HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

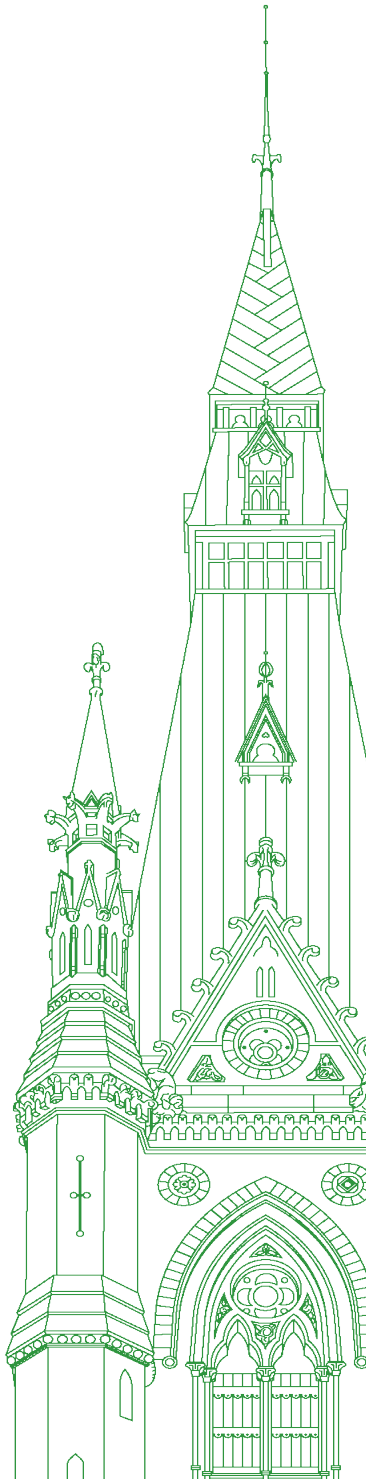
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 140

Thursday, November 21, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 21, 2024

● (1555)

[*Translation*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I call this meeting to order.

Welcome to meeting number 140 of the Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

Is everybody ready to go here?

Okay, good.

[*Translation*]

Before we begin, I would ask all in-person participants to read the guidelines written on the updated cards on the table. These measures are in place to help prevent audio and feedback incidents, and to protect the health and safety of all participants, including the interpreters. You will also notice a QR code on the card, which links to a short awareness video.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, October 29, 2024, the committee is commencing its study of privacy breaches at the Canada Revenue Agency, or CRA.

I would like to welcome our witnesses for the first hour.

Appearing today we have the honourable Marie-Claude Bibeau, Minister of National Revenue. By her side, from the Canada Revenue Agency, we have Bob Hamilton, commissioner of revenue.

Minister, you have up to five minutes for your opening remarks.

Hon. Marie-Claude Bibeau (Minister of National Revenue): Thank you, Mr. Chair.

Thank you for the opportunity to discuss the Canada Revenue Agency's work regarding unauthorized access to taxpayer information.

First and foremost, it is absolutely essential to mention that protecting taxpayer information remains one of the highest priorities for the Government of Canada and the agency. We have zero tolerance for fraud in all of its forms.

Allow me to use this introduction to paint you a picture of the world we are currently living in. Unfortunately, the increase in fraud and identity theft is a global trend. All government institutions and private sector organizations around the world face these constant and persistent threats. No organization is immune to this phenomenon, not even Government of Canada institutions. In fact, the Canadian Anti-Fraud Centre continues to warn Canadians about these ongoing threats. Within the agency, since 2020, there has been a significant increase of identity theft cases and unauthorized use of third-party taxpayer information following the announcement of COVID-19 emergency benefits.

Later that year, the agency also saw a marked increase in external data breaches and cyber-threats. I want to reassure everyone that the agency has implemented a multi-layered security approach to counter these threats. First, the agency regularly monitors taxpayer accounts for suspicious activity to identify, prevent, and quickly address potential fraud and identity theft.

The agency has also implemented many tangible measures to make its systems more robust. These include multifactor authentication, the revocation of high-risk identifiers, the requirement to have an email registered in the agency's My Account portal, CAPTCHA tests, which ensure that the agency is dealing with a human, not a robot, and increased penetration testing of its computer systems. To combat fraud, the agency also combines advanced data analytics with intelligence gathered from a variety of sources, including law enforcement and financial institutions.

In addition, the agency continues to collaborate with domestic and international partners to develop and update its strategy, and prevent these violations from continuing. To this end, the agency maintains regular communication with the Office of the Privacy Commissioner of Canada on various subjects. These communications include privacy breach management, privacy investigations, and new or amended initiatives that involve the use of personal information.

[*English*]

Internationally, the agency is a member of the joint chiefs of global tax enforcement, known as the J5. This organization brings together five countries, including Canada, which conduct coordinated operations to apprehend fraudsters who commit cross-border tax crimes.

In addition, the agency has dedicated teams to address issues related to fraud, whether it be privacy breaches, identity theft or tax schemes of all kinds. In recent years, the agency has also increased the resources dedicated to combatting fraud of all kinds.

Finally, I can assure you that the agency continues to invest tirelessly in security while improving its technologies, processes and controls.

I'll conclude by telling you that the Government of Canada and the agency take the fairness and integrity of Canada's tax system very seriously. Canada's self-assessment system is based on the trust of individuals and businesses in the agency. Everyone here is doing everything in their power to keep that trust at a high level.

Thank you, Mr. Chair.

● (1600)

The Chair: Thank you, Minister.

For the benefit of other committee members, I've asked Mr. Hamilton to make his declaration in the second hour, so that we can maximize the time we have with the minister.

Minister and Mr. Hamilton, as you know, members have short periods of time to ask questions. Please don't take any offence if they want to reclaim their time and ask another question.

Mr. Chambers, you have six minutes. Go ahead, sir.

Mr. Adam Chambers (Simcoe North, CPC): Thank you very much, Mr. Chair.

Thank you for coming. I believe it's our first time at committee together.

When were you first made aware of the privacy breach that was reported by the CBC just a couple of weeks ago?

Hon. Marie-Claude Bibeau: As you know, I can't speak of any specific occurrence.

[*Translation*]

However, I can tell you that as soon as I took up my post at the Canada Revenue Agency in July, I was given a comprehensive briefing on all potential fraud situations and the cases being examined. I am also notified of any situation that requires special attention.

[*English*]

Mr. Adam Chambers: You were informed of fraud when you arrived at the CRA, or when you received your first briefing. Is that correct?

[*Translation*]

Hon. Marie-Claude Bibeau: I was given a general briefing on background and the possible problems.

[*English*]

Mr. Adam Chambers: I appreciate that, but as it relates to the specific privacy breach that was reported in connection with H&R Block, when were you made aware of those cases?

[*Translation*]

Hon. Marie-Claude Bibeau: Mr. Chambers, I'm sure you're well aware that, under section 241 of the Income Tax Act, I can't talk about a specific case, whether this one or any other. I can't answer that question.

[*English*]

Mr. Adam Chambers: Minister, I'm very familiar with section 241. We are not talking about a particular taxpayer at the moment. We're asking when you were made aware.

There is a briefing note, a memo, that has the following in it: “Consensus is that these gaps pose major risks to the agency. While there are [internal] funding and [human] resource considerations, all agree that visibility is needed”.

Do you recall receiving that memo?

[*Translation*]

Hon. Marie-Claude Bibeau: I get quite a lot of memos. I am briefed, whether verbally or in writing, on a regular basis. It wouldn't surprise me.

[*English*]

Mr. Adam Chambers: Perhaps the commissioner might be able to shed some light.

Do you recall the memo that I'm referring to? This was reported by the CBC.

Mr. Bob Hamilton (Commissioner of Revenue, Canada Revenue Agency): No, I do not.

I would just echo what the minister said, that we don't talk about specific cases.

Mr. Adam Chambers: I have very limited time, Commissioner. I appreciate it.

Minister, your testimony is that you cannot tell Canadians when you learned of a serious privacy breach that was reported in the news.

[*Translation*]

Hon. Marie-Claude Bibeau: I am quickly notified when the agency detects a potential fraud case.

[*English*]

Mr. Adam Chambers: It would be fair to say that, if you were rapidly informed, when the breach occurred you likely would have been informed shortly thereafter. Is that correct?

[*Translation*]

Hon. Marie-Claude Bibeau: Absolutely. When there is a privacy breach of any significance, I am quickly notified.

[*English*]

Mr. Adam Chambers: Wonderful.

Why was that breach not reported to the public, as a material breach, when you learned of it, shortly after it occurred?

[*Translation*]

Hon. Marie-Claude Bibeau: The way we operate at the agency is as follows: As soon as we suspect that identity theft has occurred, we block the account and then we communicate directly with the individual, individuals or company concerned.

Only in cases where the issue is more widespread, such as during the COVID-19 pandemic, do we alert the public. However, the individual or individuals involved were immediately notified.

[*English*]

Mr. Adam Chambers: There are thousands of taxpayers affected, though. If this breach occurred outside of government, there are obligations for those organizations to inform the public. Why is it that this breach was not publicized? Worse, why was it withheld from the Privacy Commissioner until after the deadline passed for him to include it in his report in 2024?

[*Translation*]

Hon. Marie-Claude Bibeau: As the Auditor General of Canada's 2022 report shows, we had begun disclosing, and passing on, the information. You're talking today about 31,000 accounts that were affected by identity theft, but that happened over a number of years. If you go back to the Auditor General's report from 2022, it's clear that 23,000 cases had already been made public.

● (1605)

[*English*]

Mr. Adam Chambers: If the process at CRA works really well and the minister is informed relatively shortly after—you're made aware of privacy breaches that happened over multiple years—it is reasonable to assume that you or your predecessor were made aware of these privacy breaches well before the March deadline that the Privacy Commissioner needs in order to include these privacy breaches in their annual report to Parliament. Why was it that these privacy breaches were reported to the Privacy Commissioner after the deadline, when your own testimony suggests that you would have been made aware of these privacy breaches well before the deadline to report these to the public?

[*Translation*]

Hon. Marie-Claude Bibeau: I am quickly notified whenever there is any attempted identity theft, which must then be verified. That involves immediately notifying the individual or individuals of the problem and reporting it. As I said, we had already started reporting the situation, as per the Auditor General's 2022 report.

[*English*]

Mr. Adam Chambers: Minister, according to the Privacy Commissioner, there have been very few breaches at the CRA, because he was not made aware of them to include them in his report in 2024. The timeline just doesn't quite work for me at this moment, but I believe I've exceeded my time.

The Chair: Thank you, Mr. Chambers.

Next, we're going to go to our friend from Châteauguay—Lacolle.

Ms. Shanahan, you have six minutes. Go ahead, please.

[*Translation*]

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you, Mr. Chair.

My riding of Châteauguay—Lacolle will soon be called Châteauguay—Les Jardins-de-Napierville. I'm very proud the name was changed and will be used by local associations.

Minister, thank you for being with us today.

For those who don't know, I worked in income tax preparation for a long time, and I discussed how important it was for Canadians to be educated, advised and supported in relation to their tax returns. I've seen how things have evolved. When I started out, tax returns were done on paper, which Mr. Villemure may also remember. We had to make sure that Quebec tax returns were consistent with federal ones.

Later, with software developments, the data were automatically transferred. Now we can access our confidential data on a website. I always tell people I know that the software is mainly for verifying that there are no errors or problems in the data.

Minister, what do you think is the best way for Canadians to make sure their returns are filed properly?

Hon. Marie-Claude Bibeau: Thank you, Mrs. Shanahan.

The agency does a lot in the way of communications. I would say the first recommendation is for people to make sure they don't use the same user name or password for everything. Easily identifiable passwords make people extremely vulnerable. In the unfortunate event a scammer figures out our log-in information, they can access our banking data, our account with the agency or what have you.

