HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 081 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, December 4, 2017

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Monday, December 4, 2017

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I call to order the Standing Committee on Access to Information, Privacy and Ethics, 42nd Parliament, first session, meeting number 81.

Pursuant to Standing Order 108(3)(h)(vii), we are holding a briefing with Equifax Canada.

We have John Russo, and....

I really want you to pronounce your name before I try.

Ms. Antonietta Di Napoli (Director, Global Operations, Equifax Canada Co.): It is Antonietta Di Napoli.

The Chair: Ms. Di Napoli, that's a very nice name.

Before we start, I want to say by way of preface that one of my first roles as chair was to visit the Equifax hearings in the United States in which we heard that 145.5 million Americans had had their security breached. At the time, there were citations that the data for as many as 100,000 Canadians had been breached. Recently, your company has released that it's closer to 19,000 Canadians whose information was breached.

It is a concern to Canadians, as it was to Americans, that the breach occurred to 19,000 Canadians. By the end of this committee, we'd like to know that Equifax has fixed the software program problem that was present in the U.S. and that the measures you saw will never happen again. I would just like to open with that.

Go ahead, Mr. Russo.

Mr. John Russo (Chief Privacy Officer and Corporate Secretary, Equifax Canada Co.): Good afternoon, Mr. Chair and members of Parliament. On behalf of Equifax Canada, I would like to thank you for the opportunity to join your committee today. I am here to provide you with current information on the recent cybersecurity incident and to answer your questions as best I can.

My name is John Russo. I am the chief privacy officer and corporate secretary at Equifax Canada. I have proudly worked at this Canadian corporation for the past 10 years. I am based in Toronto, where I have lived my entire life. I take great pride in the services that Equifax Canada offers Canadians from coast to coast to coast, as well as the work that we have undertaken with governments across the country to help strengthen privacy laws for individual Canadians.

I am joined by my colleague, Antonietta Di Napoli, director of global operations at Equifax Canada. While her involvement with the breach activity was limited, she has extensive experience in consumer-facing roles and will be able to provide excellent insight to our consumer practices and procedures.

Today I plan to address three topics. The first one is what happened when our parent company, Equifax U.S., was hacked by criminals and sensitive consumer information was stolen from its servers. Second, I will outline the remediation steps that Equifax Canada has taken to assist impacted Canadians. Third, I will discuss what Equifax Canada is doing today to help ensure this does not happen again, as well as outline what we are doing to empower consumers with greater control over their personal credit information.

However, before I cover any of these three topics, first and foremost I want to offer my sincere apology. On behalf of Equifax Canada and the entire Equifax organization, I apologize to all Canadians whose personal information was compromised. Being a trusted steward of information has long been one of Equifax's core principles, so we were devastated when this happened. I can assure you that in the months and years leading up to this incident, Equifax U.S. did not take data protection lightly. In fact, it has invested aggressively, particularly over the past five years, in security and network resilience. Nevertheless, the cyber-attack and breach occurred and information was stolen by criminals. We accept full responsibility and are accountable for both the incident and the impact it has had on all Canadians.

First and foremost, the question on your mind is, what happened?

We now know that criminals executed a major cyber-attack on our parent company, Equifax U.S. In addition to accessing information on millions of Americans, they were able to access information on approximately 19,000 Canadians. The information accessed included data such as names, addresses, dates of birth, and social insurance and credit card numbers. For your reference, I will provide a brief overview of what happened through a chronology of events.

On Friday, July 29, our parent company's security department in the United States observed suspicious network traffic associated with a U.S. consumer-facing website. In response, the Equifax U.S. security department blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on Saturday, July 30. In response, they took the web application completely off-line that day.

The criminal hack was over, but the work to determine the nature, scope, and more importantly the impact of it was just beginning. It was not known at that time that personal information had been stolen. On August 2, Equifax U.S. engaged an independent cybersecurity firm to investigate the suspicious activity and contacted the FBI.

● (1535)

Over the next several weeks, Equifax U.S. and the cybersecurity firm worked around the clock seeking to identify what had happened.

On September 7, Equifax U.S. issued a news release announcing the cybersecurity incident and referencing that it had identified unauthorized access to limited personal information for certain Canadian consumers. At that time, there were no additional details on the number of impacted Canadians or the specific data that was compromised.

On how we communicated with Canadians, as the chief privacy officer of Equifax Canada, I first found out about the cybersecurity incident and its potential Canadian impact moments before the news release on September 7. I immediately took steps to notify both federal and provincial regulators, and by September 8, I had communicated with the appropriate privacy commissioners, including the Office of the Privacy Commissioner of Canada and consumer reporting regulators across the country.

Equifax Canada also retained Ms. Chantal Bernier, former interim privacy commissioner of Canada, now counsel in the global privacy and cybersecurity group at Dentons. We wanted to meet the highest level of compliance in breach response and transparency with Canadians and regulators alike. While the independent cybersecurity firm worked to complete its investigation and provide Equifax Canada with details of impacted Canadians, we started to implement our plan to notify and assist all impacted Canadians.

We also updated our Canadian consumer website, Equifax.ca, to make it clear to all Canadians where they could go for answers. Additionally, we hired more personnel to staff our Canadian call centre, increased our call centre hours, and established a dedicated breach email address.

Then on September 19, Equifax Canada issued a news release to share the preliminary details we had received about the nature of the impact to Canadians as well as what the investigation had uncovered to date.

On October 2, Equifax U.S. issued a news release with updates, including the fact that approximately 8,000 Canadian consumers were impacted by the breach as well as an additional undetermined number of Canadians whose credit cards were compromised. Later that week, Equifax Canada received the data file containing information on the 8,000 individuals from Equifax U.S., and we reviewed it in order to construct a breach notification mailing list. We started to mail consumer notification letters in both official languages to impacted Canadians on October 13.

The notification letters informed consumers of three key facts: first, that their data had been compromised; second, which specific personal information elements were compromised; and third, it outlined the details on how to activate their free 12-month subscription to Equifax Canada credit monitoring and identity theft protection.

On November 10, Equifax determined that the number of Canadians with compromised credit cards in addition to other personal information was approximately 11,000, bringing the total number of impacted consumers in Canada to approximately 19,000. The additional 11,000 consumers have been notified by mail. Throughout this process, we continued to keep our regulators apprised and updated our Canadian consumer website regularly to include new information.

What are we doing to protect impacted Canadians? Like our parent company in the U.S., Equifax Canada is extending a full range of protection to impacted Canadians free of charge for 12 months. This protection includes daily credit monitoring with alerts informing consumers of key changes to their Equifax credit report. Second, we're offering daily access to their Equifax credit report and score. Third is Internet scanning with alerts, so if we find their SIN or credit card numbers being used on suspicious websites, we can also alert consumers. Fourth, we're offering up to $50,000 of identity theft insurance to assist affected consumers with out-of-pocket expenses.

● (1540)

Impacted consumers received an activation code in their notification letters, which they can use to activate the services online. Alternatively, they can call into our Canadian call centre to receive personal one-on-one assistance.

