. I want to reiterate that it is extremely difficult to completely protect against a malicious employee.

● (1620)

Ms. Linda Lapointe: Will you review your internal rules?

Mr. Denis Berthiaume: Concerning the security measures, we are constantly evolving. In any given year, Desjardins invests $70 million in security, and data and personal information protection. We are constantly improving in order to adapt to new technologies that create new fraud possibilities. People try to create new schemes, and we are constantly evolving to be able to identify them.

Ms. Linda Lapointe: Thank you very much.

I am glad you talked about the four procedures you have implemented. My parents are seniors and have no Internet. They went to their caisse Desjardins in person to get someone to assist them, and it did not work very well.

Mr. Guy Cormier: In the early days, Equifax enrolment was a challenge for us.

Ms. Linda Lapointe: People without Internet access cannot sign up for it.

Mr. Guy Cormier: So we made the decision to provide a service to people without Internet access. As of today, people who want to could still obtain the alert service. That service will be taken over by Desjardins, which will be able to communicate with them afterwards. We have innovated when it comes to Equifax to find a solution for those people.

Ms. Linda Lapointe: Thank you.

Mr. Francis Drouin: Thank you very much, Mr. Chair.

Mr. Cormier, you and I, like Mr. Lapointe, are victims of the leak. I understand perfectly that it is difficult to fully control a malicious employee. It is virtually impossible.

That said, the leak will have various repercussions on Desjardins members. For some, nothing will come of it, while others will be victims of fraud at some point in the future. My constituents have asked me why you are offering the Equifax service free of charge for five years and not for 10, 15 or 20 years.

Mr. Guy Cormier: Mr. Berthiaume, you can answer the question on the five-year period, and then we will come back to the answer from this morning. That is a question we have already been asked.

Mr. Denis Berthiaume: First, we wanted to respond quickly by providing five years of protection. As we were unhappy with that protection period, we decided to extend it. The president announced this morning that Desjardins was committing to provide protection for life. We did not settle for a five-year protection period. We have a partnership with Equifax to provide that protection, which is important in two ways.

We are noting a strong increase in the number of Equifax enrolments, but we are not satisfied with that number. Judging from the current trend, we fear that, at the end of the day, only 20% or 25% of our members will sign up for Equifax. That still leaves people without coverage who choose not to use the alert system for their own reasons. However, we do not want to leave 75% or 80% of our members without any protection. We want to provide them with an assistance service in case something happens. That is what led to this morning's announcement. We want to go beyond the Equifax protection and provide our members with umbrella-type coverage.

Mr. Francis Drouin: Yesterday, I experienced something while communicating with Equifax. Its website was down, and I called the company. Finally, between 45 minutes and one hour later, I could sign up.

In eastern Ontario, the Desjardins Group caisses are very popular and very represented in communities. Employees are trained to help seniors who cannot go online to enrol. I am lucky to go online and to check my credit report daily, but what about my grandmother, for instance? Will someone from Desjardins let her know that there has been movement in her credit report?

Mr. Denis Berthiaume: Yes, that is the new solution we just launched. We will get organized to ensure that people can sign up for Equifax. Then, instead of Equifax contacting the individual by email, Desjardins will liaise between Equifax and the person. We will receive alerts and make sure they are real, and then we will contact the affected members, like your grandmother, in a way that suits them. That is what we are implementing.

Mr. Francis Drouin: Thank you.

Mr. Guy Cormier: I would like to briefly point out what the key message is. The Desjardins Group quickly decided to be transparent and to provide the information on June 20. When we looked at the data of 2.7 million people, we realized that some people did not have Internet access. There were also estate accounts. Situations arose, and we saw that we had to innovate and find solutions to them. So far, for all those cases, we are collaborating well with the Equifax people. They are helping us find a different solution, including for people like your grandmother.

● (1625)

[*English*]

The Chair: Thank you, Mr. Drouin.

Mr. Motz, you have five minutes.

Mr. Glen Motz: Thank you, Chair.

Thank you for being here, gentlemen.

If we're to believe the information that we received, approximately 200,000 Canadians outside of Quebec have been impacted by this particular situation. Do you know about how many in each province were impacted?

[*Translation*]

Mr. Denis Berthiaume: The affected members are primarily in Quebec. There are some affected members in Ontario and very few in other provinces. We are talking about people who no doubt moved to other provinces and are members of Desjardins. That is an important aspect. They are affected Desjardins members.