The agency has a whole communication strategy on its website. It also provides different kinds of training and tools to help people protect themselves. Digital hygiene is extremely important because most, if not all, of the identity theft cases we're talking about today involve information stolen outside the agency. Everyone has trouble remembering all their passwords, which is why people tend to choose the same ones. The scammers we're talking about obtained access credentials and passwords from a source outside the agency and used them to get into the agency's website. Therefore, it's really important that people protect themselves.

● (1610)

Mrs. Brenda Shanahan: Thank you for that information.

Since we're talking about identity theft, I was at the Standing Committee on Public Accounts last year, when we had the same discussions. One of the witnesses was Mr. Hamilton, who is here today. The Auditor General looked into it and did an analysis, at which point it became public. There were about 20,000 cases at the time.

However, we understand that it's also a matter of timing. We file our tax returns three or four months after the beginning of the fiscal year, which starts on January 1 and ends on December 31. It takes time, both for taxpayers and the CRA, to ascertain that something has happened. Then the process takes a few more months, which can extend to two or three fiscal years. I'd like to hear your comments on that, but first I'd like to know something. The Auditor General found that the actions the agency took at the time were appropriate. Would you say the same is true now? Are you satisfied with the measures the agency is taking at this point?

Hon. Marie-Claude Bibeau: Yes, I am.

The agency has many systems in place to protect Canadians. We work in partnership with a number of institutions here in Canada, but also internationally. When a situation occurs here or abroad, the institutions disclose it and share techniques to prevent it from reoccurring. There are multiple layers of the safety net. That way, if an attack were to slip through the first layer, another layer would be there to catch it.

One layer of the safety net is multifactor authentication. Every time a citizen wants to change information in their My Account, such as their address or their bank account number, they immediately receive an email. If anyone receives an email that says their bank account number has been changed in their Canada Revenue Agency file and they haven't made that change, they need to immediately call the CRA to block the account.

As you see, we have put in place a number of security measures to prevent fraud as much as possible. Scammers are creative, but so are we. We have the skills. We have a team that keeps its eye on the ball to protect citizens every time a new scam comes up.

The Chair: Thank you, Minister and Mrs. Shanahan.

Mr. Villemure, you have the floor for six minutes.

Mr. René Villemure (Trois-Rivières, BQ): Thank you, Mr. Chair.

Minister, thank you for being with us today. I have a number of questions for you.

I heard you say in your previous answers that users often bear the burden of protecting themselves, for example by changing their passwords. As everyone knows, digital life is complicated. People tend to trust an organization like the CRA. By definition, trust means not always having to bear the burden of proof, but that's what people have to do now. There is a logical disconnect. Isn't there a way to avoid putting all the burden on users?

Hon. Marie-Claude Bibeau: I think it's a shared responsibility. Everyone has to take precautions, like buckling our seat belts. People have a personal responsibility, but I can assure you that the agency is focusing a tremendous amount of effort, energy, investment and training on protecting people from identity theft.

Again, the information in question was obtained through systems outside the CRA. People used that information to get into our system. The CRA is implementing a number of measures. For example, in order to access an account, users are required to click on all the squares of an image that feature a bicycle. That's already a way of ensuring that a person, not a machine, is trying to get into the system. Another way is entering a code sent to a cellphone. A number of similar measures are being put in place. You know what I'm talking about, right?

Mr. René Villemure: Yes, I understand very well. Thank you.

How many employees does the Canada Revenue Agency have?

Hon. Marie-Claude Bibeau: There are close to 60,000.

Mr. René Villemure: Of those 60,000 employees, how many are front-line supervisors?

Hon. Marie-Claude Bibeau: I'll ask the commissioner to answer that, because I couldn't tell you.

● (1615)

Mr. Bob Hamilton: I don't have that number at my fingertips either. I would have to check on that.

Hon. Marie-Claude Bibeau: Mr. Villemure, what do you mean by “front line”?

Mr. Bob Hamilton: We have about 400 senior managers, which is a higher management level. I'll find the information.

Mr. René Villemure: Okay. I guess that's the second level of customer service.

I'd like to know one thing. When whistle-blowers flag a problem within an organization, the reason is often that they reported the situation but to no avail. What's your take on that?

Hon. Marie-Claude Bibeau: As far as whistle-blowers are concerned, I completely agree that some situations need to be reported. That is why we support Bill C-290, which is a step in that direction.

The CRA is unique in that it is a prime target because it holds a lot of personal information. We are governed by the Income Tax Act, including section 241. A lot of measures revolve around that. We have a code of ethics, and we need to comply with it.

All employees are responsible for protecting the integrity of the tax system and obviously cannot compromise ongoing investigations.

Mr. René Villemure: Of the 60,000 employees, or the 400 people in senior management positions, how many of them are teleworking?

Mr. Bob Hamilton: According to the current rule, all employees need to work three days a week in the office.

Mr. René Villemure: Okay.

Mr. Bob Hamilton: Some employees currently have an exemption, but in general, all employees have to work three days a week in the office. There are people who have to work in the office five days a week because of their position.

Mr. René Villemure: Okay.

Were many of them hired postpandemic?

Hon. Marie-Claude Bibeau: Of course. Before the pandemic, we had 43,000 employees. At the height of the pandemic, we had 62,000. Today, we have about 58,000.

Mr. René Villemure: Every organization has a corporate culture. However, it's reasonable to believe that some employees didn't know the agency as it was before the pandemic. Admittedly, telework may have made it more difficult to adhere to the agency's culture of confidentiality. I would like to know whether employees are being properly supervised, considering that some do not work or have never worked in the office.

Hon. Marie-Claude Bibeau: I don't know what level of supervision you're talking about, but I think we do find ways to do what we need to do. COVID-19 has taught us all to work differently.

I can assure you that mechanisms are in place to ensure employee integrity. Obviously, employees' level of access to information depends on their position. Not everybody has unlimited access.

Mr. René Villemure: However, the whistle-blowers still felt that nothing was done.

Hon. Marie-Claude Bibeau: Once again, keep in mind there are nearly 60,000 employees. Obviously, not all employees are aware of all the work that the security team, other teams and partners are doing to try to improve the systems.

Furthermore, I have a problem with the use of the term “whistleblower” in our situation. The information that was publicized in the media was already made public in the Auditor General's reports and the evidence of the Standing Committee on Finance and the Standing Committee on Public Accounts. The media didn't say anything new. Perhaps it was news to the general public, but the agency and parliamentarians already knew it.

Mr. René Villemure: Okay. I will get back to that in the next round. Thank you.

Hon. Marie-Claude Bibeau: Thank you, Mr. Villemure.

[*English*]

The Chair: Thank you, Mr. Villemure.

Mr. Green, you have six minutes. Go ahead.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you very much.

Minister, I have to state right off the top that I found your responses to Mr. Chambers highly evasive. I'm going to give you the opportunity to reply on the Nixon test. I'm going to start with an agreed statement of fact that you've raised.

You stated that the AG reported in 2022 that 23,000 accounts had been breached. Is that correct?

Hon. Marie-Claude Bibeau: Yes.

Mr. Matthew Green: You took office in 2023. Is that correct?

Hon. Marie-Claude Bibeau: Yes.

Mr. Matthew Green: In that transition, you would have been updated on the breaches in 2022. Is that correct?

Hon. Marie-Claude Bibeau: Yes.

Mr. Matthew Green: You would have been aware that some $190 million in scams due to hacking came from losses that went as far back as 2020. Is that correct?

Hon. Marie-Claude Bibeau: Yes—

Mr. Matthew Green: We now know that in July, 31,000 accounts were breached. Is that correct?

● (1620)

Hon. Marie-Claude Bibeau: Yes, it's reasonable.

Mr. Matthew Green: When did you know that the 31,000 accounts had been breached? Was that back in July 2024?

Hon. Marie-Claude Bibeau: I can't be that specific.

Mr. Matthew Green: Why not?

Hon. Marie-Claude Bibeau: Because I don't recall every briefing I've gotten in the last year.

Mr. Matthew Green: This is a significant breach.

Hon. Marie-Claude Bibeau: I know, but you're asking me about specific numbers.

Mr. Matthew Green: Respectfully, Minister, we're talking about a material breach of the privacy of thousands of people, regarding hundreds of millions of dollars, in your department.

Mr. Hamilton, I'll put to you the Nixon test. At what point in time did you know these breaches happened?

Mr. Bob Hamilton: I am kept regularly aware of the breaches that happen. I think, just for clarification—

Mr. Matthew Green: The date, sir. I'd like to know the date that you knew.

Mr. Bob Hamilton: I don't know the dates off the top of my head.

Mr. Matthew Green: You don't know the date.

Mr. Bob Hamilton: No.

Mr. Matthew Green: Did you know that you were coming to this committee to talk about this issue?

Mr. Bob Hamilton: Yes.

Mr. Matthew Green: What briefings did you do in preparation for this committee?

Mr. Bob Hamilton: I made sure that I was aware of all the actions we have taken, the history of the file—

Mr. Matthew Green: Including the dates?

Mr. Bob Hamilton: I think it's important—not the specific date of when I became aware, but—

Mr. Matthew Green: Okay.

Mr. Chair, I just want to make reference that the commissioner has on his desk right now—I'll describe for the Hansard—a briefing document.

I would put to you, Minister, that you would also be well aware of the last five weeks of filibusters that we've had, based on a committee's ability to demand documents. Is that correct?

The reason I'm bringing that up, sir, is that I don't want to have to ask this committee to move a motion to request that you submit all the documents that are sitting on that table. What I'd rather you do is just answer with clarity, because I am unwilling to accept that you came to this committee without any understanding of the dates on which you would have been informed that these breaches happened.

Mr. Bob Hamilton: Can I take a stab at answering your question?

Mr. Matthew Green: You can attempt. Sure.

Mr. Bob Hamilton: I think it's important, first off, to differentiate between two periods. There was the pandemic and there's post-pandemic, and there were a lot of breaches that occurred during the pandemic. I think you referenced 23,000 or whatever, and as we went—

Mr. Matthew Green: My clock is running. Unfortunately—

Mr. Bob Hamilton: —more cases became known, and it grew to 31,000.

Mr. Matthew Green: At what point does it become material enough that you feel like you have a duty of candour to the public to let them know that this scale of privacy breach has happened within your department, sir?

Mr. Bob Hamilton: There was actually a press conference at the time of the pandemic that indicated we had a—

Mr. Matthew Green: I'm talking about under this minister's administration.

Mr. Bob Hamilton: —and then we report these in a transparent way to the Privacy Commissioner. I am acknowledging there was a delay in the reporting, but—

Mr. Matthew Green: Mr. Hamilton, there seems to be a culture of secrecy here. Can you please tell me about your department's policy on whistle-blowers?

Mr. Bob Hamilton: Sure. I can tell you we're among the most transparent in giving information out. I acknowledge the delay. Our policy on whistle-blowers is that we encourage people to talk to their managers, their supervisors, if they see something. Secondly, we have an internal process whereby, in anonymity, people can bring the concerns they have if they think they see something is going wrong. Then, above that, across the whole government, we have a Public Sector Integrity Commissioner whom people can complain to.

Mr. Matthew Green: That leads me to the email that you sent out. I'm sure you'll recall the email that you sent out about upholding our integrity. When we speak about whistle-blowers in the context of public disclosure, we often mean taking a risk at your place of employment to disclose to the public potential malfeasance or malpractice that would be happening within your workplace for the benefit of the public good. You haven't described that. What's your opinion on whistle-blowing as it relates to employees inside your agency who might present to the public problems that are happening within your agency?

Mr. Bob Hamilton: There are two things I would say. We have good internal processes for people to whistle-blow and for action to be taken. The second thing is that employees have a responsibility to not talk about taxpayer information.

Mr. Matthew Green: It's not information specifically. It's not disaggregated information.

Mr. Bob Hamilton: It can be.

Mr. Matthew Green: It's about a major and massive breach of privacy to the average Canadian for whom, by the way, when that happens, there's the kind of pain.... I help process thousands of tax returns for people, and I know that if there's fraudulent work that's happening there, many of these people—seniors, people on fixed incomes—all of a sudden are not getting their OAS or their GIS. They're not getting all their entitlements, not to mention their tax returns.