Here's what we're doing to help ensure this doesn't happen again. As I mentioned earlier, as soon as the intrusion was discovered, our parent company, Equifax Inc, started a forensic investigation regarding the attacker activity. That investigation is now complete, and we understand what occurred and the extent of the intrusion. Equifax Inc. took steps to fix vulnerabilities, and has undertaken multiple other short-term and long-term initiatives to protect the consumer data that has been entrusted to it.

It has undertaken a revisit of its entire IT and data security practice. It is further hardening networks, changing procedures to require confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. It has also engaged industry experts PwC and Mandiant to assist with the global security program, including strategic remediation and transformation initiatives that will help to identify and implement solutions to strengthen our long-term data protection and cybersecurity defences.

Finally, we have committed to working proactively with the entire industry to develop solutions to the growing cybersecurity and data protection challenges we all face. We see this breach as a turning point not just for Equifax but for everyone interested in protecting personal information.

You may have heard Equifax Inc.'s interim CEO share plans to launch a new consumer service that will enable consumers to lock and unlock their credit file at will, free of charge, and for life, through a mobile interface. That product is scheduled to launch in the U.S. in January. We are working to bring similar functionality to Canadians as soon as possible in the new year to ensure that Canadian consumers will have the same control over their credit information as do their American counterparts.

In closing, on behalf of the entire Equifax Canada team, I would again like to express my sincere apologies to all Canadians. While we have taken steps to protect impacted Canadians, we understand that Canadians across the country were upset by the news that Equifax Inc. suffered a cybersecurity breach, which in turn impacted Canadians' personal information. Many Canadians, whether they were personally affected or not, expressed their concerns and fears to me personally, to my organization, to the media, and to elected officials. I share their concerns, as does my organization. We at Equifax Canada are truly committed to doing everything in our power to win back their confidence and trust.

Thank you.

Ms. Di Napoli and I welcome any questions you may have at this time.

● (1545)

The Chair: Thank you, Mr. Russo.

Just for clarity, for the committee's sake, questions can go until approximately 5:15 pm. We have a motion that's going to be brought before committee at the end of that time, and then we have some committee business as well. We can eat into that if we have questions that are still forthcoming, but that's the agenda I would pursue.

First off, for seven minutes, we have Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

At the outset, I would say that Equifax and other agencies similar to Equifax are effectively turning a private profit through providing a public good. The sheer number of Canadians and Americans who have had their data compromised is shocking.

I have a clarification question at the outset. You mentioned 19,000 Canadians. Are those only Canadians living in the United States?

Mr. John Russo: No, those are Canadians residing in Canada.

Mr. Nathaniel Erskine-Smith: Do you have numbers for Canadians living in the United States?

Mr. John Russo: I don't have those numbers at this time.

Mr. Nathaniel Erskine-Smith: Shouldn't you have those numbers?

Mr. John Russo: I'd be happy to provide them to you in writing.

Mr. Nathaniel Erskine-Smith: It's interesting. In preparation for today, one would think you would have provided those numbers, but it would be great for you to provide those numbers in writing.

You provided a timeline for us, but as you well know—and I know because I attended the Equifax hearing before Congress—the timeline is extraordinarily incomplete. You don't mention at all what occurred in March.

Perhaps you could explain to this committee and to the Canadian public that the Department of Homeland Security did provide a warning in March. Perhaps you could provide some information about the steps that Equifax Inc. took to respond to that warning, and whether you think those steps were sufficient.

Mr. John Russo: Sure. The timeline in the U.S. began on March 9. Equifax disseminated the US-CERT notification, as you mentioned, internally by email, requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with our patching policy, the Equifax security department required that patching occur within a 48-hour period of time.

Mr. Nathaniel Erskine-Smith: What was the follow-up with DHS? DHS warned you on March 8 or March 9. I understand that there was an internal request that the software be upgraded, that the patch be run. The security department ran scans that did not find the same vulnerability that DHS found. What was the follow-up with DHS?

Mr. John Russo: On March 15 our security department also ran scans, as you mentioned, that should have identified the systems that were vulnerable to the Apache Struts.

● (1550)

Mr. Nathaniel Erskine-Smith: Subsequent to that, what was the follow-up with DHS? A security agency, perhaps one of the most important security agencies, says to Equifax, "You have a vulnerability that could affect millions of Americans." Your security officials run a program and don't find anything. I'm wondering if there was any communication after that with DHS to say, "We ran this and there are no problems. What did you find that we didn't find?"

Mr. John Russo: I'm here in my capacity as a chief privacy officer in Canada. I wouldn't be privy to those discussions or any of the discussions that were had in relation to that.

Mr. Nathaniel Erskine-Smith: Perhaps you could request that information and follow up in writing to this committee on any follow-up communication with DHS from Equifax's point of view. It occurs to me that if DHS came to my company and said that I have a massive data vulnerability, and I ran my own search and didn't find anything, I would certainly want to be communicating with DHS to let them know I didn't find anything and to ensure that they have followed up on that.

As well, May 13 isn't in your notes, but May 13, as I understand it, is when the hackers first accessed the information. It was between May 13 and the end of July that the hackers had access to the Equifax system. Is that right?

Mr. John Russo: That's correct. It was between May 13 and July 30.

Mr. Nathaniel Erskine-Smith: We have just finished a study on protecting Canadians' personal information. We're in the midst of making recommendations. A number of witnesses who came before us testified to the importance of encryption. It is astounding to me that over 145 million Americans and 19,000 Canadians had their information compromised, that it was that easy to get into a system. The information wasn't encrypted. Perhaps you could explain why there weren't sufficient encryption practices.

Mr. John Russo: The standards we had in place in the U.S. were best-in-class standards. They were recognized industry practice. It wasn't like industry practice wasn't followed. In this case, as a result of human error and IT error, the vulnerability occurred and the hackers got in.

Mr. Nathaniel Erskine-Smith: I expect you don't have an answer to this today, but perhaps you could follow up in writing as well. On a going-forward basis to ensure that something like this never happens again—that was the third point you made before us, and I appreciate that—could you explain to this committee what steps you are taking to strengthen your encryption practices?

Mr. John Russo: Sure. In Canada our information is encrypted and tokenized. We're PCI compliant and we follow the security standards.

Going back to the vulnerabilities that occurred, we're having closed-loop confirmation. In basic terms, we're not only issuing the order to patch but now we're also receiving confirmation, closing that loop that it has been patched.

Mr. Nathaniel Erskine-Smith: It's great to see that you have some measures, including providing for the next 12 months up to $50,000 in insurance for identity theft. There's no guarantee that identity theft happens over that period of 12 months, and Equifax has quite clearly been negligent in this case with people's data. Are you committed to ensuring that all Canadians are made whole as a result of any identity theft that is a consequence of Equifax's negligence?

Mr. John Russo: For the impacted 19,000 or so, we're offering our premier credit monitoring, a product that's been used in other major breaches in Canada, Home Depot being one of them. That's offered free for 12 months for all consumers impacted. For other consumers who are worried or afraid, they can put an alert on their file. They can come to Equifax. We're offering it free of charge.

Mr. Nathaniel Erskine-Smith: For 12 months?

Mr. John Russo: For six years.

Mr. Nathaniel Erskine-Smith: So that insurance of up to $50,000 is available for six years?