Clients of State Farm or Patrimoine Aviso, which are our partners, are unaffected. We are talking about only caisse members who may have moved to other provinces or members of our caisses in Ontario.

[*English*]

Mr. Glen Motz: Okay.

You mentioned that you purchased State Farm in 2015. You're saying that none of them are impacted.

Mr. Denis Berthiaume: They are not impacted at all, no.

Mr. Glen Motz: In 2017 you created Aviso Wealth. That was the combination of a merged Credential Financial, Qtrade Canada and NEI Investments. Those all merged.

Mr. Denis Berthiaume: That's correct.

Mr. Glen Motz: Were any of those impacted?

Mr. Denis Berthiaume: Those were not impacted at all outside of the scope of what we talked about—

Mr. Glen Motz: What about previous Desjardins clients whose accounts were closed? Has any of their data been impacted?

Mr. Denis Berthiaume: I'm not sure I—

Mr. Glen Motz: They used to be clients. Do you still store their data even though they are no longer clients? Was any of that data compromised?

Mr. Denis Berthiaume: Let me be very, very specific here. It's strictly the members of our caisse network who are impacted. Let's say you were a member a year ago and you closed your account for whatever reason. If you do not receive a letter, you will not be impacted. There is no impact. You haven't been impacted—

Mr. Glen Motz: Just to be clear, if you do not have an active account with Desjardins, you have not been impacted by this data breach. Is that what I'm hearing you say?

Mr. Denis Berthiaume: If you did not receive a letter.... The key is whether you have personally received a letter. If you received a letter, it means you're a member that may be affected and we encourage you to subscribe to Equifax.

Mr. Glen Motz: It doesn't really answer my question. If I'm hearing you correctly, you have to have an active account with Desjardins to have been impacted by this data breach. Is that a yes or a no?

Mr. Denis Berthiaume: The answer is no, because you could be a former member of Desjardins and you closed your account a year ago—

Mr. Glen Motz: That's what I asked previously.

Mr. Denis Berthiaume: —but you may be affected if you receive a letter.

Mr. Glen Motz: I'm not worried about the letter because Canadians don't care about the letter. They want to know, if I am a current member, is it yes or no? The answer is yes. Current or former clients could be impacted.

Mr. Denis Berthiaume: Yes.

Mr. Glen Motz: In 2018, Desjardins Ontario merged with about 11 Ontario credit unions, if I remember correctly. Would any of those potential clients be impacted by this data breach?

Mr. Denis Berthiaume: We're talking about the Ontario caisses....

Mr. Guy Cormier: The answer is yes. For the caisses in Ontario, merged or not merged, it's possible that there are some members of these caisses who have been impacted by the breach.

Mr. Glen Motz: In 2013 the Desjardins Group purchased insurance firms out west, particularly Coast Capital Insurance in B.C., First Insurance in B.C., Craig Insurance in Alberta, and Melfort Agencies and Prestige Insurance in Saskatchewan.

Would any of these clients be impacted by the Desjardins data breach?

Mr. Denis Berthiaume: The answer is no.

Mr. Glen Motz: Could the phones of clients who use Apple Pay or Android Pay as part of their banking practices be compromised by this data breach, and are they at higher risk for any fraudulent texts that could occur as a result of this?

Mr. Denis Berthiaume: The data that has been leaked outside includes some phone numbers and some emails. The answer to your question is yes, there may be phishing, but again, that's if they are members of a caisse, not if they're clients. If they're clients of Aviso Wealth or of former insurance operations or of life and health insurance, or they're property and casualty clients, they are not impacted.

● (1630)

Mr. Glen Motz: It's only the financial side.

Mr. Denis Berthiaume: It's only caisse members.

Mr. Glen Motz: I'll share my time with Mr.—

The Chair: You're going to have to share six seconds with him.

We'll go to Mr. Graham for five minutes.

[*Translation*]

Mr. David de Burgh Graham: I will continue somewhat along the lines of Mr. Motz's comments. Many of those who have not received a letter are worrying and wondering whether they are affected or not.

Can we say to all those who have not received a letter that they are not affected?

Mr. Denis Berthiaume: According to the information we have, only those who receive a letter are affected.

Mr. David de Burgh Graham: So if someone does not receive a letter, they are not affected. Is that right?