I'm going to put one last question to you, sir, in this round, and I'm going to ask you to answer it honestly, so that I don't have to move a motion to demand that you provide it to this committee. What is the total amount lost to the public purse, including on bogus payouts on GST and business returns, whether or not it's from the hacked accounts?

Mr. Bob Hamilton: What was the last part, sorry?

Mr. Matthew Green: It was whether or not it's from the hacked accounts. Generally speaking, what is the cost of the total amounts lost due to bogus payouts on GST and business returns?

● (1625)

Mr. Bob Hamilton: I don't have that number. We actually have officials who will come for the second hour who might be able to help; otherwise, we'll have to get back to you.

Mr. Matthew Green: Thank you.

Mr. Bob Hamilton: The other thing I would say on your whistle-blower is, yes, you can't give out taxpayer-specific information, and we also don't talk publicly about the schemes that people are trying to do with us or our actions, because we don't want to perpetuate the playbook, if you like, out in the public domain. We have a strong culture of trying to encourage people, if they see something going wrong, to go through the mechanisms.

The Chair: I'm sorry. We have to stop you there.

My understanding is that there's a problem with the English translation.

Mr. Matthew Green: On a point of order, there's French translation coming in.

The Chair: I was just made aware of that, Mr. Green. I wonder if we can have a test here to determine....

A voice: It's good.

The Chair: Okay.

[*Translation*]

That concludes the first round of questions. We will now begin the second round.

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

Mr. Luc Berthold (Mégantic—L'Érable, CPC): Thank you, Mr. Chair.

Good afternoon, Ms. Bibeau.

In your opening remarks, you used what I would call government-speak. Unfortunately, your finely crafted presentation provided little detail on what happened, the scope of the problem and the consequences for the citizens who were victims of fraud. There were 31,000 privacy breaches between 2020 and 2023, and 62,000 Canadian taxpayers were directly affected. Have all those cases now been resolved?

Hon. Marie-Claude Bibeau: I can assure you that, as soon as we have the slightest suspicion that there has been a privacy breach, we notify the person concerned immediately. I want to make that clear.

Mr. Luc Berthold: So you've told us, Ms. Bibeau.

What I want to know is how many people are still waiting for their cases to be resolved. How many people are still waiting for cheques? Have all the cases been resolved?

Hon. Marie-Claude Bibeau: I would have to check with the team, but what I can tell you is that there are different levels of privacy breaches. In some cases, the fraudster will have had access to the file, but will not have been able to see anything. So they couldn't have used the information for anything else. Cases like that are resolved quickly.

Mr. Luc Berthold: I'm talking about cases where fraud has occurred, where money has been paid and an investigation has been launched. As we know, when people are under investigation, no transaction is possible until the situation has been resolved.

I can tell you about two cases, but I'm not allowed to name the people involved, either. In the first case, a complaint was received on April 28, 2022, and it was resolved on July 26, 2024. Therefore, the person was unable to access all the government assistance amounts to which they were entitled for two years. The other case was reported to us on May 20, 2020, but it was not resolved until October 8, 2024.

Ms. Bibeau, as minister, are you not affected when you hear that or read those kinds of articles?

Hon. Marie-Claude Bibeau: Of course I am affected. Each case is certainly important, and I assure you that the agency is doing its utmost, which depends on the level—

Mr. Luc Berthold: Ms. Bibeau, I want to know what you do, not what the agency does. Do you call the agency to tell it that the problem has to be resolved quickly or do you wait for the next briefing? Do you go after whistle-blowers so that the story doesn't get picked up by the media?

Hon. Marie-Claude Bibeau: No, that wouldn't be fair.

Mr. Luc Berthold: Tell me what's fair for the people who are waiting for their cases to be resolved and who don't have access to government assistance. Tell me what's fair right now.

Hon. Marie-Claude Bibeau: I assure you that the people on our teams are working hard.

What I'm trying to say is that the level of attack or access to customers' accounts varies. Some cases can be resolved very easily, while others have a greater impact, requiring more time. We're there to help people. There are protection systems in place, and we are working with TransUnion, for example, to protect the data.

Mr. Luc Berthold: Can you commit to resolving these cases much more quickly? We're talking about people who don't have access to government assistance and families who aren't able to buy food. We all work hard as members of Parliament. You know that there have been horrible cases where people are waiting for solutions. However, what I'm hearing from you is that you can't talk about specific cases, that you're doing your best and that there are different levels of privacy breaches. Again, this is government language.

As minister, you are responsible for the agency. Don't you feel like rattling the cage and telling the agency that these cases must be resolved in two months, so that you can move on to something else?

Hon. Marie-Claude Bibeau: I'm sure we'll be able to give you much more detailed examples, and I assure you that we're trying to act as quickly as possible, but it doesn't always just depend on the agency. It controls what it can, and it is able to act quickly. However, the situation sometimes goes beyond the agency, which has to work in partnership with other players because it doesn't have all the levers.

● (1630)

Mr. Luc Berthold: Have complaints been made to the police about all those frauds? Is an organized criminal network involved?

Hon. Marie-Claude Bibeau: The agency can come under different types of attacks. For example, there are “credential stuffing” attacks—

Mr. Luc Berthold: Have complaints been made to the police?

Hon. Marie-Claude Bibeau: Yes, there are all possible status categories.

Mr. Luc Berthold: How many police investigations into fraud cases are currently open at the agency?

Hon. Marie-Claude Bibeau: I couldn't tell you how many investigations are currently open.

Mr. Luc Berthold: Mr. Hamilton, can you answer that question?

[*English*]

Mr. Bob Hamilton: Yes. I can't say how many for sure, but what I can tell you is the way we look at these cases. If we see that there is a possibility of criminal activity, we have our own criminal investigators, and we can also refer it to the law enforcement authority.

[*Translation*]

Mr. Luc Berthold: How many cases have been referred to the police?

Mr. Chair, perhaps the minister could send that information to the committee.

[*English*]

The Chair: Please answer that question quickly, Mr. Hamilton.

Mr. Luc Berthold: The question is very clear. How many have you sent to the police?

Mr. Bob Hamilton: I would have to consult with my team about exactly how many, and we may even have to get back to you on that, but we do have the ability to do that, and that also applies not just in fraudulent cases like this but also in tax evasion cases where we might see criminal activity.

The Chair: Okay, thank you.

Mr. Housefather, you have five minutes. Go ahead.

[*Translation*]

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you very much, Mr. Chair.

Minister, thank you for appearing before the committee today. Before I ask you questions, I'll turn to Mr. Hamilton.

[*English*]

Mr. Hamilton, on the 31,000 cases that keep getting cited, this was not just one breach. This was a series of different, smaller breaches. Is that correct?

Mr. Bob Hamilton: Yes, that's right. It was a similar type of breach in many cases, but yes, it was a bunch of breaches.

Mr. Anthony Housefather: These were third party breaches. These were not breaches of the CRA's own system; these were breaches of third party systems linked to the CRA. Is that correct?

Mr. Bob Hamilton: Yes. If you take a stylized example, it would be where somebody gets information from another third party outside, maybe a financial institution. That information is sold on the dark web or however, and then people use that information, that password or identifier, to try to break into the CRA system. We saw instances of that during the pandemic, when there were significant amounts of money at play, and that caused us to really ramp up our activities in the fraud space beyond what we had before the pandemic.

Mr. Anthony Housefather: Thank you.

I'm trying to clarify things that have come up in some previous rounds to give you a chance to explain. There were a number of questions from Mr. Green about the timing of when you became aware of these breaches, and because there were a number of different breaches, you became aware of them, no doubt, at different times.

I'm not trying to ask for a specific date, because I think that's where you were getting caught up. You were trying to think if you heard on February 14, February 27 or March. Can you remember around what period you became aware of the different breaches?

Mr. Bob Hamilton: Are you referring to all the way along?

I would say that there was a big event in about August 2020, when we uncovered that there was a lot happening, and we saw some vectors coming in. That was a big number. Since then, we've seen some of those types, but we've also seen other types of cases where people have not necessarily come in and tried to get CERB money or what have you; they're using the speed with which we give out refunds, etc., to try to create false returns and get refunds. It's a different kind of fraud, but we did see those coming up. That's a continuum; it doesn't happen all on one day. It happens as you go. I would honestly have to say that I don't know the specific dates of when it went from 23 to 25 to something else, but perhaps some of my colleagues do.

Mr. Anthony Housefather: No, I understand. I think it's because this was happening over rolling periods because there were different breaches, so you don't have one specific date that you can just remember offhand, because you were probably briefed a number of different times about breaches. Is that correct?

Mr. Bob Hamilton: Yes, that's exactly right, and they continue. At least where people are trying to attack us, I think we're getting better and better at resisting those. The other thing we pay a lot of attention to is that, when we know about it, we block the account; we take action, and then we pay attention to the individual. We try to resolve that as quickly as we can.

Earlier we talked about there being some delays. It's a big backlog coming out of the pandemic, and we spend a lot of our efforts trying to focus on protecting that individual's account and giving them credit protection where it's warranted. Then we work through it, solve the case and see exactly what happened and what needs to be done to remedy it. I'd like to be able to move even faster. We are moving faster now, but we are still dealing with many cases that came up in the early 2020s.

● (1635)

Mr. Anthony Housefather: Thank you very much.

[*Translation*]

Minister, I know you are a really hands-on person, and this is not new to you.

When you took on your role at the Canada Revenue Agency, you clearly told employees to inform you of anything important, right?

Hon. Marie-Claude Bibeau: You know me very well, Mr. Housefather.

Let me take a quick second to answer Mr. Berthold's question. There have been 135 convictions, $25 million in fines imposed, 58 individuals sentenced to prison terms for a total of 108 years, and $44 million in federal taxes evaded. Those results cover the last five years, from 2019 to 2024.

Thank you, Mr. Housefather.

Mr. Anthony Housefather: Thank you, Ms. Bibeau.

Mr. Chair, do I have any time left?

The Chair: You have three seconds. Your time is up.

[*English*]

Thank you, Mr. Housefather.

[*Translation*]

Mr. Villemure, you have the floor for two and a half minutes.

Mr. René Villemure: Thank you very much, Mr. Chair. Two and a half minutes isn't much, so I'll go quickly.

Minister, I get the impression that there's more of a culture of secrecy than a culture of whistle-blowing at the Canada Revenue Agency. How many cases of snooping are there?

Hon. Marie-Claude Bibeau: You're talking about snooping by employees, right?

Mr. René Villemure: Yes.

Hon. Marie-Claude Bibeau: I assure you that we are monitoring that closely. We have mechanisms in place. Our systems enable us to know when an employee consults a file. An employee who just consults their own file gets five days' suspension. We take that very, very seriously.

Mr. René Villemure: I'm sure you do. However, there may be 3,000 employees a year who do that.

Hon. Marie-Claude Bibeau: Right now, we are in human resources management, generally speaking. There is a gradual scale of punishment. If it does not go to trial, it stays in the human resources management bubble. However, I can assure you that it is taken very seriously.

Mr. René Villemure: However, if I told you that there were 3,000 last year, does that surprise you or not?

Hon. Marie-Claude Bibeau: I don't know.

Mr. René Villemure: Okay. This issue will be raised with you again at some point.

In any event, whistle-blowers will often act out of desperation, when nothing they've done has worked. The supervision wasn't working. Something wasn't working. Why do you think a whistle-blower takes action?

Hon. Marie-Claude Bibeau: Again, I struggle with the use of the term “whistle-blower” in our context.

Mr. René Villemure: Take it out of context. In general, why does a whistle-blower—as there have been in the past at the agency—take action?

Hon. Marie-Claude Bibeau: They take action because they believe that the organization could behave differently, as a matter of paradigm.

Mr. René Villemure: Okay. In general, how many whistle-blower cases are there per year?

Hon. Marie-Claude Bibeau: Again, do you mean the whistle-blowers who are speaking to the media, or the employees who go to the Public Sector Integrity Commissioner?