Mr. John Russo: That's for people subscribing to the credit monitoring product, which we're offering to the impacted Canadians. All other Canadians—

Mr. Nathaniel Erskine-Smith: No, I'm talking about the impact on Canadians, those who are susceptible to damages as a result of Equifax's negligence. I want to make sure that those Canadians are made whole without having to start a class action or individual small claims suits. That's what I want to make sure of, so I hope today you are able to confirm to this committee that Equifax is guaranteeing that those Canadians will be made whole.

Mr. John Russo: Yes, for the 19,000 Canadians impacted by this incident, they are made whole in terms of the premier product we're offering them. It offers them up to $50,000 in identity theft insurance.

Mr. Nathaniel Erskine-Smith: Is that over a 12-month or a six-year period?

Mr. John Russo: It's over a 12-month period.

Mr. Nathaniel Erskine-Smith: What happens after those 12 months? How are they made whole if identity theft happens after those 12 months?

Mr. John Russo: In terms of the product we're offering, they can continue their subscription to credit monitoring after that.

Mr. Nathaniel Erskine-Smith: They would pay for it.

Mr. John Russo: It's a paid service here in Canada.

Mr. Nathaniel Erskine-Smith: It sounds as though you're not actually guaranteeing that they will be made whole if identity theft happens after 12 months.

Mr. John Russo: The product offers 12 months of credit monitoring and it offers other indicators, such as a lost wallet: if there's information from their wallet that's stolen or lost, we'll monitor that. We'll also give them alerts. Any time anybody accesses their credit file, they'll be alerted to that fact within that 12-month period. The 12-month clock starts ticking when they subscribe to the product. It's not as of the date of the breach or their letter; it's when they subscribe to the product.

● (1555)

Mr. Nathaniel Erskine-Smith: That's my time.

The Chair: Thank you, Mr. Erskine-Smith.

Next up is Mr. Kent, for seven minutes.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair, and thank you both for attending today.

When we attended the congressional hearings in Washington, there were significant comments and statements that in fact your company, and the sector, is seriously under-regulated. In your opening remarks you mentioned that Equifax Canada continued to keep your regulators informed. Who are your regulators? Whom are you responsible to?

Mr. John Russo: The regulators here in Canada are twofold. We have privacy regulators, such as the Office of the Privacy Commissioner, and provincial commissioners, such as in B.C., Alberta, and Quebec, as well as consumer reporting regulators. We're licensed under the consumer reporting acts in the various provinces that have consumer reporting legislation, so we have two sets of regulators.

Hon. Peter Kent: Do you understand from the discussion, certainly in the United States and as it's beginning now in Canada, that there may well be a public mood to create more specific and stringent regulations with regard to private information?

Mr. John Russo: Yes. That's why I mentioned in my opening statement that we're proactively taking steps, such as in the U.S., to reveal this lock and unlock feature, giving consumers more access to their credit information and more access to their personal information, being able to control it more than they ever have. That's a free service offered to all Canadians.

Hon. Peter Kent: Do I understand correctly that Equifax Canada uses the same Apache Struts program and would be required to have applied the same patch?

Mr. John Russo: There are various patches. The global security would cover all of those for the various 24 countries we operate in.

Hon. Peter Kent: We heard in Washington that the original breach was recognized by national security agencies who informed Equifax U.S. Did you get the same warning back in March in Canada?

Mr. John Russo: Do you mean by Equifax Canada?

Hon. Peter Kent: Yes. Was the alert given to Equifax in the United States from the national security agencies immediately passed on to Equifax Canada?

Mr. John Russo: I can get back to you on that answer. I wouldn't have that information.

Hon. Peter Kent: That's where most of the questions exist now: this huge inexplicable period where there was knowledge in the company that a breach had occurred; some inadequate types of remedial action seemingly taken; and then the download of the information of these millions of people.

Mr. John Russo: Just to follow up on your question, it was only on July 29 that we noticed suspicious activity. In the March, April and May timeline, there was no evidence to Equifax that a breach had occurred. There was suspicious activity on July 29 and July 30, and we shut down the U.S. portal.

Hon. Peter Kent: However, there was knowledge, and the warning from the national security agencies, although I don't recall specifically which ones, was that there had been penetration of the system.

The questions in Washington and our questions here today are very similar: why the big delay in the realization that the system had been penetrated and was vulnerable to a breach, which eventually, logically occurred?

Mr. John Russo: Yes. The warnings were to require that the patching occur and it didn't. For that, we're feeling repercussions worldwide.

Hon. Peter Kent: Is there any consideration of a firewall between the Canadian portion of the company and the United States portion, given the problems that obviously developed at head office?

Mr. John Russo: Given our global security and the fact that we operate in 24 different countries, we want to make sure those are consistent. We don't want decentralized systems. We want to make sure that they're centralized, so that we have a consistent policy across the board. You wouldn't want one country to have a belt and another one to have a belt and suspenders.

We want to make sure those efforts...anything that's low vulnerability, we're now raising to medium. Anything that's medium, we're raising to high. We want to go above and beyond the industry standard. Again, this incident was a watershed moment for us and for the industry. We want to make sure it doesn't happen again.

● (1600)

Hon. Peter Kent: Given that the company in the United States lost faith in the former CEO, could the same be said in Canada and in other Equifax national operations? Are there remaining questions about the interim leadership of the company?

Mr. John Russo: I can speak for Canada in terms of...when I found out and when our leadership team found out on the evening of September 7, we took immediate proactive steps to make sure that all Canadian consumers.... That was our number one priority, Mr. Kent, that Canadian consumers were protected and notified. We had to obtain that data from our U.S. parent and that took time. There were over 11,000 files that our forensic experts were combing through and then, later on in the investigation, they narrowed it down to 28 files that contained Canadian data.

The Canadian part of it only came to light late in the investigation. Before the U.S. released that people had been impacted in the U.S., about September 4 or 5, the U.K. and Canadian data portions were identified. All they knew was that there were certain elements. We didn't know the scope. We didn't know what type of data, but once we had that information, the Canadian leadership team took over and were able to lead that charge here in this country.

Hon. Peter Kent: Okay.

We were led to believe from some sources in the United States that the Canadians who were affected had a history in the U.S. credit measuring universe. How did the Canadians get into the American universe? You said earlier that the 8,000...or the 19,000, down from 100,000 originally, are Canadians in Canada who have been exposed. Could the number of Canadians in the United States or who have been in the United States in previous years or decades be much larger?

Mr. John Russo: No. In terms of the U.S. residents, if they had a U.S. social security number, then they would be treated in that 145 million. Those numbers are very small. I don't have those numbers today, but it's not a huge amount.

In terms of—

Hon. Peter Kent: As one of those potentially exposed individuals, who couldn't get into the Equifax U.S. website—I gave up after about two hours. The access rules seem to keep changing, so you can see where that raises great concern.

Mr. John Russo: I appreciate your frustration.

In terms of the 18,000 or 19,000 Canadians, those were any Canadians who had a business to consumer relationship with Equifax. Anybody who purchased something online with Equifax and put in payment card details, since there's some personal information, those were the majority of the 19,000 that were compromised in Canada.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

We'll move to Mr. Weir for seven minutes.

Mr. Erin Weir (Regina—Lewvan, NDP): Thanks very much.