Mr. Denis Berthiaume: If they have not received a letter, they are not affected.

Mr. Guy Cormier: On June 14, we received information from the Laval police force. That information enabled our computer investigative teams to provide us with the figures of 2.7 million individuals and 173,000 businesses. We sent letters to those people.

Despite everything, we are hearing people's concerns. That is why, this morning, we decided to speed up the launch of this protection program for all members, be they affected or not.

Mr. David de Burgh Graham: That protection is a good thing, but in some of the towns in my riding, Laurentides—Labelle, a number of people don't have Internet access or a cellphone. They are fewer than when I first took office, but there are still some. A number of them have even lost their Desjardins branch. What can those people do?

I have had an account with Equifax for several years. When something changes, I receive an email, but I must go on the website to try to figure out what it is, as it is not clear at all. So for those with an Internet connection, the Equifax-provided information is unclear, and those without a connection have nothing at all.

You talked a bit about this, but could you elaborate further?

Mr. Guy Cormier: There are two things to consider. First, it is urgent to connect Canadians across the country to the Internet if we want to enter the 21st century. On our end, as some of our members are not connected to the Internet—sometimes by choice, sometimes because they have no access to it—we have proposed an additional solution in partnership with Equifax. Mr. Berthiaume can explain that.

Mr. Denis Berthiaume: People who don't go online and don't necessarily have an email address must still be reached. Therefore, we have set up a call centre so they can reach us by telephone. We will undertake to sign them up for the Equifax services.

We have implemented an innovative solution with Equifax, which will enrol them, take care of monitoring and alerts, and then send us the results. At that point, we will contact those without Internet or email access. That is what we implemented today.

Mr. David de Burgh Graham: So Equifax, and not Desjardins, will take care of the technical aspect.

Mr. Denis Berthiaume: Yes. Currently, Equifax has the ability to handle alerts. As we were saying earlier, Equifax holds 70% of the Canadian market when it comes to credit bureaus and detection and alert systems. So those are the services we use for this aspect.

Once again, we liaise for people who have more difficulty accessing the Internet or don't have an email address. We reassure people and, in case of alert, we contact them.

Mr. David de Burgh Graham: Fine.

In your statement, you talked about changing our digital identity system. What examples would you like us to follow?

Mr. Guy Cormier: Far be it from me to give you the perfect example that should be followed, because there will always be gaps in the perfect solutions that we think we have found. There will always be dishonest people who will try to get around these solutions. However, countries such as Estonia, India and even some European countries have put in place measures regarding unique identifiers or, at the very least, measures to ensure that government-issued cards, whether drivers' licences or health insurance cards, do not become ways of identifying people. The objective of these countries was to restore the primary role of these cards, which have become identification documents over time. Canada should draw inspiration from these countries.

● (1635)

Mr. David de Burgh Graham: Very well.

I have one last question. What did the 2.9 million Desjardins clients who were affected have in common? Do we know why they were affected and not the others?

Mr. Denis Berthiaume: On this subject, we have nothing conclusive. We relied on the data provided to us by the police services. We don't have conclusive data on why someone was on the list or not. We don't have that information.

Mr. David de Burgh Graham: Thank you.

[*English*]

The Chair: We'll go to Mr. Clarke.

[*Translation*]

Mr. Alupa Clarke: Mr. Cormier, I would just like to reiterate what my colleague said. The fundamental objective of today's meeting, for us Conservatives, is to determine what the government, its agencies and institutions could do to help you and, in turn, to help Desjardins members, which is the most important thing. They are Canadian and Quebec citizens.

As you know, I have contacted the three directors of the Desjardins branches in my riding to express my support.

Has Canada's Department of Employment and Social Development contacted you to obtain the list of the 2.9 million citizens? This is a very important question.

Mr. Guy Cormier: The department is in contact with us and collaborates with us. We have been talking directly with its representatives for more than two weeks now, whether it is about social insurance numbers or the situation Desjardins is in.

I do not believe that the information was requested, at least not on an operational level. I don't have that information. I don't know if Mr. Brun or Mr. Berthiaume know more, but I don't think so.

Mr. Alupa Clarke: When you have the answer, could you give it to the analysts or the clerk? It would be important for us to know that. If the request has been made, could you provide a list of these Canadians? We are trying to find out what the government can do, but first it should know who it is talking about. So would you be able to send this list to the Canadian government? Unfortunately, it would still involve sending data, but the recipient would be the government.