Mr. René Villemure: I'm talking about the whistle-blowers who go outside.

Hon. Marie-Claude Bibeau: Okay. I can't give you a specific answer.

Mr. René Villemure: So there could be 100 or 1,000.

Hon. Marie-Claude Bibeau: I'd be shocked if it was 1,000.

Mr. René Villemure: This is not the first time there has been a breach of confidentiality or fraud at the Canada Revenue Agency.

Hon. Marie-Claude Bibeau: Let me put things in perspective, though.

Mr. René Villemure: Please do.

Hon. Marie-Claude Bibeau: If I may, I'll give you the dollar amounts.

We hit a spike in identity theft during COVID-19 owing to attestation-based programs. It was the worst year for identity theft, as there was no comparison. In 2020, as you know, and someone mentioned it earlier—

Mr. René Villemure: However, there have been cases of fraud in the past.

Hon. Marie-Claude Bibeau: Yes, there are always some. However, we're talking about losses of $3 million in identity theft last year, when we're bringing out $59 billion. You see the comparison between the $3 million and the $59 billion. I just wanted to put that in perspective.

● (1640)

The Chair: Thank you, Ms. Bibeau.

[*English*]

Mr. Green, I'm going to give you an equal amount of time of three minutes in this round, because Mr. Villemure just had it. Go ahead.

Mr. Matthew Green: Thank you. I appreciate the equity, sir.

Minister, are you currently investigating whistle-blowers within the CRA?

[*Translation*]

Hon. Marie-Claude Bibeau: We are not investigating the employees. We are in the process of reminding employees of their obligations under section 241 of the Income Tax Act.

[*English*]

Mr. Matthew Green: Thank you.

Mr. Hamilton, in a CBC story, you wouldn't deny the fact that you were going through the use of computers to see who was accessing what files and for what. Are you currently investigating whistle-blowers within the CRA?

Mr. Bob Hamilton: When you talk about whistle-blowers, let me say—

Mr. Matthew Green: I mean people who presented information to the public.

Mr. Bob Hamilton: In the public domain, we will always investigate if somebody does something inappropriate relative to our code of ethics or their duty of loyalty to us. For example, when we found there were a bunch of employees who had claimed CERB, that was inappropriate.

Mr. Matthew Green: Sure.

Are you currently investigating the whistle-blowers who resulted in the story by *The Fifth Estate*?

Mr. Bob Hamilton: We are currently looking at all sorts of things that go on in the agency.

Mr. Matthew Green: I'm asking you for a direct answer, sir. Could you please provide the committee with a direct answer?

One more time, are you investigating the whistle-blowers who resulted in the story by *The Fifth Estate*?

Mr. Bob Hamilton: We are looking to determine whether information was true and how it got into the public domain.

Mr. Matthew Green: Will there be retribution? If so, what will it be for the whistle-blowers?

Mr. Bob Hamilton: I have no idea at this stage.

Mr. Matthew Green: Do you not have any policies for this, sir?

Mr. Bob Hamilton: We have policies—

Mr. Matthew Green: What are the policies?

Mr. Bob Hamilton: —but, as it's been indicated, it can go from minor discipline, such as a verbal or written reprimand, all the way up to termination. It depends on the severity of what happened.

We have strict policies about that, so when something bad happens.... To take the CERB case again, there were people who were fired.

Mr. Matthew Green: We're talking with specificity about *The Fifth Estate*. For the people who are watching, and particularly those who, in the public interest, shared information with the public.... Perhaps they felt their loyalty was to the Canadian taxpayer and making sure that they had the right information, not to a bureaucracy or a government per se.

What do you say to those people who are watching this today?

Mr. Bob Hamilton: I say we take very seriously our responsibility in that regard to be honest and truthful and to protect the Canadian public. However, we also have to protect the information that's within the agency, because your information and my information—

Mr. Matthew Green: Is it information or embarrassment?

Mr. Bob Hamilton: We can't allow people to—

Mr. Matthew Green: Is it information or embarrassment? It's not—

Mr. Bob Hamilton: No. It's information—

Mr. Matthew Green: —disaggregated information. It's not like they're talking about my receipts. They're talking about a huge breach that resulted in 31,000 cases of fraud. These aren't material privacy breaches of individual files. There is a systematic and structural failure within the agency to figure out what was going on with these third parties.

They obviously felt it wasn't being addressed, so they went public.

As an MP, quite frankly, I feel like we had a duty to know as well. We also did not have the opportunity to know until we found out in the media.

The Chair: That's the three minutes.

Mr. Matthew Green: I'll let you answer when we come back in the next round.

The Chair: You'll have a chance, Mr. Hamilton, in the second hour. I'm almost certain we're going to revisit this.

Mr. Chambers, you have five minutes, and then we're going to finish this off with Mr. Bains for five minutes.

Mr. Adam Chambers: Thank you, Mr. Chair.

Minister, you testified earlier that you have “zero tolerance for fraud in all of its forms” at the CRA. What's been the loss to taxpayers from all forms of fraud at the CRA, say, last year?

Hon. Marie-Claude Bibeau: Last year, it was about $2 million. This year, as of now, it's $3 million.

Mr. Adam Chambers: I'm sorry. Is that for fraud in all of its forms?

[*Translation*]

Hon. Marie-Claude Bibeau: I'm talking about identity theft.

[*English*]

Mr. Adam Chambers: No, I'm asking for all types of fraud, including GST fraud and carousel schemes. You said “zero tolerance for fraud in all of its forms”.

I'm asking for a number for how much fraud has been perpetrated against the Canadian taxpayer.

[*Translation*]

Hon. Marie-Claude Bibeau: When we say we have zero tolerance, that means we have a strong team, we have systems and we have tools to—

[*English*]

Mr. Adam Chambers: You don't know a number. Is that the testimony? You don't have a number.

[*Translation*]

Hon. Marie-Claude Bibeau: Every time fraud is committed, we counter it and we put all the measures in place so that it won't happen again. Then there are prosecutions. That's where we have zero tolerance.

[*English*]

Mr. Adam Chambers: Okay. Thank you.

With respect to identity fraud, I have just one more question on this matter. Since it was a significant number of instances—a sophisticated operation, no doubt—did you report this to the RCMP? Has it been engaged to potentially consider links to organized crime and maybe an inside individual within the CRA who has potentially been aiding and abetting these kinds of schemes?

Have you engaged the RCMP on the identity fraud cases?

● (1645)

[*Translation*]

Hon. Marie-Claude Bibeau: The 31,000 privacy breaches we are talking about involve a number of groups. That includes a stuffing attack, among other things, but there are also a number of more or less individual cases. Prosecutions are under way, and our internal criminal investigation team is working on the files. There are different levels of investigations going on.

[*English*]

Mr. Adam Chambers: Okay, but your criminal investigations team is not the RCMP, so the question still remains.

Have any of these identity theft cases, especially those with respect to the third party breaches, been referred to the RCMP, or are you asking for help from the RCMP?

[*Translation*]

Hon. Marie-Claude Bibeau: We use the RCMP in some cases, certainly. As I said, over the past five years, there have been 135—

[*English*]

Mr. Adam Chambers: I'm sorry. You said "definitely", so is that a yes, that you've asked the RCMP for help?

[*Translation*]

Hon. Marie-Claude Bibeau: Certainly. There have been 135 convictions in the last five years. Therefore, convictions must invariably come from the police.

[*English*]

Mr. Adam Chambers: With respect to the 31,000 breaches and the issue with H&R Block, have you engaged the support of the RCMP?

[*Translation*]

Hon. Marie-Claude Bibeau: If you're referring to a specific case, I can't answer that.

[*English*]

Mr. Adam Chambers: Okay. We'll put a pin in that. We can follow up with the commissioner in the next hour.

These frauds often result in a debt owing to the government, a debt owing to the taxpayer. With respect to the very sophisticated GST carousel schemes, what's the highest amount the government has written off with respect to the GST carousel schemes?

[*Translation*]

Hon. Marie-Claude Bibeau: Once again, you're trying to lead me to a specific issue. I can't do that.

However, what I can tell you about carousel schemes is that we have put a number of measures in place. I can talk about that.

[*English*]

Mr. Adam Chambers: More generally, what's the single largest amount to a corporate taxpayer that the CRA wrote off last year?

[*Translation*]

Hon. Marie-Claude Bibeau: I can't talk about a specific case.

[*English*]

Mr. Adam Chambers: That's because of section 241. Is that correct?

Hon. Marie-Claude Bibeau: Yes.

Mr. Adam Chambers: Would your position be that your predecessor and the CRA violated section 241 when in 2019 they said that the highest amount they wrote off in 2019 was $133 million? They actually were free to give the highest amount that a corporate taxpayer wrote off.

Minister, do you still want to rely on section 241 privacy?

[*Translation*]

Hon. Marie-Claude Bibeau: I'll turn to the commissioner of revenue to see if—

[*English*]

Mr. Adam Chambers: Is it $100 million? Is it $200 million? Could it be $500 million or maybe $600 million? Like, what amount are we talking about here?

[*Translation*]

Hon. Marie-Claude Bibeau: I have the process in front of me, but I can't give you the amounts.

Do you want to answer, Mr. Hamilton?

[*English*]

Mr. Bob Hamilton: I won't have a number for you either—

Mr. Adam Chambers: I'm sorry. I want to be very clear about this. Section 241 does not allow you to hide behind giving anonymized details. A previous minister in a previous CRA department released a number that said that in 2019, $133 million was written off to one taxpayer. My question is this: What was the highest amount written off in the last year?

Mr. Bob Hamilton: First, I'll just repeat that I won't be able to answer that question, because I don't know. We are very public with our writeoffs in the public accounts. That's where there are some numbers. As much as we can reveal is revealed there.

We can go back and look at those. Maybe I can find the number that you're looking for. We actually have some officials who may—

The Chair: Thank you, Mr. Hamilton and Mr. Chambers.

Mr. Bains, you have five minutes. Go ahead.

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

Thank you to the minister and our officials for joining us today.

Minister, in your opening remarks you talked about the fact that there's an international effort to combat tax fraud. Can you give us some more details about this, please? Are there partnerships internationally that allow you to re-collect funds that would have gone abroad?

[*Translation*]

Hon. Marie-Claude Bibeau: Thank you. Yes, we are involved in a variety of partnerships.

One is the OECD Forum on Tax Administration, chaired by Commissioner Hamilton. The J5 is another such partnership, which we often talk about and which was in Ottawa about a month ago. The J5 brings together both public agencies—our counterparts in the five member countries—and financial institutions. In other words, it brings together both the public and private sectors.

There is also the international tax treaty network, which enables us to share information on specific cases—for example, on multinationals. There are international electronic funds transfers, for which we have information-sharing agreements with about 100 countries. In addition, we of course have a lot of tools that we share here in Canada.

Therefore, we are very active on the international stage to share information and track down tax evaders.

● (1650)

[*English*]

Mr. Parm Bains: Are you able to re-collect the funds that have gone abroad and that are fraudulently lost?

[*Translation*]

Hon. Marie-Claude Bibeau: We already have agreements with certain countries that enable us to share information. I don't have any concrete examples I could use to illustrate how much money we've been able to recover.

Can you add to my answer, Commissioner?

[*English*]

Mr. Bob Hamilton: We would have mechanisms in place not just to share information. If we have a dispute that arises about money that should have been paid in one jurisdiction or another but wasn't, we have methods of trying to resolve it. We work very closely with other countries to have those mutual agreement procedures to resolve disputes.

Mr. Parm Bains: Are we successful in those? Have we successfully recovered funds? Has that happened?

[*Translation*]

Hon. Marie-Claude Bibeau: I have an example in front of me. In the case of the Panama Papers, we were able to recover $83 million.

[*English*]

Mr. Parm Bains: I want to go back to what my colleague across the way was talking about. There are fraudsters pretending to be CRA agents, and it's difficult for CRA agents to ensure they're interacting with the right person. Similarly, it's difficult for taxpayers to ensure they're really in touch with a CRA agent.