Mr. Kent asked you about the delay between the hacking and Equifax finding out about it. I'd like to ask you about the delay between Equifax finding out about it at the end of July and disclosing it publicly in September.

Mr. John Russo: In terms of the timeline, July 29 and July 30 was when our security team in the U.S. noticed suspicious activity. At that time they didn't know there was a breach; they wouldn't even know there was personal information involved. That was on a U.S. online consumer dispute resolution portal. On August 2, Equifax Inc. contacted King & Spalding, retained them as outside counsel, and King & Spalding engaged Mandiant, a forensic expert, to perform that forensic investigation. As you can appreciate, with the 145 million U.S. citizens impacted, plus a certain number of Canadian and U.K. residents, there was a lot of data to comb through. They had to go back and query everything that the criminals had. Remember that this was a criminal hack. Again, the FBI was involved as well. There were a lot of moving parts, a lot of individuals involved, people working around the clock to get information and get the answers both the American and Canadian public wanted. Given the complexity, the number of files, the data they had to comb through was unstructured so it wasn't as if you were looking into neat files, and given the enormous volume, it took time to work through it.

As I mentioned earlier to Mr. Kent, the Canadian part of it came to light 48 hours before the announcement on September 7. Because the datasets were so enormous, it took time to make sure we did a complete, thorough investigation so we could identify each individual consumer, match them with a correct address so we weren't notifying a previous address, and it took time for the crisis incident response team, given the size of the breach, to be ready to respond to those consumers' questions, fears, concerns, and frustrations.

● (1605)

Mr. Erin Weir: Presumably it would have been possible to disclose a breach before combing through all that information. Was it because of the FBI investigation that you weren't able to make that announcement sooner?

Mr. John Russo: It wasn't because of the FBI. That was one part of it. With these breaches you also see copycat attacks. We knew that if anybody had made that announcement on whatever date it was made, we had to be ready for the copycat attacks and make sure all our systems worldwide were not as vulnerable as they were in March. That took enormous effort, involved everybody from legal, privacy, security, IT, all hands on deck. Again, given the enormity of those impacted, it did take 40 days or so to do that.

Mr. Erin Weir: Okay.

Mr. Erskine-Smith indicated that Equifax essentially sells a public good. Would you accept that characterization, that Equifax is essentially analogous to being a utility?

Mr. John Russo: We facilitate protection for consumers, fraud protection, identity theft protection, and we have products on the market that have been used worldwide in giving consumers some peace of mind and protection of their identity when they want it. Again, we have free products like an alert, where you can put on your credit file to “please contact John Russo at this number before granting credit”. You alert everybody who's accessing your file that you want to be alerted before granting credit. We facilitate consumers in life events. When you apply for a mortgage, a new car, the house of your dreams, people come to us to be able to do that in an efficient and accurate way. Without that credit information, it would slow down the whole economic system in applying for credit. As you can imagine, the banks and the financial institutions want that easily, and they want to make sure it's correct information.

Mr. Erin Weir: But essentially people have to participate in it and have to subject their information to.

Mr. John Russo: You're correct. Consumer consent and permissible purpose are two key elements under the Consumer Reporting Act. Without that, the institution that is trying to access an Equifax credit file could not. You need the consumer's consent, and you have to have one of the allocated permissible purposes under legislation to do so.

Mr. Erin Weir: For sure you need consumer consent, but as you mentioned, credit is required for all sorts of life events that essentially everyone passes through. People don't really have the choice to not participate in the credit system or not provide their information into the network.

Mr. John Russo: The information they're providing is to better serve consumers, so that they're getting the best rates possible and getting credit that allows them to take part in those life events and engage in commercial transactions in Canada.

Mr. Erin Weir: The number of Canadians affected seemed, at least for a while, like a moving target. We talked about 100,000 and 19,000. At one point in time, the number 8,000 was out there. At this point, are we pretty solid on the number of 19,000?

Mr. John Russo: Yes, the investigation is complete, and the number is approximately 19,000. The reason was that the forensic investigation was ongoing at that time, so we put out that number as a preliminary estimate in order to make clear that the magnitude of the breach in Canada was limited in comparison to the U.S. Our forensic experts advised us that it was up to 100,000 that may have been impacted in Canada.

When we went and got the final numbers, there was always that credit card issue, which was that 209,000 credit cardholders were impacted. That number had certain Canadian components to it, which we later identified, so there was the 8,000 plus 11,000 credit cardholders for a total of about 19,000 Canadian residents.

● (1610)

Mr. Erin Weir: Do you have a sense of who hacked Equifax?

Mr. John Russo: We don't have that information at this time.

Mr. Erin Weir: When you say criminals hacked Equifax, do you mean that the hacking itself was the crime?

Mr. John Russo: Yes, I mean with the FBI it's currently a criminal investigation in the U.S., because the act was a criminal act by whoever committed it.

The Chair: Thank you, Mr. Weir.

Next up is Mr. Picard for seven minutes.

[*Translation*]

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

If I understand correctly, you sell your clients identity theft protection services.

Is that right?

[*English*]

Mr. John Russo: We offered identify theft protection to consumers who were impacted.

[*Translation*]

Mr. Michel Picard: Is it a product that Equifax offers to its clients in general, similar to a service or product like insurance, for instance?

[*English*]

Mr. John Russo: Equifax has two types of services. There are commercial and consumer services. This is a consumer service we offer to Canadians, which we sell online for identify theft protection and identify theft insurance. It's called credit monitoring.

[*Translation*]

Mr. Michel Picard: So you sell an identity theft protection service.

For example, if someone by chance takes my identity because of an error with my bank or a transaction I made in a store, will I be protected through you if I'm an Equifax client?

Does the fraudulent transaction through which my identity was stolen have to involve information from the Equifax database?

[*English*]

Mr. John Russo: You don't have to be a victim to use the services we offer. You could buy credit monitoring today if you're a concerned Canadian and want to put those protections in place. We have the credit monitoring service. We have our free credit report.

[*Translation*]

Mr. Michel Picard: That's not the question I'm asking.

If I am an Equifax client, and I pay insurance for identity theft protection and my identity is stolen following a transaction in a store or restaurant, does the Equifax identity theft protection service cover losses incurred because of the fraud?

[*English*]

Mr. John Russo: No. The identity theft insurance would cover you for out-of-pocket expenses. If you have to hire a notary or a lawyer, or if you have to take time off work to rehabilitate your stolen identity, that would be covered in the $50,000 insurance. The losses for the credit card company would arise if your credit card was stolen and somebody went to the restaurant and used your card to pay for a meal. That would be up to the card carriers and issuing banks to cover.

[*Translation*]

Mr. Michel Picard: Have you assessed the financial cost of the piracy Equifax suffered?

[*English*]

Mr. John Russo: Given that our number one priority has been protecting consumers, I wouldn't have figures in terms of what that cost. What I can tell you is that the services we're offering are free to consumers who have been impacted.

[*Translation*]

Mr. Michel Picard: I don't want to know what happens afterwards, but what happens before.

Is there an annual amount at Equifax that generally covers your risk management expectations?