Mr. Denis Berthiaume: We will have to see if this is possible. From a legal point of view, I am not sure.

Mr. Alupa Clarke: Next, I would like to know if a member of the current cabinet has contacted you since June 20.

Mr. Guy Cormier: When you talk about the current cabinet, you are talking about the cabinet....

Mr. Alupa Clarke: I am talking about the federal cabinet. So it would be a minister.

Mr. Guy Cormier: Yes, that's right. I had a discussion with Minister Morneau on the situation. He offered me his support to see how the federal government could support Desjardins in this situation.

Mr. Alupa Clarke: Fine.

In your introduction, you mentioned very humbly and respectfully that you had some questions. Personally, I would have liked to know your answers as an expert in your field. I don't remember your first question very well, but it was still interesting. You were wondering if Canada had an adequate system for social insurance numbers, for example. I would like to know your perspective on this.

Mr. Guy Cormier: The first question was whether Canada is well equipped to manage technological development, which is full of promise, but also involves new risks.

Do we need to adapt our identification systems?

Mr. Alupa Clarke: I would like to have your answers on both points.

Mr. Guy Cormier: My two answers are simple: I think the status quo is not an option. The status quo in Canada today is not sufficient in the digital age, in the upcoming 5G era, and in the era of reflection about the world of financial services, including open financial services. On these two issues, I think we should not be satisfied with the status quo.

That is why we humbly propose the creation of a committee composed of several stakeholders, including citizens, governments, businesses—not just financial institutions, but companies that process data—to reflect on these issues and see if, using examples from other countries around the world, we can continue to be leaders.

As I mentioned in the beginning, I think that in artificial intelligence, Canada is taking an important leadership position in the world. At the same time, we must have the same ambition with regard to personal information and data protection. My answer revolves around these points.

Mr. Alupa Clarke: I have a supplementary question, which will probably be the last one. I am addressing Mr. Cormier, the citizen.

You made a very important announcement this morning. You said that the protection applies to all members, whether or not they are affected by this unfortunate event. You said all they have to do is call you and you can take care of them. You will establish contacts, take action and take the necessary steps.

Do you think that's exactly the kind of attitude that the government, the federal state, should have right now towards the 2.9 million Canadian citizens?

Citizens are being asked to contact us, and I think it is the federal government that should contact citizens. Let's say that citizens are communicating with the federal government, shouldn't the federal government have the same approach as you and say that it takes care of everything?

The representative of Employment and Social Development Canada said that, if citizens' social insurance numbers were changed, they would have to call all their former employers. That's not what you're doing. You, incredibly, say you're going to take care of everyone at the last minute.

As a citizen, would you like the federal government to act in the same way towards the affected members?

● (1640)

Mr. Guy Cormier: As a citizen, I would say that elected officials are elected to provide a framework and adopt laws. In the current digital age, regulatory parameters must be put in place to protect citizens in this regard. That's my message, as a citizen.

This is also why, despite the fact that we found this meeting premature, we still made the decision to be present. We feel that this situation is sounding the alarm and that there is an awareness and a real willingness on the part of elected officials to address this issue. We wanted to provide our point of view on this subject.

[*English*]

The Chair: Thank you, Mr. Clarke.

We'll go to Mr. Dubé for three minutes and then Mr. Fortin for three minutes.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

I have a question that is somewhat similar to what Mr. Graham was saying about Internet and telephone access. Seniors have special needs.

Are we also looking at that?

Mr. Denis Berthiaume: That's what I was saying. Often, seniors do not necessarily have an Internet connection or an email address. We take care of them. These people can call us. We will take charge of the situation from that moment on and act as intermediaries with Equifax regarding the alert system and what these people will receive as a message.

Mr. Matthew Dubé: There is an interesting article in *La Presse*, in today's issue, if I'm not mistaken. It talks about how credit watch agencies, companies like Equifax, are regulated and that this regulation focuses more on consumer issues.

It may be too much speculation for what you are comfortable talking about today, but given the somewhat symbiotic relationship they have with financial institutions and the breach Equifax has experienced, do you think it would be relevant in the digital age to review how these agencies are regulated?

This has become more important than consumer protection; they now have a responsibility to protect data. We see that there are important consequences.