What are the best practices that you're recommending to taxpayers with respect to that? Should they always be those initiating the calls by using the number on your website? What is the mechanism in place for that?

[*Translation*]

Hon. Marie-Claude Bibeau: Yes, we have to be very careful when we share information. If a Canada Revenue Agency agent calls you, they will have information to share with you, not information to ask for. When in doubt, when the agency reaches out to you, whether in writing or verbally, you can always end the interaction and call the agency at its general number. In addition, when you receive an email, it contains a code. So, if you call back the agency and provide it with this code, and you're told that the code means nothing, it's because it was fraud. Conversely, if the code is related to our file, it's because it was indeed an email from the agency. So someone from the agency who calls you will give you information, but they won't ask you for it.

[*English*]

Mr. Parm Bains: What happens to taxpayers who are victims of identity theft? Are there measures to support them?

[*Translation*]

Hon. Marie-Claude Bibeau: When identity theft occurs, we work with TransUnion, among others, an agency that is more or less the equivalent of Equifax, which many people know. This makes it possible to track the financial accounts of clients who have experienced identity theft. Again, it depends on the severity of the identity theft. Did the fraudster simply change a piece of information? Did they just change the bank account number to receive benefits, without seeing the taxpayer's other information? In some other cases, the fraudster was able to see everything. It's rarer, but it happens, as well. So the level of support for the customer's protection can vary depending on the severity of the fraud.

[*English*]

The Chair: Thank you, Mr. Bains.

I have a question, Madam Minister. There were 31,468 privacy breaches between March 2020 and December 2023, which directly affected 62,000 Canadian taxpayers. Only 113 of those privacy breaches were reported to the Office of the Privacy Commissioner, yet 31,468 were reported retroactively. Why weren't those numbers known at the time—that only 113 were given to the Privacy Commissioner? Why wasn't he able to access that information?

● (1655)

[*Translation*]

Hon. Marie-Claude Bibeau: It's true that there was some delay, but we disclose that information on a quarterly basis in the Auditor General's reports. In addition, we come to this committee, to the Standing Committee on Finance or the Standing Committee on Public Accounts, and we provide that information.

The reason for the delay in disclosure is that there was an unusual wave of identity theft. In such cases, our priority is to freeze the account in question and to call the individual to verify whether identity theft has in fact occurred. Sometimes, we fear that there has been identity theft, but we realize that the person has actually made a change. So that validation must be done, and that's our priority. However, since the number of identity thefts was unusual, our team was really mobilized to protect people, to follow up and to tighten things up.

Once again, every time a situation involving identity theft occurs, there's a rush to understand what happened and close the loophole.

[*English*]

The Chair: Are you able to break down...? I'm not asking for the information, but I just want to know: Of these 31,000 people who had their privacy affected, do we know who they are, and have they been contacted individually or not?

[*Translation*]

Hon. Marie-Claude Bibeau: Absolutely. The first thing we do is block the account and call the individual.

The Chair: Thank you, Madam Minister.

We will suspend the meeting for a few minutes while we prepare for the second hour of the meeting.

● (1655)

_____(Pause)_____

● (1700)

[*English*]

The Chair: Welcome back, everyone.

The committee is resuming its study of privacy breaches at the Canada Revenue Agency. Our witnesses are here for the second hour.

From the agency, we have Mr. Hamilton, commissioner of the CRA, back with us. We also have Sophie Galarneau, assistant commissioner, public affairs branch, and chief privacy officer; Harry Gill, assistant commissioner, security branch, and agency security officer; Gillian Pranke, assistant commissioner, assessment, benefit and service branch; and Marc Lemieux, assistant commissioner, collections and verification branch.

Commissioner, I want to thank you for holding off on your statement. You have up to five minutes to do it now. Go ahead, sir.

Mr. Bob Hamilton: Thank you, Mr. Chair.

Thank you for the opportunity to continue our discussion. You've introduced people already, and they are people who can answer some of the more detailed questions that we talked about earlier.

I want to say that the protection of taxpayer information remains one of our highest priorities. If you look at our mission in the agency, it's to provide service to Canadians, fairness in the tax system through compliance and protection of information, so we take it very seriously.

In today's increasingly digital world, the rise in fraud and identity theft has become a global trend. We're not the only jurisdiction or the only organization that's facing it. Internationally, responses to these trends include the joint chiefs of global tax enforcement, J5, which the minister mentioned, convening a special working group targeting cybercrime. The agency, representing Canada, is an active member of the J5.

Despite the rigorous security controls already in place, the agency, like any organization, recognizes that it's not immune to these growing trends and acknowledges that privacy breaches and identity theft cause concern among those affected.

The agency does not publicly discuss tax schemes utilized by bad actors, to avoid inspiring other would-be fraudsters to follow suit. Nevertheless, it's important to note that a privacy breach does not necessarily mean that our systems have been compromised or that information has been extracted. In the vast majority of cases that we encounter, fraudsters access data external to the agency, attempting to exploit it by posing as real taxpayers, which we discussed in the earlier session.

That said, the agency has a multi-layered system of defences to identify, protect, detect and respond to threats like fraud, identity theft and tax schemes. We are successful in protecting hundreds of thousands of fraudulent attempts to gain personal and business taxpayer accounts.

To support transparency, we report all material privacy breaches to the Treasury Board of Canada Secretariat and the Office of the Privacy Commissioner of Canada. Admittedly, as we've discussed before, there have been some delays following the pandemic, but we do report them and consider ourselves to be very transparent in that regard.

We also report on privacy breaches at the end of each fiscal year in our “Annual Report to Parliament—The Administration of the Privacy Act”.

● (1705)

[*Translation*]

When fraud is suspected, the agency takes immediate precautionary measures on the taxpayer's account, such as blocking it to prevent transactions, and conducts in-depth reviews with the people involved.

Our identity protection service then takes over. This service is dedicated to both private and corporate clients. We offer an accessible, high-quality service to those affected by identity theft. When identity theft is reported, the agency offers credit protection and monitors the accounts of affected customers to prevent taxpayers from being victimized again.

[*English*]

In rare cases in which fraudulent funds are paid out, the agency takes every available enforcement action to return the funds to the Crown and to hold the offending parties accountable. This includes criminal investigations at our own operation, which could also be referred to the RCMP.

There is no silver bullet to protect against fraud or privacy breaches. That's why we have implemented these multi-layer safeguards, including multifactor authentication as a mandatory measure. This requires persons to enter a one-time password every time they access the agency's log-in services.

The agency also regularly performs security assessments such as vulnerability scanning, penetration testing and security risk assessments of the agency's digital services and systems. We regularly conduct routine checks to identify taxpayer credentials that may have been obtained by unauthorized external parties, and we take immediate steps to revoke these IDs to prevent them from being exploited by fraudsters.

[*Translation*]

In addition, we continually invest in security by enhancing our technologies, processes and controls to ensure the safety of taxpayer information. As fraudsters' tactics evolve, the agency adapts by remaining vigilant in its efforts to stay one step ahead.

[*English*]

Thank you, Mr. Chair.

We would be pleased to answer any questions from the committee.

The Chair: Thank you, Mr. Hamilton.

We will have six-minute rounds, starting with Mr. Chambers for six minutes.

Go ahead.

Mr. Adam Chambers: Thank you, Mr. Chair.

Thank you to the witnesses for appearing at committee.

Mr. Commissioner, you mentioned that there were some delays in reporting the privacy breaches. I'm just trying to get a handle on the decision rights framework within CRA. Whose decision would it have been to not report those breaches in a timely manner?

Mr. Bob Hamilton: I take responsibility for what happens within the CRA. It wasn't a conscious decision in the sense of, “Well, let's not report them.” It was that we had a massive backlog. We were sorting out the process to report these privacy breaches, because we hadn't had that number in the past. We had processes to make sure that we blocked the accounts to prevent the damage and that we informed the people, and then we tried to find out what had gone on. Then, as time went by, we were able to report them.

Mr. Adam Chambers: The minister had no knowledge of this, so you're saying that the decision to not report was not a ministerial decision.

Mr. Bob Hamilton: I'm sorry, but what did you say?

Mr. Adam Chambers: The decision to not report was not a ministerial decision.

Mr. Bob Hamilton: Well, I guess I just take responsibility for it. It was a circumstance that we couldn't...as a result of the workload.

Mr. Adam Chambers: Look, here's the issue. For example, since we're on this issue about decision rights, whose decision was it to reverse the decision on bare trusts? Was it a ministerial decision to reverse that decision, or was it a departmental decision to reverse the requirement to file for bare trust?

Mr. Bob Hamilton: I'm trying to remember exactly how we came to that decision. I have some delegated authorities in that regard, and I discussed it with the minister, for sure.

Mr. Adam Chambers: A former boss of mine said that you can always delegate responsibility but not accountability. It seems to me that there's a bit of murkiness around decision and veto rights, who makes a recommendation and who, ultimately, decides. On one hand, if it's the department deciding on, as an example, bare trusts.... The testimony is that the CRA can decide on its own to not implement a decision by the government or the finance department. It seems to me that there's a bit of unclarity, or it's unclear about who actually is the final authority on some of these questions. We're going to poke a bit more on that later, I hope.

With respect to these privacy breaches, the CRA says that these are a result of external breaches. There was no compromise to the CRA's systems as a result of these 31,000 cases. Is that...?

● (1710)

Mr. Bob Hamilton: Yes, certainly the vast majority of cases arose from external sources. I don't think any of the 31,000 came from ours, but I'll ask my colleagues about that.

To your previous question, I derive my powers from the minister. She can delegate them to me. I'm sure you know how that works.

I don't know, Marc, whether you want to add to that.

Mr. Marc Lemieux (Assistant Commissioner, Collections and Verification Branch, Canada Revenue Agency): For the identity theft cases that we're working on, we've been working on these cases since the summer of 2020, when they actually happened. We've been contacting the taxpayers, making sure that we were talking to the right person, and doing an inquiry to figure out what happened. We took all the actions to—

Mr. Adam Chambers: I'm sorry, but I'm just going to cut in, because it's a fair bit of time. The IRS has some fairly onerous protocols in place that would prevent payments to people who live on "Tomato Street" or what have you. Why is it that we seem to have taken this position? Have we not learned from COVID that the "pay now, audit later" function really hasn't worked out that well for taxpayers?

Mr. Bob Hamilton: I think what you're raising is actually a very good question. I can say, from talking to my colleagues internationally, including in the IRS, that this is an issue that all tax jurisdictions are facing. As we move into a more digital world, we can do things faster. That's good for service, but we also have to make sure that we have proper risk containment measures in place to prevent bad things from happening.

You can't go to one extreme or the other. If we stopped everything and reviewed every transaction, then things would stop, but we also can't let them go through, clearly. I would argue that it's not clear to me that the IRS or anyone else has a better system for trying to strike that balance.

Mr. Adam Chambers: Is there an acceptable level of fraud that you think...? If you pay out—I don't know, insert a number—$100 billion or $60 billion in payments to Canadians, is there a level at which you say, "Do you know what? Speed is important," so if it's 1%, it's not a big deal?

Mr. Bob Hamilton: I don't have a number for that.

Mr. Adam Chambers: Okay.

Mr. Bob Hamilton: In a sense, in concept, what you're saying is correct. You have to be able to risk-manage and think about what is an acceptable level, so that you strike that balance between service and scrutiny.

Mr. Adam Chambers: In my remaining time, I have a few follow-up questions that are reasonably detailed with respect to the memo from before, so we'll ask for that. I'll provide those to the clerk. I hope we can maybe follow up in writing with some specific answers on what we've spoken about today.

Finally, why, in 2019, would the department be totally fine with telling the public about the largest single corporate tax writeoff of $133 million but today, now, try to hide behind section 241 with the largest corporate write-off?

Mr. Bob Hamilton: Yes, and maybe I will turn to my colleague, Marc Lemieux, for that. I don't have a particular memory of 2019.

Mr. Marc Lemieux: I was not there in 2019, so I can't respond to that question, but we had that question this year. We validated, and we can't divulge that information.