● (1615)

[*English*]

Mr. John Russo: Yes, there are reserves that companies take to help protect against that, as well as insurance, cybersecurity insurance.

[*Translation*]

Mr. Michel Picard: Is it a percentage or a set amount?

[*English*]

Mr. John Russo: It's a percentage. You may have heard from the U.S. testimony that about 12% of our IT budget was spent in terms of cybersecurity protection and security for the IT systems in place.

[*Translation*]

Mr. Michel Picard: What steps do you take to screen the candidates you recruit into your IT department?

[*English*]

Mr. John Russo: I don't work in HR or security, but I could get back to you on that question in writing with regard to our HR procedures and policies. I can tell you that there are background checks that all Equifax employees go through—a thorough background check.

[*Translation*]

Mr. Michel Picard: I would like your company to provide the committee with the recruiting procedures and security measures used for hiring and recruiting IT staff.

[*English*]

The Chair: Okay.

[*Translation*]

Mr. Michel Picard: The allegations that it's a criminal activity come from you, not necessarily from the FBI, because you don't know who made the transaction. Are there any allegations that help could have been provided internally?

[*English*]

Mr. John Russo: Yes, we continue our investigation with both the FBI and local law enforcement.

Mr. Michel Picard: That's not my question. I'm going to switch to English, because they don't get it.

Do you have any information regarding inside help on this hacking?

Mr. John Russo: Do you mean an insider?

Mr. Michel Picard: Yes.

Mr. John Russo: None. In our information, there is no indication that there was—

Mr. Michel Picard: How about the supplier of the technology you use for your database?

Mr. John Russo: There are no facts substantiating that, Mr. Picard.

Mr. Michel Picard: What was the third party able to do that your security department wasn't able to do?

Mr. John Russo: Could you repeat—

Mr. Michel Picard: What was the third party and the FBI...when you referred to an outside third party to investigate—

Mr. John Russo: It was Mandiant.

Mr. Michel Picard: What was their expertise that your security department obviously was not able to accomplish?

Mr. John Russo: In regard to our external forensic.... Mandiant, as well as PwC, were able to recreate the steps, the inquiries, that the criminals had exploited in terms of the hack, and they worked with our internal security department to uncover that information to get a clear picture of what had happened. In terms of remediation, we're working with Mandiant and PwC to come up with remediation steps so that this incident never happens again.

Mr. Michel Picard: Your security department was not in a position to do the investigation itself.

Mr. John Russo: They were in a position, on the guidance of counsel, King & Spalding, to retain an independent forensic expert, outside help, to help better investigate what had transpired.

Mr. Michel Picard: I have a question, but I guess my time is up.

The Chair: You have five seconds. Thank you, Mr. Picard.

Next up is a visitor to our committee, Ms. Boucher.

[*Translation*]

Mrs. Sylvie Boucher (Beauport—Côte-de-Beaupré—Île d'Orléans—Charlevoix, CPC): Good afternoon. I'm very happy to be here.

This is really very interesting, and I will continue along the same lines as my colleagues.

I'm really surprised. We all know that Equifax still has a big impact on our respective credits. Let's talk more about Canada. There has been a breach in the system, and we are told that the files of 8,000 people have been hacked. Are you sure of that number? I think 8,000 people seems very low considering the number of Equifax clients.

Have you made sure that the alleged victims of this hacking have been informed, either by letter or by telephone?

[*English*]

Mr. John Russo: This is a correction. There are 19,000 impacted Canadians, not 8,000. Our core assets, our core consumer credit information, was not impacted nor affected, because it was not hacked. The reason the number is 18,000 to 19,000 is that these were individuals who had purchased a product online with their payment card processing with the U.S. that transaction. Our core commercial and consumer database was not affected at all. No other database outside of that U.S. consumer portal was.

We worked with the Office of the Privacy Commissioner to notify everybody in writing to make sure they were all advised. We didn't want to call or email because that's susceptible to phishing scams and people calling vulnerable people, elderly and youth. It was the best course of action to write to each Canadian. Maybe Antonietta can describe some of the consumer relations aspects to your question.

● (1620)

Ms. Antonietta Di Napoli: Thank you very much for your question.

As Mr. Russo said, we did notify all Canadians via written mail, that being the method of communication that we were suggested to use. Each impacted consumer received a letter. The letter informed them of the actual security breach and what information was impacted.

There were different permutations that were possible. Some consumers may have had their names and their addresses impacted. For some other consumers, it may have been credit card information. Each consumer received the information that was compromised to them in that letter. Along with that was the protection that we were offering them for 12 months, as we specified, and how to activate that service along with how to communicate with Equifax should they have any additional questions.

[*Translation*]

Mrs. Sylvie Boucher: Earlier, you told Mr. Erskine Smith that you were offering one year of compensation.

That doesn't seem like much to me. If it is an indictable offence and the perpetrators wait for a year before committing the same type of fraud, using the information they already have, will you again compensate Canadians who have been victimized?

People have information in their hands. If, after a year, the information that criminals have stolen is used again—criminals don't necessarily think like us—have you planned to help Canadians who are victims of this fraud?

[*English*]

Mr. John Russo: That's the reason we're following our U.S. counterpart in terms of the lock and unlock feature of the credit file that we're rolling out next year for all Canadians in addition to the credit monitoring, where you have alerts and triggers to notify you every time somebody has touched your file. I always say to clients and consumers that it's like a fingerprint. Any time anybody touches your file, they leave a fingerprint. That's the monitoring.

The unlock and lock ability would give the consumer control over who accesses their credit file. Nobody would have access if you turn off that feature, and then, when you go for a loan at the bank, you could turn it back on. You control your personal information as a consumer. That's why we're proactively looking to launch that in Canada in the new year. That affords consumers protections, as well as the alert, as I mentioned, that stays on your file for six years that notifies any credit granter who accesses your credit information that you've been impacted, and you want them to call you at a certain number, perhaps your mobile telephone, before granting credit. Those are all steps that a consumer can take to be vigilant to look out for identity thieves.

The Chair: Thank you, Madam Boucher.

Next up is Ms. Fortier.

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Thank you for taking the time to appear today and answer our questions.

Honestly, this is an issue, as I'm sure we can all appreciate and see in front of us, that affects every Canadian in this country. You mentioned it in your opening remarks. As many of us around this table are also keenly aware, credit scores and credit rates are very confusing and stressful to our constituents, and they rely in large part on services such as yours to get the information that they need. For many in my riding, and especially those who may not have extra funds, this breach was very personal and very troubling.

My concern lies with what happens moving forward. I know you mentioned in your brief and again here that this information was stolen by criminals. I'm wondering how it is you plan on monitoring where this information ultimately ends up. Have you contracted security firms to try to reacquire it or at least locate who may have stolen this information?

● (1625)

Mr. John Russo: Thank you for that question, Ms. Fortier.

In terms of monitoring the dark web, we are monitoring the dark web for any suspicious traffic to ensure that your information is not being traded online. Canadians can be assured that we're looking out for those 19,000 to ensure that their credit card information, their birth date, SIN, are not being traded online so we can alert them to that fact.