Should we review this in the context of all these changes you alluded to?

Mr. Guy Cormier: I told you a few minutes ago: I think the status quo is not an option. That's why we're here today. Desjardins will be very honoured to participate in the discussions, if they are held.

I think we need to bring together the stakeholders who work in the data field in Canada to think about how we want to change the situation. Sometimes it could be about regulation, sometimes it could be about business processes, sometimes it could be about working together. I think the status quo is not an option.

Mr. Matthew Dubé: I have one minute left. In closing, I would like to say that we are pleased to have you here. We understand that this is a difficult situation. I appreciate the fact that you understand why we have a duty to do this.

Citizens are calling us. It affects them, they are worried. Our objective is not only to reassure them in this case, but also to ensure that they and other citizens who are clients of other financial institutions do not experience the same thing. You are sharing your experience, which is very useful not only today, but also for the future Parliament. We still want to put in place a roadmap in this rapidly evolving area.

Mr. Guy Cormier: That is why we accepted the invitation.

Mr. Matthew Dubé: Your presence is very much appreciated, thank you.

The Chair: Mr. Fortin, you have three minutes, please.

Mr. Rhéal Fortin: Thank you, Mr. Chair.

Mr. Cormier, Mr. Brun and Mr. Berthiaume, I too will begin by congratulating you. I must admit that when I arrived here this morning, I had questions and concerns, which you answered. I think that your statement this morning is very beneficial to Desjardins. I too am affected by what happened at Desjardins, and I appreciate the measures you have taken.

About two or three weeks ago, the Bank of Canada established the Financial Sector Resiliency Group to address IT threats. As far as I know, Desjardins Group has not been invited to join this group. Chartered banks, among others, and systemically important banks were invited.

First, can you confirm that Desjardins Group has not been invited? Then, do you consider it would be appropriate for it to participate in such a working group?

Mr. Guy Cormier: Mr. Brun, I know you've talked to this group. Can you give us the true story on that?

Mr. Bernard Brun: Thank you for this very relevant question.

The Bank of Canada obviously has an extremely important role to play in ensuring financial stability. Recently, it announced the creation of a committee to develop supervision and review oversight by discussing matters with all kinds of partners. Naturally, it turned to the big banks and the regulator. We have had discussions with people at the Bank of Canada and we feel that they have an opportunity to explore this.

As already mentioned, the financial system is extremely interconnected. All the players in this sector have issues, regulations and regulators, but they must be able to work together, go beyond that and discuss matters. We certainly have a great interest in participating in all of this. We felt that there was an opening in this direction and we are waiting to see what form this will take.

Desjardins Group is certainly a Canadian and Quebec financial institution of systemic importance. If there are discussions, we should be involved.

● (1645)

Mr. Rhéal Fortin: You have the support of the Bloc Québécois on this. I hope my colleagues across the way will follow up on this and propose that the Bank of Canada invite you.

Presently, there are discussions on the establishment of a national identity validation system. Previously, the social insurance number was used in the relationship between the employer and employees and the government. Now we see that it is used in almost every way. It is no longer clear how to behave in this regard, but it is clear that the simple social insurance number is no longer sufficient to ensure a certain level of security for citizens.

In your opinion, would an identity validation system, which would include a PIN, fingerprint or whatever, be useful in a situation like the one you have experienced?

Mr. Guy Cormier: That is why we humbly submit a recommendation to the committee today.

In Canada, 30, 40 or 50 years ago, we put in place certain mechanisms, which today are no longer used for what they were created for. It is time for industry players to sit down together to rethink all of this, and try to draw inspiration from best practices around the world; this reflection, as I can see very well, has already begun.

[*English*]

The Chair: Thank you, Monsieur Fortin.

I want to thank the witnesses for their appearance here. I'm happy to note that your announcement of your package coincided with your appearance here. That's quite fortunate. There are four or five members of this committee who are uniquely vulnerable as members of your association. I'm wondering whether their unique vulnerabilities as public figures is covered by your announcement today.

Mr. Guy Cormier: All of the information, per the announcement we made this morning, of all of the people who were on the list of the members who have been affected by this leak will be taken care of by this program. With this protection program, if it's their financial activities in their accounts, if it's having access to assistance for recovery of their identity, or if there are problems with some fees they have to pay regarding the recovery of their identity, they will be allowed to go under this program.