The Chair: Maybe you can circle back on that later, Mr. Chambers.

Ms. Khalid, you have six minutes. Go ahead.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair.

Thank you to our officials for being here today. I really appreciate it.

I'll start with something that came up in questioning in the previous round with respect to the Privacy Commissioner and your interaction with the Privacy Commissioner. Obviously, we're dealing with significant amounts of data and many privacy concerns for Canadians. You have over 31 million clients, as you would call them, within the CRA, and 60,000 employees. What is your interaction like with the Privacy Commissioner? How often do you communicate with them, with their office, and what are the concerns that you raise with them?

● (1715)

Mr. Bob Hamilton: I'll start, but maybe my colleague Sophie can elaborate, because she's the one who has the closest relationship with that group.

I would describe our relationship as quite good, just for the reasons you've described. We're a big organization with potential risks, and we're very open with them, notwithstanding the delay that we talked about earlier of the 30,000. Not only do we endeavour to report to them completely and transparently—and we are all caught up on that backlog now—but we have regular interactions, and, in some cases, we will even give them an early heads-up if we see something coming. You'll hear from the Privacy Commissioner, and he may have a different take on it, but I don't think so.

Sophie, I don't know if there's anything you want to highlight.

Ms. Sophie Galarneau (Assistant Commissioner, Public Affairs Branch and Chief Privacy Officer, Canada Revenue Agency): I'll just add that what the commissioner just said is absolutely quite right. We do have a very good collaborative relationship with the Privacy Commissioner, and we're in full respect of regulations and obligations with regard to our reporting obligations.

Within seven days of a material breach being confirmed, we provide those privacy breach reports, and we've been in discussion with them on this 31,000 workload. We were in close discussion with them to determine the best ways to report them after they requested that from us in their February 2024 report. Again, we are now in compliance with that requirement.

Ms. Iqra Khalid: This breach happened multiple years ago. How do you interact on a regular basis? Is it just on an issue-by-issue basis, or do you have a regular framework as to how you communicate and work with the Privacy Commissioner's office?

Ms. Sophie Galarneau: I would say that it is on a case-by-case basis, and it's when it's required. That said, when we do have cases that arise that we think are significant, even before we're able to confirm, we will give them a call to give them an early heads-up. Certainly I've always found that the lines of communication there are well established and productive.

Ms. Iqra Khalid: Thank you. I appreciate it.

Commissioner Hamilton, you mentioned earlier a criminal investigations unit within the CRA. Can you elaborate on that, please?

Mr. Bob Hamilton: The criminal investigations unit would be involved in things like identity theft, potentially, and other fraud cases, but they also investigate tax evasion more generally, so we have our own set of investigators who can take on criminal cases and, as I mentioned, where appropriate, refer them to law enforcement and others. We talked about the Panama papers earlier. That would be the group that gets involved and pushes forward if there's a criminal activity.

Harry, do you want to add anything to that?

Mr. Harry Gill (Assistant Commissioner, Security Branch and Agency Security Officer, Canada Revenue Agency): I would add that our criminal investigations section within the CRA investigates cases of tax fraud, GST fraud and legislation that we enforce. It is our link with the RCMP.

The question came up earlier about the RCMP. Our first step is to refer it to them. At that point, our team does its internal processes and makes the decision as to whether it goes to the RCMP. Those details are closely guarded, for obvious reasons, as you would understand, to not compromise any investigations.

We typically don't get feedback on the civil side of things, which is the side I work on. We wouldn't normally get feedback, even from within our criminal investigations function within the CRA, about the progress of a file if it's been referred to the RCMP and that kind of thing. Those details are quite closely guarded.

Ms. Iqra Khalid: Thank you.

Lastly, I'll ask about reporting and the internal structure within the CRA for reporting and whistle-blowers. Can you elaborate on how that system has evolved over the years and how you feel about that?

What are the measures that have been taken over the years? How can we better improve that system?

Mr. Bob Hamilton: I can't talk so much about how it's evolved over time, but in describing it today, I feel quite comfortable with it, to be honest with you.

We actively communicate with employees that they can raise concerns they have with their manager. We say that's probably the first route to take, but then we have an internal process, as I mentioned earlier, which is anonymous. People can have a safe space to raise concerns if they see something happening that they don't think is appropriate. Finally, there's the overview of the Public Sector Integrity Commissioner. Cases can go to her.

We have had a few that have gone to the Public Sector Integrity Commissioner, but to my memory, not very many reached her. This could say our internal systems are working well, but I wouldn't say that with total confidence.

I feel very comfortable that what we have is an open regime that people understand. Hopefully, they feel comfortable raising internally, in that anonymous framework, anything they see going on that's inappropriate.

● (1720)

The Chair: Thank you, Mr. Hamilton.

[*Translation*]

Mr. Villemure, you have the floor for six minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

Mr. Hamilton, I'd like to dig a little deeper into a subject that was raised a little earlier. In a series of annual reports, the Privacy Commissioner reported only 113 privacy breaches for the years 2020 to 2024. However, in response to questions from CBC/Radio-Canada, we realized that this number was closer to 32,000.

What happened? How much money is involved?

Mr. Bob Hamilton: There are two parts to this question, as I see it.

With regard to the 2023-24 report, unfortunately these cases were reported to us just after the due date. However, we now know about them. That's one of the reasons for the difference, in my opinion, but Ms. Galarneau may want to add something else.

As far as the 31,000 cases are concerned, the amount of fraud is $190 million, if I remember correctly. Someone can correct me if I'm wrong. This amount is cumulative, from 2020 to the end of the period. Unfortunately, because of the process, these amounts continue to rise. That's the story about the 31,000 cases, isn't it, Ms. Galarneau?

Ms. Sophie Galarneau: I'd like to make a small correction. There is no deadline. We were indeed a little late, and we explained why: We were really focusing on protecting accounts, protecting citizens and strengthening our systems. However, we are now up to date with our reports to the Privacy Commissioner and Treasury Board. We have reported on all of these cases.

I would also like to clarify that in relation to the $190 million reported by the Commissioner, the vast majority of the frauds took place in the first year, that is, in 2020, at the time of the pandemic. We're talking about $180 million fraudulently obtained at that time.

Mr. René Villemure: It went badly during the pandemic, didn't it?

According to a CBC/Radio-Canada article, the agency has had to develop a reporting process for these types of privacy breaches since the revelations of recent weeks. I wonder why the CRA hadn't already put this process in place.

Ms. Sophie Galarneau: What I can tell you first is that we've been very transparent with Canadians about the risk. This isn't the first time we've talked about it. We've been educating Canadians for years. We have websites. There are Government of Canada communications initiatives about scams. In one of the websites, we talk about identity theft and inform Canadians about how to protect themselves.

We haven't hidden anything here. There was indeed a delay in reporting, but we are now up to date.

Mr. René Villemure: Is this website widely consulted?

Ms. Sophie Galarneau: I'd have to go back and see how many hits there were, but the website is easy to find. If you type in the word “scam”, you'll find it.

Mr. René Villemure: All right.

Often, in cases like this, we notice that we leave the burden of responsibility on the user rather than the agency. That's what I'm trying to find out with my question. Without accusing anyone, it's easy to say that there are resources, that there is this and that. But sometimes, people just don't know. Literacy on certain subjects, such as digital or financial literacy, may not be high enough. Nevertheless, that doesn't prevent these people from having rights.

Let's get back to whistle-blowers. There's one thing I'd like to know, because I've been interested in this subject for a long time. When a whistle-blower comes forward, it's usually because they haven't been listened to internally, or because they're afraid because the person concerned is their superior. So there's at least some discomfort. You don't raise an alarm for nothing, and I take it for granted that people are generally honest. So I'd like to know what's going on.

The agency's culture seems to favour secrecy. It seems to me that there has been more of an attempt to find out who the whistle-blowers are than to find out who the culprit actually is. When you look at the sequence of events, it seems that the culprit is actually the whistle-blower.

I'd like you to shed some light on this situation.

● (1725)

Mr. Bob Hamilton: There's no culture of secrecy at the agency, in my opinion. However, we are very aware that we have a lot of sensitive information about taxpayers. So it's necessary to take precautions to ensure that this information isn't shared with anyone else working at the agency or outside the agency.

We're in a need-to-know environment, but I think most people at the agency respect the fact that we have to do things the right way.

Mr. René Villemure: I understand that confidentiality is essential. However, I'm not talking about the confidentiality necessary for the agency's operations, but about the lack of transparency with regard to citizens.

Secrecy would be a logical extension of confidentiality, to a certain extent. However, at the Canada Revenue Agency, just as, for that matter, within provincial organizations that deal with revenue, secrecy is quite present.

So would you say that you have a culture of secrecy or a culture of transparency?

Mr. Bob Hamilton: I think it's a mixture of both. Some aspects of our work have to remain secret, because we have to protect information, but we're generally very transparent. We report breaches—

[*English*]

The Chair: Finish up quickly, please.

[*Translation*]

Mr. Bob Hamilton: —and other things. Also, when there's a scam, fraud or conviction, we pass the information on to the public—

[*English*]

The Chair: Thank you.

[*Translation*]

Mr. Bob Hamilton: —because it's a deterrent, and it's good for us.

[*English*]

The Chair: I'm sorry. When I cut you off, we were 30 seconds over. When I ask you to go short, I need you to go short, please, okay? I have to be fair to all the other members, including Mr. Green.

Mr. Green, you have six minutes. Please go ahead.

Mr. Matthew Green: Thank you very much.

I did as I suggested. We'll be taking a bit of a different tone with staff. Obviously, with ministers, it's a bit more adversarial. However, I am keenly interested in the concept of whistle-blowers.

Mr. Hamilton, who in your department is responsible for the Public Servants Disclosure Protection Act?

Mr. Bob Hamilton: That would be the Integrity Commissioner and the act that defines that.

Mr. Matthew Green: I understand that, under the act, every chief executive in the federal public service “must designate a senior officer” and establish an internal disclosure mechanism. Who would that be?

Mr. Bob Hamilton: In our department, it was Nathalie Meilleur, I believe.

Mr. Matthew Green: We understand that there are categories of disclosure. You spoke earlier about loyalty, and I think that when the average taxpayer hears that with all the conspiracies about deep state and all these other things, that might become problematic. I want to take an opportunity to unpack that a bit.

Under what circumstances is it legally allowed for a public sector employee to provide disclosure to the media?

Mr. Bob Hamilton: As public servants, we can all do that. We do have spokespersons for the agency—

Mr. Matthew Green: I'm sorry. If there are staff within the agency who are acting as whistle-blowers—being defined as staff who go public with information, not internally—are there ever instances, in your opinion, when staff from the CRA have the right to disclose to the media publicly in the absence of the internal mechanism?

Mr. Bob Hamilton: I would differentiate two things.

One, sometimes we do speak publicly, not about a problem within the agency but about what's happening, in a factual type of technical briefing. We can have those, but it tends to be controlled, if I can put it that way, so—

Mr. Matthew Green: Mr. Hamilton, I want to be direct, and sometimes I don't ask questions in direct ways, maybe.

In the context of this, we're talking about *The Fifth Estate* investigation where staff—I don't know which level of staff—have disclosed to the media. We're now getting reports that there is an investigation. You suggested, sir, in the previous round of testimony that it could include retaliation up to termination.

I'm asking you, as the commissioner, under what circumstances it would be ethically and legally allowed, under the act, to have protected disclosure.

● (1730)

Mr. Bob Hamilton: I believe the act says you can disclose to the Public Sector Integrity Commissioner, but I am not a lawyer. I don't have the act in front of me. In those circumstances—

Mr. Matthew Green: I'll share with you that, as a labour guy and as the labour critic for our party, looking at the PSDPA, disclosure can be made to the media in cases where there is not sufficient time to follow through on a regular internal process. It can be to the media, but obviously there needs to be a serious breach of law or "an imminent risk of a substantial and specific danger to the life, health and safety of persons, or to the environment." Of course, they would want to get internal union advice on that.