The second part of your question, in terms of consumers generally getting educated about Equifax, we look forward to working with you and your constituents in your riding, be it through seminars or Equifax 101. We'd be happy to do this with any constituent riding and any MP. There are simple tips like just checking your credit file. You can do it for free in Canada. You can check your credit file every day if you want to. You can visit Toni's consumer relations and ask questions about your credit file and your credit information, and visit our website at Equifax.ca to get some of that background information. We like to do those Equifax 101 tours, as we call them, with regulators, consumers, consumer advocacy groups across the country so they're informed, so consumers have that information at their fingertips and can make better decisions when they're looking to apply for credit.

Toni works with consumers and she fields those calls pre-breach and post-incident so she can give you a flavour in terms of what consumers are asking for.

Ms. Antonietta Di Napoli: Thank you, John.

Many of our consumers, as Mr. Russo said, are coming to us because they're denied credit, victims of fraud. Most of our conversations with consumers are really around credit education. We explain to them how credit works in Canada, how the credit score works, how to improve your credit, what affects a credit score. Our primary role, really, is consumer education. As John mentioned, Canadians can access their credit file for free, unlimited times throughout the year. There are many ways they can get it. They can visit one of our Equifax offices across the country. We have an automated telephone line that's available 24-7 to consumers. They can send their request in writing, and we'll be able to provide them a copy of their credit file.

As John also mentioned, there's an alert that can be added to their credit file. We encourage the non-impacted Canadians, if they are afraid or concerned about their credit, to take these steps in order to protect themselves.

Mrs. Mona Fortier: Thank you.

Again, with respect to moving forward productively with Canadians and with your former clients, how do you plan to regain their trust? One thing that has repeatedly been raised to me is the time that elapsed, and we've been talking about this, between when you discovered the data breach and when you informed your customers. My other question is, what do you do in cases where there is no valid address or phone number, or a person just doesn't check their mail? How are they informed?

Mr. John Russo: Toni, do you want to take the second part of the question first?

Ms. Antonietta Di Napoli: Absolutely.

Obviously we realized that mailing to consumers may have presented some challenges. We did do lots of scrubbing of the data and that was one factor in some of the delay that caused us to do some of our mailings. We ensured that we had the proper, most current address. We verified the data. As you can imagine, we do have some of this information accessible to us so we were able to cross-reference and do some of that scrubbing of the initial data. There has been some mail returned to us and we are addressing that case by case, verifying if the addresses were incorrect to see if there was a new address with a different source, or possibly contacting creditors of these consumers to see if they have an updated address.

● (1630)

Mr. John Russo: In regard to the first part of your question, Ms. Fortier, in terms of regaining trust, we've met with most of our members, if not all, in terms of answering their questions. We met with the CBA, the Canadian Bankers Association, to ensure that their members were fully informed. We've had meetings face to face. I've been out to many of our clients to work with them, to help mitigate any loss or harm that could be caused to consumers as a result of this incident. One is too many, so we want to make sure that we have processes and procedures in place at Equifax, because security starts with me as an employee. It starts with Toni. Everybody's in security, and we pride ourselves on that here in Canada. As well, our members can take steps at the bank, at the credit card companies, to put flags or alerts on consumers' files to inform them that they were part of this breach.

The Chair: Thank you, Mrs. Fortier.

Next up is Mr. Kent for five minutes.

Hon. Peter Kent: Thank you, Chair.

Just for the benefit of the committee, could you describe the Canadian credit data universe? Besides Equifax Canada, which are the other service companies and what are their relative sizes and comparable annual revenues?

Mr. John Russo: Sure. I can't speak to our competition's, TransUnion Canada's, revenues. There are some smaller credit bureaus, but the two major ones in Canada are Equifax Canada and TransUnion. In the U.S., Mr. Kent, as you are probably aware, there are three: Experian, TransUnion, and Equifax. In terms of the revenues, I don't know about my competition's.... They're posted on their—

Hon. Peter Kent: It's a pretty profitable endeavour, I would think, given that credit agencies, credit providers go to the best source of complete information on any of the individuals they may be dealing with.

Mr. John Russo: Equifax has been around for 118 years. We fulfill a service in the community in terms of allowing people to open up small businesses or apply for their first college or university loan. We help facilitate that, and we are just one small part in that ecosystem.

Hon. Peter Kent: Since word of the breach became public, has the Privacy Commissioner contacted you for explanations, for details, or did you proactively contact the Privacy Commissioner?

Mr. John Russo: As I mentioned in my opening statement, within 24 hours either Ms. Bernier, as our counsel, or I had contacted each of the various privacy commissioners across Canada. The OPC has an open investigation, and we are working diligently with them to answer any and all questions they may have. We have been very co-operative. We run our privacy department in Canada based on the three Cs, communication, co-operation, and common sense, and we pride ourselves on that. We do that with all our partners and all our regulators.

Hon. Peter Kent: Can you provide us with any information about the current status of the two class action lawsuits? One of them, I believe, is for $550 million. I'm not sure what the claim is on the other. I assume you will defend these actions vigorously in court.

Mr. John Russo: Yes, and we have retained counsel to defend Equifax Canada based on the claims of the class action both here and in the United States.

Hon. Peter Kent: At the moment, how long do you think it will take for the two class action suits to run their course?

Mr. John Russo: I can't even opine in terms of the.... I don't know what the backlogs or the courts are like these days. I haven't been in private practice for 10 years now. It's based on court volumes, so I wouldn't even want to fathom a guess on how long it would take to run through the courts.

Hon. Peter Kent: Thanks, Chair.

The Chair: Thank you, Mr. Kent.

Next up, for five minutes, is Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Going back, I would like to understand a bit more what happened in the United States. The Department of Homeland Security in March advised Equifax that there was a potential weakness in the system and that Equifax should install a patch. Is that correct?

● (1635)

Mr. John Russo: Yes, there was a notice in terms of an upgrade to the software. The personnel responsible for that at Equifax, the team responsible for that, did not put the patch. The IT system that was supposed to run and see that the patch was in place did not catch that either, so there was a combination of human error and IT error.

Mr. Frank Baylis: You were advised, but for whatever reasons it was decided or it didn't happen.

Had that patch been put in place, would that have protected this data?

Mr. John Russo: To the best of my knowledge, I wouldn't be here before you today—yes.

Mr. Frank Baylis: The concern I have, and it has been raised by a few of the members here, is what happens on the 13th month after someone's data has been stolen. If someone has stolen a credit card, it's not a big deal. We can replace a credit card. However, I can't change my SIN or my date of birth, and I probably don't want to move just because of this. There are a few things that are hardwired and that are going to be susceptible to being taken advantage of, say, on month 13 or month 14.

If that person is defrauded on month 13 and it costs them $20,000 to get their identity back or to fight the person who has taken it, how much will Equifax reimburse that person?

Mr. John Russo: As I mentioned, the services we're offering, in terms of our industry norms, have been used in other breaches. In terms of working with the regulators, the 12-month period is an acceptable standard that we've seen in the past as we've supported many of those breached clients. Again, there are free services, like monitoring your credit file, where you, the consumer, can look at your credit file information to ensure that nobody has stolen your identity and that nobody has changed your address.

Mr. Frank Baylis: Is that the norm: this happens other places, and the norm is that we protect you for 12 months, and after that you're on your own?