The Chair: I have taken note of that, as you mentioned it earlier. However, what I'm talking about is the unique vulnerability of public officials. If that vulnerability arises, will it be addressed by this particular package?

Mr. Guy Cormier: This is something that we are looking at right now in our files. Among these 2.7 million people, we are looking right now if there are some more sensitive people. You probably read about policemen, judges, people like officials. This is something that we're looking at right now. Our priority was to send the letters to make contact with the people. Now we're looking what may be other sensitivity that we should be more careful—

The Chair: So in the initial thrust, not necessarily.

Mr. Guy Cormier: Yes. We will look at it.

The Chair: My question is that we've been doing this for awhile now and one of, if you will, the gold standards of protection is what's called “zero trust”, which was brought up by a previous witness, who said, “identify and protect critical assets. Know where your key data lives; protect it; monitor the protection, and be ready to respond.”

Do you feel that Desjardins adhered to the zero trust principle that seems to be the gold standard for protection of data?

Mr. Denis Berthiaume: When we say “zero trust”, we need to identify what we are talking about. Zero trust, we have people who have access to data. They need it to actually do their work. With zero trust, clearly we want to make sure that we have security mechanisms in place that aim at the zero trust principle. However, when you put it in practical terms, sometimes there's a difference between the theory and what you can really do practically. The objective is there to make sure that the data given to us by our customers, by our clients, is fully secure. That's our goal.

● (1650)

The Chair: That's the goal.

With that I want to thank you again for your appearance here. We will suspend for a couple of minutes and re-empanel with the officials and finish our questioning with them. Thank you.

● (1650)

(Pause)

● (1650)

The Chair: We're reconvened. Thank you to the officials all and sundry for your patience with us. We were in the middle of questioning and I believe it's Mr. Graham up for five minutes, please.

[*Translation*]

Mr. David de Burgh Graham: Thank you.

Ms. Boisjoly, earlier you heard the people from Desjardins talk about the need to rethink the social insurance number system. Is research being done on the future of the social insurance number?

Ms. Elise Boisjoly: Thank you for your question.

As you know, the social insurance number is one identifier among many. As we have already mentioned, on our website, we are advising citizens that they should only give their social insurance number in very limited circumstances. This is explained to them. We tell them not to give their social insurance numbers to organizations that cannot legally request them. However, from what we hear, citizens often give it voluntarily to organizations that are not authorized to take it.

We are certainly aware of the discussions. We are still looking at what we can do to improve the protection of our systems and practices related to the social insurance number.

We want to hear the recommendations or see the report that this committee will publish, as well as other reports.

I can assure you that work on improving the security of our systems is ongoing. I know that Treasury Board is also very actively working on digital identity projects. We are participating in these discussions to see how we can improve the digital identity of citizens in Canada.

● (1655)

Mr. David de Burgh Graham: Among the data that was taken, we know that there was a lot of information, not just social insurance numbers. There were also addresses, phone numbers, and so on. You have spoken several times about additional information to authenticate the social insurance number. Is all this information included in the data that was taken?

Ms. Elise Boisjoly: The social insurance number is an identifier that provides access to federal programs and services, as well as to income and tax systems. In the case involving the federal government, with respect to benefits, for example, my colleague explained that at the Canada Revenue Agency you have to ask an additional, secret question to identify individuals, such as the amount entered on a certain line of the tax return. In the case of employment insurance, participants are given a program access code, and must give two digits of this code in order to access private information related to the employment insurance program.

The social insurance number is an identifier, but it is accompanied by other questions to validate the identity of the person with whom we do business.

Mr. David de Burgh Graham: There are Service Canada officers in every city. If people come to their offices to find out what they need to do about the current situation, what instructions will they be given?

Ms. Elise Boisjoly: Thank you for your question.

All our call centres, Service Canada offices and agents have received very clear instructions. Our call centres and Service Canada offices answered questions from approximately 1,500 citizens. They have informed them of the steps to take, including contacting a credit bureau, verifying their financial and banking transactions, and exercising extra vigilance with respect to the transactions they make. If they identify activities that are not related to their transactions, they should contact the police, Service Canada offices and the various institutions so that we can resolve the situation. To date, no fraud has been reported.

Mr. David de Burgh Graham: The leak is recent, however.