However, the point we're trying to make here is that, from time to time, when there are systems failures that are not about disclosing individual cases or disaggregated information about privacy matters of individual citizens but rather about aggregated cases of systemic failures, would you not agree that there is, in some instances, an ethical rationale for going public?

Mr. Bob Hamilton: I suppose in theory there could be something where you've exhausted all of your opportunities—

Mr. Matthew Green: Okay.

I'll give you one other example in which their disclosure would be protected. I asked you earlier, and I'll let you close with the question that I asked you at the end, which was, to refresh your memory, this: What do you have to say to those people who might be feeling like they're being investigated now for being whistle-blowers to the media and, as you testified, could be facing termination?

I want to put to you that there is another example in which they could be protected, and that is in the instance of a public parliamentary hearing. In theory, I could invite, publicly, all the whistle-blowers to make anonymous submissions to this committee, which, in theory—based on my reading, although I'm not a lawyer and they would probably want to talk to the union—could protect them under the act.

Would you agree that's a possibility here, given the parliamentary privileges extended by Parliament?

Mr. Bob Hamilton: I don't have a particular comment on the parliamentary privilege and what's in or out.

What I would say, and what I would say to our employees, is that if they thought they saw something going wrong in the agency that they wanted to talk about, I would point them to the avenues that we have, which are the three that I've mentioned, and if they were frustrated in that, I would like somebody to come and talk to me.

Mr. Matthew Green: In the event that they don't, what's the consequence?

Mr. Bob Hamilton: In the event that they don't what?

Mr. Matthew Green: In the event that they don't go through the internal process and they go public to the media and they're under investigation, what's the consequence?

Mr. Bob Hamilton: That would depend on what the action was, because it could be relatively minor, or it could be major. It could be disclosing taxpayer information. It could be something like talking about things that we don't—

Mr. Matthew Green: Hypothetically, what would talking to *The Fifth Estate* about major privacy breaches to the tune of 31,000 different files look like in terms of retaliation within the whistle-blower act?

Mr. Bob Hamilton: Again, it's not so much related to it being 31,000 files. What it's really about is this: What was the action that was taken by the employee? How serious a violation of something was that? We would have to look at that.

Mr. Matthew Green: I am out of time, but I did commit to you that I'd give you the opportunity to answer. That was the six minutes that I had.

Thank you.

The Chair: Thank you, Mr. Green.

We will now have a five-minute round.

Mr. Chambers, go ahead.

Mr. Adam Chambers: Thank you, Mr. Chair.

I know my colleague, Mr. Green, is not a lawyer, but he plays a good one on TV sometimes.

Mr. Matthew Green: Thank you.

Mr. Adam Chambers: Mrs. Galarneau, I'm just a little confused about the timeline. Is it that the agency was unaware of the totality of the privacy breaches when you were working through the backlog, or did you know the number and choose not to report it?

Ms. Sophie Galarneau: First of all, I want to say that there was no nefarious intent here to hide any information, nor was there an intention to delay any kind of reporting. I think that's an important piece to put forth.

Mr. Adam Chambers: I understand. The question is, were you aware? It's one thing to not know that there were 31,000, but it's another to be aware that there are 31,000 and not report.

● (1735)

Mr. Bob Hamilton: Maybe Marc could respond.

Mr. Adam Chambers: Mr. Lemieux.

Mr. Marc Lemieux: We were aware that we had thousands of those cases. It was reported in the OAG report. At that time, the report was saying that in July 2022, we had 23,000 of them for $131 million. That was information we gave to the OAG that was in the report.

I came to committee in February, and I said that we were at 26,000 at that time. We were continuing to find those cases. It takes a long time. We have to validate everything. Our intent was to report on those, but our priority was to deal with these. It was never our intention not to disclose those. We had to find a mechanism to do it.

What I can assure you is that we really reported on—

Mr. Adam Chambers: I'm sorry, my time is very limited.

Mr. Marc Lemieux: —all of those that we had.

Mr. Adam Chambers: I understand it's not your intention, but the result was that there was a miscommunication or a lack of communication between the CRA and the Privacy Commissioner. Is that a fair assessment, then?

Mr. Marc Lemieux: I don't know to what extent the Privacy Commissioner was not aware of when those breaches were reported by the OAG.

Mr. Adam Chambers: That's fair. I'd like to move on.

With respect to the fraud, the GST schemes and the carousel schemes, when did the CRA first learn that this was a serious issue—not a date, but what year? Are we going back a couple of years? Is it just the last year? When did these schemes really come on your radar?

Mr. Bob Hamilton: The carousel schemes within the GST have been known in the GST community internationally for a number of years. On the severity of it, I'm not sure when it became—

Mr. Adam Chambers: The question is, in previous years, has the CRA made any recommendations to the finance department to enact legislative changes to help prevent these schemes?

Mr. Bob Hamilton: We do two things—

Ms. Iqra Khalid: I have a point of order, Mr. Chair. I understand that you are very lenient, but I think that the tighter we can keep it, the better it is for this specific issue, and I would question relevance on this question.

The Chair: Thank you for that.

Go ahead.

Mr. Adam Chambers: GST carousel schemes are fraud. We're talking about fraud today. The question is, has the CRA made recommendations for legislative change to help combat these schemes? Have you spoken to the finance department about this?

Mr. Bob Hamilton: I can say that we have had discussions with our finance colleagues about this, because there are things that are done in other jurisdictions, but we also take responsibility ourselves.

Mr. Adam Chambers: There has been no legislative fix for this, though, and we've known about it for multiple years.

Mr. Bob Hamilton: There has not been a legislative change.

Mr. Adam Chambers: Okay.

Mr. Bob Hamilton: What we have been doing is on the administrative side, trying to get in earlier to capture this—

Mr. Adam Chambers: Thank you very much.

In my final minute, I'll go back to these writeoffs that may be a result of fraud. Some of them are a result of fraud. There was a significant increase in the amount of corporate writeoffs, $4.9 billion in one year. You've previously disclosed the amounts. We talked about that today in terms of the largest amounts.

Do you think, as a matter of public interest, that we ought to consider amending section 241 to make public the names of corporations that receive very large tax writeoffs and that owe the Canadian public money?

Mr. Bob Hamilton: I don't have a view that I would express on that. Section 241 is in the law. That's a Ministry of Finance responsibility, but—

Mr. Adam Chambers: That's right, but these writeoffs now are getting to serious levels: 11 corporate taxpayers wrote off over $1 billion. We don't know who those corporations are. As a matter of public interest, now that we're talking about real money, don't you think the public should know who these corporations are?

Mr. Bob Hamilton: Again, I don't really have a comment on that. We do our best to be as transparent as we can with what we have.

If you'd like, in a later questioning, perhaps Marc could outline a bit more about the writeoff process, but we concentrate on having a robust process to try to get debts collected.

The Chair: Okay. Thank you.

Next is Mrs. Shanahan for five minutes.

Go ahead.

Mrs. Brenda Shanahan: Thank you, Chair.

I want to come back to the 31,000 cases and how that number evolved, because I was there at the public accounts committee. I don't remember specifically how everyone testified, but I remember that the real crux of the matter was why we had that sudden huge number of identity fraud cases emerging, obviously out of a very difficult time, COVID, and the fact that there were decisions made around doing a post-verification rather than a pre-verification. That was, of course, to make sure that Canadians had the money they needed to survive the lockdowns that we all needed to have to protect public health.

However, I can understand that put a huge pressure on the system. I know that in my own riding we came across cases where there was clearly identity theft, and bogus bank accounts were opened up. Because we're a small community, the banks were actually pretty good at recognizing the cases, and they froze the accounts. There were constituents who had not applied for COVID but who had COVID money in an account, in their name, and those accounts were frozen.

It was very interesting to see that there was the ability, there was some oversight, where possible, on that. I think the banks are very good at this. They recognize unusual activity in the opening of accounts and the use of accounts and so on, and certainly in any rapid closure of accounts and taking out all of the money.

I just looked, for fun, because we all get notices from the CRA, and someone was concerned that the onus is on the taxpayer to go and check their CRA account. I certainly recommend it to people, and I think as the apps become more user-friendly and so on, it's easier to do. However, just putting in "CRA", I had a bunch of messages from them over the last year and a half, or whatever, that I had new mail that I should take a look at and check to see what it was. I appreciate that kind of service.

Now, maybe someone can give me a hint. Is there anything I should be looking for if it were a bogus message? We have certainly seen that kind of thing, and my constituents are very concerned about texts and so on that they receive that are clearly fraud.

● (1740)

Mr. Marc Lemieux: It's quite possible that some people will call saying that they are the agency. I would say, if you have a doubt, it's better not to divulge any information to those callers. If it happens—because sometimes we have to call taxpayers when we have identity theft—this is one of the exceptions where we would call someone.

If you don't feel good about that, if you have any doubts, don't take the call. Tell the person that you don't believe it's the CRA. If it's the agency, the person will explain to you the steps to validate that they are calling from there. They will give you a number. They will ask you to go on the website to find for yourself the 1-800 number that you should be calling. From there, someone will confirm to you that someone at CRA is trying to call you, and they could put you in contact with that person.

We have an identity protection service in the agency. There is a specific line for those cases. If you call the general inquiry line, when you listen to the message, you can press a number, and they will direct your call to the identity protection services. The wait there is quite short, and people will take care of your call.

If in doubt, call the agency. We are there, and we will be able to see if someone from CRA is really trying to reach you.

Mrs. Brenda Shanahan: Thank you very much for that, Mr. Lemieux. I have instructed my mother that, for anybody who's calling, asking her anything, she is to hang up that phone or not answer. She actually thwarted one of those grandparent schemes by doing that. What a tremendous relief it was.

Mr. Marc Lemieux: I would add that if you don't want to talk to someone from the CRA, they will send you a paper letter.

Mrs. Brenda Shanahan: Thank you very much.

● (1745)

The Chair: Thank you, Ms. Shanahan.

I always love those calls from the local magistrate that say that your tax account has been seized or whatever bullshit they give you.

[*Translation*]

Mr. Villemure, you have the floor for two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair.

I always smile when I hear the Canada Revenue Agency tell me that the waiting time is short.

I'd like to propose a motion of which I gave notice about a week ago.

The Chair: All right.

Mr. René Villemure: The motion reads:

> Whereas on November 6, 2024, the Liberal government announced the closure of the Canadian subsidiary of the social network TikTok, the committee invite to testify:
>
> (a) For two hours, François-Philippe Champagne, Minister of Innovation, Science and Industry;
>
> (b) For one hour each:
>
> (i) David Vigneault, former Director of CSIS; and
>
> (ii) Philippe Dufresne, Privacy Commissioner of Canada;
>
> That the Committee report its observations and conclusions to the House of Commons.

The Chair: Thank you, Mr. Villemure.

The motion is in order and we will discuss it. I would ask the witnesses to remain in their seats for a moment.

Do you have any comments to add, Mr. Villemure?

Mr. René Villemure: Recently, we learned from the newspapers that the Minister of Innovation, Science and Industry had undertaken an investigation into TikTok, a long time ago. The committee has met with TikTok representatives on a number of occasions to ask questions to which we have not received answers. We tried in vain to find out when the investigation would be completed. We now know that it was recently completed.

The minister has issued a press release stating that the government is banning TikTok from Canada. In the same press release, however, it is said that Canadians can continue to use the TikTok application, as this is a matter of personal choice. That's a bit of a paradox, if you ask me.

One important aspect is left completely in the dark in this case: If TikTok is not in Canada, the Privacy Commissioner of Canada will have no power of surveillance or control. He'll still be able to monitor, but he won't be able to do anything.

I think this motion is directly in line with the committee's mission. I would like to see the investigation begin as soon as possible. Thank you.

The Chair: Thank you, Mr. Villemure.

[*English*]

You had your hand up, Frank.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): Mr. Chair, I believe this would be considered a friendly amendment, which is just to add to Mr. Villemure's motion that such would occur prior to our breaking on December 17, 2024.