Mr. John Russo: With regard to the cases in Canada and the standards, 12 months is a standard that has been set, yes.

Mr. Frank Baylis: Who sets that standard?

Mr. John Russo: It has been used in other organizations. The courts have opined on it. You saw it with regard to Home Depot in terms of the class action there. It has been an acceptable norm in the industry and in industry practice for many years.

Mr. Frank Baylis: Is that an accepted norm if there is no fault? Let's say Home Depot did everything right, and through no fault of its own someone managed to break in and take its data. However, in this case, it seems to be that there is blame to be put on the shoulders of Equifax. It was informed to do something and chose not to do it, so there is a fault there.

Is that the norm whether there's fault or no fault?

Mr. John Russo: In terms of the actions.... I can't opine in terms of the standard. Each organization's breach and situation is different. We're willing to work with all Canadian consumers who have been impacted. Given the scale of the 19,000 who have been impacted here in this country, with our consumer relations department and our incident response team, we take each individual Canadian independently and work with them to make sure they are confident that their information has not been compromised, that it has not been traded on the dark web.

Mr. Frank Baylis: I have a different type of question. Is there a standard set for security that should be used? We have standards for a number of different things, like electrical outlets. Is there a standard that companies with personal data have to adhere to?

Mr. John Russo: For example, in the credit card space, there are additional safeguards for PCI compliance. We went through that in 2015 at Equifax Canada. That PCI remediation and enrichment process helped in Canada. It encrypted our data. We tokenized our data for credit cards.

Mr. Frank Baylis: Who sets that standard?

Mr. John Russo: The PCI standard policy and procedures organization.

Mr. Frank Baylis: Has Equifax adhered to that standard for credit cards?

Mr. John Russo: For credit card information. Then there are other standards that we're regulated under, such as consumer reporting legislation, for example, which dictates where our information is stored, how it's accessed, and how we update it. There's consumer reporting legislation that dictates how we, as a credit bureau in Canada, operate our business.

● (1640)

Mr. Frank Baylis: Were those standards being met when this breach happened or not?

Mr. John Russo: In Canada, those standards were being met, yes.

Mr. Frank Baylis: But the breach happened in the United States, right? Do the Americans have equivalent standards, and were they being met?

Mr. John Russo: Equifax has standards in terms of when we transfer data: the standards we have here have to be at par, or better, where that information resides. In this situation, the policies and procedures were in place, but as a result of human error and IT error, the incident occurred, and the 19,000 Canadians were impacted.

Mr. Frank Baylis: Thank you.

The Chair: Up next is Mr. Weir for five minutes.

Mr. Erin Weir: I'm struck by the fact that the credit monitoring industry does not seem to be very competitive. You mentioned three major companies in the United States and only two major companies in Canada. I suppose it stands to reason. There is a big cost to setting up a credit monitoring network, and once that infrastructure is in place, it doesn't cost too much more to cover additional individuals or businesses. Perhaps it's a bit of a natural monopoly.

Would you accept that lack of competition as a rationale for greater regulation of credit monitoring than other sectors?

Mr. John Russo: In terms of the industry, who better to serve Canadians in terms of monitoring their information than Equifax? We have every trade, every credit card that reports to us, all our members, the banks, and everybody you bank with. That information, and being able to update and alert you to the fact that somebody has put a fingerprint on your file.... We're in that spot where we have that information and access to that information to help better serve consumers.

Your question is fair. There are not many more industries that would have that amount of data to be able to best serve consumers to fight fraud, and to be able to alert them as to who has touched or accessed their information.

In terms of fraud prevention and awareness, we're well positioned in the industry.

Mr. Erin Weir: I suppose the pitfall of having all that data agglomerated in one place is that it's then potentially vulnerable to being stolen, which is what happened in this case. I wonder if you or your parent company have any estimates of the cost of this breach in terms of what it cost Equifax and what it might cost consumers.

Mr. John Russo: It's in the millions for sure. I wouldn't have an estimate here. Again, the investigation is complete, but on the costs associated with it, as Mr. Kent mentioned, in terms of the litigation and dealing with the security measures we're putting in place, we want to be above and beyond any best practices and industry standard. We're working under our new interim CEO, Paulino Barros, to ensure that security comes first in our organization.

Mr. Erin Weir: Has Equifax set aside a certain amount of money to compensate people whose security was breached?

Mr. John Russo: There are reserves taken in all areas in terms of litigation reserves for each country, based on litigation happening in each of our 24 properties.

Mr. Erin Weir: Okay, but at this point it's pretty difficult to put any sort of overall number on the cost of this episode, either to the company or to its customers.

Mr. John Russo: That's correct, Mr. Weir. We wouldn't have those figures at this time.

Mr. Erin Weir: Okay.

Is it your sense that other credit bureaus are vulnerable to this type of security breach, or is it your sense that they have adequate safeguards in place?

Mr. John Russo: I couldn't speak to our competition and the procedures and practices they have in place. Again, I'm here as chief privacy officer on behalf of Equifax Canada. I know, working with our security department and our senior leadership team here in Canada, what we're doing and what we've done in terms of going from good to better, but I couldn't opine on TransUnion or any other credit bureau here in Canada.

Mr. Erin Weir: Have they ever had any significant breaches, not on this scale but on any kind of significant scale?

Mr. John Russo: Again, I wouldn't be in a position to opine on what's transpired besides what I've read in the media.

Mr. Erin Weir: Okay. In terms of what you've read in the media, do you know about any similar instances at other companies?

● (1645)

Mr. John Russo: In the U.S., there have been similar instances with some of our competitors over the years, with incidents of data breaches and incidents regarding their consumers and personal information.

Mr. Erin Weir: Thank you.

Mr. John Russo: You're welcome. Thank you for your questions.

The Chair: Thank you, Mr. Weir.

We're going to continue with questions from the committee.

Ms. Shanahan, you're up for the next seven minutes.

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

Thank you very much to the witnesses for being here today on an issue which, as somebody who has just heard and read about it, I also was deeply concerned to hear about.

In my former career as a banker, we relied on Equifax—this would have been in the eighties and nineties—for information. In fact, I recall at that time that the problem we had with Equifax was that the data on consumers was inaccurate. We regularly had to check up on it ourselves. We would receive the report on a customer, whether commercial or an individual, and we would follow up ourselves and do the checking. It came out not too long afterwards that consumers themselves were discovering that their records were inaccurate. Indeed—correct me if I'm wrong—there was a court judgment saying that consumers had the right to see their information.

I know that as a banker I was not allowed to provide customers with their information, because it was a service that was sold between Equifax and businesses, including the banks. At that time, it had nothing to do with the consideration of the consumer, which was nowhere to be found in the buying and selling of that information.

Fast-forward to today, and now I see on your website that you're selling consumers their own information. It's information that you are collecting and your business customers are paying you for, and you're selling back to customers the verification of that information for $20 a month. Could you please explain the business model behind this?

Mr. John Russo: Sure.