Ms. Elise Boisjoly: As I was saying, despite the number of leaks detected in recent years, there are about 60 cases per year requiring a change in the social insurance number.

Mr. David de Burgh Graham: Is there a way to indicate somewhere that the social insurance number is no longer valid and then remove the liability associated with it?

If I change my social insurance number and I am still responsible for the old one, in my opinion, it doesn't make sense. Can you tell us more about this?

Ms. Elise Boisjoly: One of the reasons is that we do not know to whom citizens have given their social insurance number. The social insurance number should only be used as an identifier to link certain information to provide benefits. Individuals are the only ones who know to whom they have given their social insurance number and for what purpose. You can give your social insurance number for private pensions, insurance and car rentals or purchases, for example.

The social insurance number should not be used to identify the person. This is a number that allows you to link certain files. We need this number to link the information. We now link the two social insurance numbers in our systems, but the first should never again be used by the individual.

● (1700)

[*English*]

The Chair: Thank you, Mr. Graham.

Mr. Clarke, for five minutes, please.

[*Translation*]

Mr. Alupa Clarke: Thank you, Mr. Chair.

Good afternoon, everyone.

Thank you for waiting and staying here.

Ms. Boisjoly, you are the assistant deputy minister at the Department of Employment and Social Development Canada. Did your minister instruct you to get the list? I asked the same question of Mr. Cormier. Have you received ministerial instructions to obtain the list of the 2.9 million Canadians affected by the massive data leak at Desjardins?

Ms. Elise Boisjoly: You raise an interesting question.

The first thing to do, according to the Personal Information Protection and Electronic Documents Act, is to inform third parties. As you have heard, Desjardins has contacted us to ensure that we will provide the information and help Desjardins branches obtain as much relevant information as possible to help their members. In this case, we have given a lot of information on how to protect their members.

Mr. Alupa Clarke: So there were no guidelines. In other words, you are reactive. I'm not talking about you, of course. You follow political orders, and we understand that. At the moment, everything is reactive and absolutely nothing is proactive.

You said you received 1,500 requests or calls about the social insurance number. Our goal is to know how the government can help people proactively. Since you don't know which Canadians are affected, you necessarily have to wait for them to contact you. That is what is happening right now. You wait for the people affected to contact you, not the other way around. That's impossible, because you don't have the data. Mr. Cormier, from Desjardins, seemed to say that they would be ready to send this data. I know I'm asking you to give a political opinion, but you can't.

I have to express something that royally disgusts the people in my riding. I went door-to-door a lot last week and the week before that. People have consistently told me that they doubt that the government can do anything. It saddened me very much. How is that possible? I would like to break the cynicism and listen to people. People contribute 50% of their income to the Canadian government. We Conservatives want the government to work for citizens, not the other way around.

Mr. Cormier said that when someone calls Desjardins, they are proactive and take care of things for them.

We learned something very important today. In fact, we already knew that because it had been mentioned here and there. I learned from an official like you that you can change your social insurance number. I know it's complex and that even if we change it, we still have to reach a myriad of institutions, our former employers, and so on. However, it is the government that requires that citizens have a social insurance number. It is a system that should perhaps even be called into question, and we are discussing it today, in a way.

Wouldn't it be your duty to contact the 2.9 million people? The Liberal government should do this to be proactive. It knows these people. For example, at the Pizzeria D'Youville, where I worked in 2004 when I was 17, it was the boss who sent the GST to the federal government. All these things are well known. Your departments could easily link this information and change the social insurance number, perhaps not in a comprehensive way, but it should support the citizen in the very difficult task of reaching all former employers or government agencies.

I really don't like this. I know it's not your fault. You have political directives from the Liberal government, but it is not proactive at the moment. I don't like it at all. What can you say about this?

Ms. Elise Boisjoly: In view of the multiple leaks that can occur, the goal is to ensure that citizens and the benefits due to them, whether tax refunds or other benefits, are always protected. That is why we worked very closely with Desjardins to define what measures would enable us to support it in its relations with the affected citizens.

Desjardins has implemented measures. When there were leaks at the federal level, very similar measures were taken with respect to credit bureaus, because it is really the best way to protect citizens from fraud. We continue to work with Desjardins. If an exchange of information proved to be a good solution, we would consider it. However, at this stage, the measures put in place are the best that could have been taken.