The Chair: Okay. We'll have to work that out. We'll try to get it in if we can. I don't know if we're going to add that to the motion, because we have a schedule ahead of us.

Go ahead, Ms. Shanahan.

Mrs. Brenda Shanahan: Thank you, Chair.

[*Translation*]

I'll continue in French.

I fully understand the reasons for Mr. Villemure's motion. Of course, a decision of this kind is a big decision.

Personally, I advise all Canadians not to have the TikTok app. I don't understand this kind of business. Everyone knows it's a Chinese company and, frankly, not using it makes a lot of sense. I've just heard of some very creative people who are able to create similar software. Young people love TikTok so much, but it seems to me that we have enough software, platforms and ways of sharing creative content, like dances and all the crazy ideas you can find on this app. It's incredible to see all the information that can unfortunately be collected on Canadians, when we talk so much about confidentiality and privacy.

Mr. Chair, I wonder if we should keep the witnesses here. I imagine you're thinking about that too.

The Chair: I think we can dispose of this motion quickly.

Mrs. Brenda Shanahan: I do have a couple of points. The reason I ask this question is because we're coming to the end of the period that was originally scheduled for the meeting.

In fact, it's contradictory, isn't it? We take great care to keep people's information private and confidential. On the other hand, people are attracted by software, applications where they are asked for personal information. This information isn't necessarily financial, but it is personal, isn't it? We're talking about the person's name, address, phone number, activities and, I imagine, associations they belong to, friends and so on.

I'm the first to say that all these activities should be protected by our—

● (1750)

[*English*]

Mr. Matthew Green: I have a point of order, Mr. Chair. I'm just wondering what the speaking list is because, given the time, I wouldn't want to subject these fine folks, our public servants, to what is likely to be a lengthy debate. I'm just reflecting on the fact that—

The Chair: Are we expecting a lengthy debate on this?

Mr. Matthew Green: No. What is the speaking list?

The Chair: We have roughly until around six o'clock or so. I have Ms. Khalid following Mrs. Shanahan. I actually have a question for Mr. Hamilton that I'd like to ask at the end of it.

Mr. Matthew Green: Okay, that's fair enough. We'll wait until six o'clock.

The Chair: Anyway, that's where we're at.

Go ahead, Mrs. Shanahan.

[*Translation*]

Mrs. Brenda Shanahan: I want to make a point, which is that protecting privacy is very important.

When the announcement was made about TikTok, I had a question about privacy. It said that TikTok, i.e., the Canadian subsidiary of TikTok, was banned from Canada, but that Canadians could continue to use the platform. When I heard this, I thought to myself: Wait a minute, is there a way to protect Canadians from unethical use, fraud or illegal sharing of their information? Indeed there is.

According to the Personal Information Protection and Electronic Documents Act, the authorities and the Privacy Commissioner of Canada have a right of oversight, they have the responsibility to discipline, set things straight or take action against TikTok if there are violations in this regard, regardless of where the equipment is located, the famous servers. Apparently, this equipment is located in places like Singapore and in countries with which we have agreements and good relations. I was reassured to hear that.

The other aspect I wanted to raise is access to classified information. It puts some people here in a difficult situation, because some current and former members of the committee have sat on the National Security and Intelligence Committee of Parliamentarians. I don't think it concerns the members on the other side.

Of course, it's obvious and common knowledge that this decision was made for reasons of national security. National security involves access to classified information, which requires a certain security clearance. The clearance process is very strict. In fact, it's as strict, if not stricter, than at the Canada Revenue Agency: You have to accept the fact that you can't disclose or make public information that's related to national security.

I understand the reasons for the motion. I understand the concerns raised by my colleague, because I had the same concerns, namely whether Canadians and Quebeckers will be protected even if the TikTok subsidiary is closed in Canada. The answer is yes. They are protected.

I may have had another question on another point, but I won't even get into that. Honestly, I don't want to mix things up between committees. It would certainly be more appropriate to ask certain questions related to national security and intelligence elsewhere. So I think I'll stop here. I hope my colleague understands that my comments are well intentioned.

● (1755)

We've already studied TikTok and the other platforms, because we all share the same concern. We're wondering what power the government and police forces have, within a legal framework, to get their hands on a company that operates a platform that abuses Canadians' information. That's my point. Thank you.

[*English*]

The Chair: Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thank you, Chair.

Thank you to Monsieur Villemure for moving this motion.

I'm sure all committee members—well, the permanent ones here, anyway—know how I feel about the issue of social media companies and how they operate with respect to the protection and privacy of Canadians, so in principle I think this is a good study for our government and for parliamentarians to partake in. However, I'm not sure whether this committee is the right place for this, and I'll make two very quick points on that.

The first is on the ICA, the decision that's come out from the Investment Canada Act on this. I think the RCMP commissioner and the minister would be really limited in what they're able to say, given security clearance challenges and the issue of national security and intelligence in general that surrounds this entire issue, as my colleague Brenda Shanahan said, when we're talking about China and the whole reason this company is under investigation in the first place. I would think that the National Security and Intelligence Committee of Parliamentarians would be a better place to house this. There would be more ability for the RCMP and the minister to be open and able to talk with full honesty and, with full paperwork on the table, to say, “This is what needs to happen,” or, “These are the circumstances surrounding the decision.”

The second point I would make on this, Chair, is that I know that Mr. Villemure spoke about PIPEDA and its jurisdiction. Now, I think that TikTok would still be subject to Canadian privacy laws in Canada, regardless of where TikTok operates, as long as there's that touchpoint for Canadians. I'm not sure whether it's accurate that, once they leave the country, they would no longer be under Canadian jurisdiction, because there are a lot of companies that operate in Canada that don't have headquarters in Canada but are still bound by Canadian laws. In this case, I think TikTok would definitely be bound by PIPEDA in the way that it operates in Canada, whether or not its office is located on Canadian soil or not.

Those were the two quick points that I wanted to make.

I realize that we are going a little over time. I want to make a very quick amendment to the motion before we go to a vote. The motion asks for Minister François-Philippe Champagne to appear, and I have no problem with that.

In part (b) of the motion we're asking David Vigneault, the former director of CSIS, and Philippe Dufresne, the Privacy Commissioner, to appear for one hour each. I think that the former director of CSIS does not have a role to play in any of this. I think that it should be the current director of CSIS if we are going to invite them to appear, and that would be Mr. Daniel Rogers. I move the amendment that we replace Mr. David Vigneault, former director of CSIS, with Mr. Daniel Rogers, the current director of CSIS.

● (1800)

The Chair: It's an amendment, if I understand it correctly, to replace David Vigneault with Daniel Rogers. That's it.

Mrs. Brenda Shanahan: She also wants to delete the former—

The Chair: You mentioned Philippe Dufresne in there too, so I just want to make sure—

Ms. Iqra Khalid: I was just reading out the motion.

The Chair: All right.

[*Translation*]

I yield the floor to Mr. Villemure regarding the amendment.

Mr. René Villemure: Mr. Chair, I thank my colleague for her candour and co-operation.

Ms. Khalid, I really like your idea and you make me think that it might be a good idea for us to invite David Vigneault as well as the new director, so that there won't be a gap between the testimonies. In fact, the new director wasn't there at the time the investigation took place, and Mr. Vigneault could provide additional information. For my part, I'm very comfortable inviting the two CSIS directors.

[*English*]

Ms. Iqra Khalid: Is that a subamendment then, Chair?

[*Translation*]

The Chair: Mr. Villemure, Ms. Khalid has proposed an amendment to replace Mr. Vigneault with Mr. Rogers. Would you like your proposal to be a subamendment?

Mr. René Villemure: Yes.

The Chair: All right.

[*English*]

I'm going to accept that as subamendment proposing to invite the two of them.

Ms. Shanahan, go ahead.

[*Translation*]

Mrs. Brenda Shanahan: I would like to know for what reason the former director would be summoned. Sure, people change roles, but that doesn't mean they can disclose everything they did during their tenure. The same regulations, the same laws, the same constraints will apply. Frankly, I find it redundant.

Mr. René Villemure: That's why both should come. They'll be able to complement each other. So there won't be a dead moment in the narrative. That's the reason for the subamendment.

Mrs. Brenda Shanahan: The decision has been made, however, since Mr. Rogers has been in office for some time.

The Chair: I don't know who was or wasn't here during that time.

We are currently discussing the subamendment submitted by Mr. Villemure proposing that we invite both Mr. Vigneault and Mr. Rogers.

[*English*]

I see your hand, Mr. Housefather, and then we'll have Ms. Khalid.

Go ahead on the subamendment.

Mr. Anthony Housefather: Thank you, Mr. Chair.

Mr. Chair, I'd like you to consider ruling the subamendment out of order, because it goes against the core reason for the amendment. The core reason for the amendment is to delete the gentleman's name. You can't have a subamendment that would then add it back. I would ask you, perhaps, Mr. Chair, to reconsider. I don't think it's in order.

The Chair: I'm going to accept it, Mr. Housefather.

I mean, it's up to the committee if they don't want that to occur. They can certainly vote against it if they choose to. I'm going to accept both of them together. I think it's a reasonable proposal that Mr. Villemure has put forward.

Mr. Matthew Green: I have a point of order. Going back to my original point, while it was nice in theory, they said they were going to be quick. Clearly, that's not the case. We have staff, senior level management, sitting here.

● (1805)

The Chair: I appreciate that.

Mr. Matthew Green: What I would propose to you, Mr. Chair, if it is amenable to the witnesses—and this is coming from somebody who lost their round of questions, by the way—is that we be given the opportunity to provide them questions in writing that they could respond to.

The Chair: That's fair enough.

Mr. Matthew Green: This is an unforeseeable future.

The Chair: I'm going to accept that, Mr. Green. I'm going to dismiss the witnesses.

I have a question, Mr. Hamilton, that I will be sending through the clerk on behalf of the committee and that I would like a response to. It's in relation to the CERB fraud. I know that you've done investigations within the CRA. I want an answer as to what other investigations have been done in what other departments. That will be my question for you, sir, when I'm able to do that in writing.

Now, on the subamendment, I have Ms. Khalid.

I have asked for more resources, too.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thanks very much, Chair.

Do you know what? I think I've made my points.

I will just add, with respect to the ICA, in case I didn't clarify for anybody who was listening, that the ICA refers to the Investment Canada Act.

The reason I said it would be a limited study is that it has a certain classification with respect to its clearance level. The ICA is a specific classification of document, and members of Parliament.... I do have my top secret security clearance, but others don't, so I don't think this is something that should be public with respect to any review or any discussion around those documents.

With that, I will stop there, and then, again, I reiterate my points that any current director of CSIS should be able to talk about anything that has happened in its history. I don't think we need to bring in former directors. I think the job would be done with the current director. It just doesn't make sense to bring somebody back.

I'll park my comments there, Chair.

Thank you.

The Chair: We have a subamendment on the floor. I'm going to look for unanimous consent, since I have no other speakers on the subamendment.

Do I have unanimous consent on the subamendment?

On division?

We're going to go to a recorded vote on the subamendment.

I will break the tie by voting in favour.

(Subamendment agreed to: yeas 6; nays 5)

The Chair: The subamendment passes. The amendment now includes Mr. Vigneault and Mr. Rogers.

Do I have consensus on the amendment as amended?

● (1810)

Mrs. Brenda Shanahan: I'd like a recorded vote.

The Chair: Thank you.

Just so we're clear, we're on the amendment, which includes Mr. Vigneault and Mr. Rogers. That's where we're at right now, because that was approved in the subamendment.

If you're voting yes, you're voting for Mr. Rogers and Mr. Vigneault to come. If you're voting no, you're voting against the amendment as amended. Let's get back to the vote.

(Amendment agreed to: yeas 10; nays 0)

The Chair: Now we are on the main motion as amended. I have no speakers, so I'm going to call the vote.

(Motion as amended agreed to: yeas 10; nays 0)

The Chair: I have no other business for the committee. I am going to adjourn the meeting.

Have a great weekend. Thank you, everyone.