● (1705)

Mr. Alupa Clarke: Thank you, Ms. Boisjoly.

[*English*]

The Chair: Are there any questions over here? No.

Mr. Dubé, for three minutes.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

I would like to come back to the question I asked, namely whether you want to hold information sessions in major centres in Quebec, among others. I know that people outside Quebec are also affected, but it is in Quebec that the leak had the greatest impact. The population must be informed.

I forgot what it was, but I have already received a letter in the mail regarding a change in federal policy. I would like to believe that it is possible to send letters by mail to the people of Quebec informing them of the schedule of public consultations or information sessions that will take place in the next two months. You are giving us information today and I think people are listening, of course. Nevertheless, we should make sure to reach as many people as possible. Despite the pervasiveness of social media, I am not convinced that this response is adequate.

Is this something you are open to? I believe that the Department of Finance and the Canada Revenue Agency also have a role to play.

Ms. Elise Boisjoly: Absolutely.

To be proactive, we have put additional information on our website. We have issued press releases. We used social media, as you said. We hold workshops on the social insurance number in several communities. These are workshops that are given on a regular basis and I won't see why we can't use this method as well.

So, thanks for the recommendation. We will take it into consideration.

Mr. Matthew Dubé: Perfect. We thank you for that because these are indeed special circumstances, and when there are natural disasters, for example, the local government—whether it is the municipalities or the Government of Quebec—always answers.

As my colleagues said, and not to insult anyone, the federal government is the furthest away. In this case, there are real impacts on people's lives.

Either way, if we ourselves—I'm just talking about myself right now—don't necessarily know how to navigate the social insurance number system when we are federal legislators, I don't think it's because of our own ignorance. It's just a very complex system. That's why you're here today, and that would be knowledge worth sharing.

Thank you for your openness. This completes my questions.

The Chair: Fine.

You have two minutes, Mr. Fortin.

Mr. Rhéal Fortin: Thank you, Mr. Chair.

I'll start with Ms. Boisjoly.

If we consider that the social insurance number was created in 1964 to govern employer-employee and government-to-government relations, we see that it is used in every way now, but in any case, much more widely than before.

Wouldn't it be necessary to review the security regulations concerning its use? For example, there could be a PIN that matches the health card, fingerprints or other data, for example.

In your opinion, can anything be done with this?

Ms. Elise Boisjoly: That is an excellent question.

As I always say, it is important, when you have situations like this, to review and rethink certain things.

As far as the social insurance number is concerned, as I said, it is one of several identifiers. At the federal level—and, of course, in many places— people are invited to add secret questions that only they can answer. It is not a PIN, but it is an additional way to ensure security and identify the right person.

Mr. Rhéal Fortin: Correct me if I'm wrong, but the social insurance number is valid, regardless of whether or not we have matching questions.

I am asked for my social insurance number for a transaction, whatever it is, with a bank, or whatever. I don't have a PIN. I just have the number.

Ms. Elise Boisjoly: You are absolutely right. You do not have a PIN.

Is this something we could consider? Maybe. What is important to say is that, to access a service, you must give other identifiers such as the line...

Mr. Rhéal Fortin: It depends on the companies we request services from, but, I agree, you're right.

Wouldn't a penalty be appropriate? We see that retailers or banks frequently ask for social insurance numbers, and this is not always necessary. Shouldn't there be a system of penalties for those who ask for a social insurance number when they don't need it?

● (1710)

Ms. Elise Boisjoly: That is an interesting question. I don't know if any predecessors have addressed this issue.

Currently, we have a very clear list of who can do so. We have very clear instructions for citizens. When someone asks them for a social insurance number and they are not on the list of people who should ask them for it, they can seek redress with the Privacy Commissioner of Canada.

Mr. Rhéal Fortin: Couldn't we include criminal provisions in the act for this, whether it be a fine or some other sanction?

Ms. Elise Boisjoly: Yes, it would be something to check, but I don't have any information on that today.

Mr. Rhéal Fortin: All right. Fine.

I have one last question if you...

The Chair: Unfortunately, your time is up, Mr. Fortin.

[*English*]

That ends our questioning.

On behalf of the committee, I want to thank the officials not only for your initial appearance but also for your subsequent appearance and waiting for the other witnesses.

We are going to suspend and then go in camera. We will take a couple of minutes to clear the room.

[*Proceedings continue in camera*]