First, in regard to any inaccuracies or information that's lacking on the file, we welcome questions from consumers across Canada. Toni can speak to our consumer call centres. We want to make sure that information is fair and accurate. That's what our legislation says. That's how we operate our business. It's to be—

Mrs. Brenda Shanahan: In fact, it's because you're selling that information. It has to be accurate. That's your business model. It's up to you to make sure that the information is accurate, not the consumer. If there is suspicious activity on the consumer's account, you should be paying for that investigation. If the consumer wants to know what their credit score is, yes, they should have access to it immediately, for free, and that's what the court judgment in Canada said, that consumers have that access.

I seem to remember it being once a year that consumers had to go in and do it on a paper basis and provide all their information. I know, because I used to provide that education to consumers. It was very onerous and difficult to find the website. I will give you kudos today, because I see that it is actually accessible. You only have to go to the bottom of the Equifax consumer website page to find that access.

However, in terms of consumers having to pay for a restoration specialist to help them recover from ID theft, you should be paying for that if somebody is able to steal their ID.

It's $19.95 per month. I'd like to know what costing went in to discover that this was actually the cost of providing this service to customers. You say they can cancel at any time, but sorry, there are no partial month refunds.

Mr. John Russo: If you're one of the 19,000 Canadians impacted, we are paying for that service. We're affording all Canadians, and we've seen close to 2,000 Canadians, so far, subscribe to the service that we've offered for free to them.

Mrs. Brenda Shanahan: It is for 12 months. Am I correct on that?

Mr. John Russo: Yes, it's for 12 months.

Mrs. Brenda Shanahan: It should be for life, Mr. Russo—for life. Consumers have their social security number and their birthdate for life. They are potentially at risk for life. I would leave that for you to think about.

Do I still have time?

The Chair: You have another three minutes.

Mrs. Brenda Shanahan: Okay, please continue.

Mr. John Russo: I will turn to Ms. Di Napoli to outline some of the access to information we have that consumers generally can get in terms of monitoring their credit and fighting fraud, something as simple as a free credit report.

● (1650)

Ms. Antonietta Di Napoli: As I have mentioned, there are free services that we have. Canadians do have unlimited access to their credit file throughout the year. Mr. Russo mentioned that we are looking at launching functionality where consumers will be able to lock and unlock their files for free. After the 12 months, impacted consumers from this breach will have the possibility to do so, therefore mitigating any fraudulent activity, or possibility of fraudulent activity, on their consumer file.

Mrs. Brenda Shanahan: I'm sorry, I didn't catch that. Does that have to do with the locking and unlocking?

I would like to learn more about that service that you're looking at providing to consumers free of charge. What does that mean, and how will that help people protect themselves?

Mr. John Russo: Similar to our U.S. consumer offering, as you heard from our interim CEO, Paulino Barros, by the end of January, with this service, consumers will have greater control of their information.

For example, if I have a mobile device and I want to lock my credit file, the functionality would be that until I unlock it, a bank, a car leasing company, or a landlord could not access that information. If I'm applying for credit, I can turn it back on at my fingertips, easily, in seconds, so a bank can access and adjudicate me for credit because I'm the individual who wants that credit.

Mrs. Brenda Shanahan: An example of how that would be used is if you lose your wallet. It's not so much that you want to stop your own landlord from accessing it, assuming that you actually want to take out that lease. It's not the people you want to access it that you want to stop from accessing it, it's the people you don't want accessing that account. Therefore, how does it protect?

Mr. John Russo: That functionality would allow you in the future to be at the bank, and at your fingertips, to unlock that functionality. You know that at this one instance you're going to unlock it for the bank to adjudicate you for your car lease or your loan.

At the same time, there are features, as you've heard, in the U.S. where they have a credit freeze, where it's frozen. That's not very consumer friendly in most instances, because to unfreeze it takes time and re-authentication.

What we're building is an easy-to-use service that consumers with an iPhone or a device are able to do instantaneously, within seconds, to allow themselves to be protected. Then at the time they're at the institution seeking credit, they unlock it for that one transaction, and then turn a switch back on to lock it. They'll have that control at their fingertips.

Mrs. Brenda Shanahan: It sounds as though there's some potential there for protecting people, but again, I come back to the integrity of the data. You buy and sell that data; it's for you to protect that data. It's your cost to protect that data. If you need to charge somebody, charge the businesses, the financial institutions, that use that data to then charge 24% on a credit card.

The Chair: Thank you, Ms. Shanahan.

Next up is Mr. Kent.

Hon. Peter Kent: That's a tough act to follow.

Given that the vulnerability of Equifax in the United States wasn't detected by the company, by those responsible for the Apache Struts patch being put into place—it was a national security agency, or an aspect of a national security agency, the United States Computer Emergency Readiness Team—I'm just wondering, given the increasing threats to cybersecurity around the world, whether in fact Equifax Canada would be more comfortable if there were a similar national security agency that monitored its networks, all business networks in Canada, to prevent exactly the sort of problems that evolved during that very significant delay between the original vulnerability being detected and the hacks and the shutting down of the system.

Mr. John Russo: That's an excellent question, Mr. Kent. We're looking at all alternatives with regard to how we can better do our business. Security starts with us as employees, and I can assure you, as our interim CEO said in the Senate hearings, that we will fix this, and whatever the options are in terms of working with this committee or working with others in Parliament to better serve Canadians, we're all for them.

Hon. Peter Kent: My last question is about the interim CEO. Is there any understanding of how long the term of the interim CEO is going to last? Is this because there's headhunting going on for an appropriate replacement, or would you expect that the interim CEO would be responsible throughout the litigation process, which as you indicated earlier, could drag on for some time?

● (1655)

Mr. John Russo: That's at the board level, and I'm not privy to that decision. I can assure you that I've worked with Mr. Barros for the past 10 years. He has been in many capacities, as international president and as president of U.S. business, and he's a man of integrity. His background is in engineering, and when he says he'll fix it, he'll work his darndest to make sure it gets done.

Hon. Peter Kent: Thank you.

Can I concede my time to Sylvie?

The Chair: Go ahead. She already has another seven following.

[*Translation*]

Mrs. Sylvie Boucher: Now?

[*English*]

The Chair: Ms. Boucher, go ahead for seven plus two minutes.

[*Translation*]

Mrs. Sylvie Boucher: I'm replacing one of my colleagues today.

After what I've heard, I would like to ask a few questions.

I am amazed just to what extent Equifax's reputation is being eroded by this breach. With all due respect, I must say that your answers do not enlighten me enough.

I have several questions for you, but there is one in particular that has been on my mind for a while.

In the wake of the Equifax breach in the United States, has Equifax Canada, which protects Canadians on this side of the border, put in place a much greater form of protection against this kind of fraud?

And, as everyone knows, when there is a problem like fraud, for example, or when someone steals their identity, it's also the consumer's reputation that is tarnished. Have you looked at this issue and have you provided for compensation? It took you a long time to discover the breach. Here in Canada, we had a press release in September.

Lastly, did you plan to rectify this type of situation, which could have happened if one of your Canadian consumers had their identity stolen somewhere between the time of the fraud and your reaction?

[*English*]

Mr. John Russo: Thank you very much for those two questions.

In regard to what we're doing here in Canada, as I mentioned, we've retained globally PwC and Mandiant to work with all the Equifax entities. We have 24 companies across the world, and we're working with them.

In terms of the closed-loop confirmation that I mentioned earlier, where we not only issue the order to patch, but we also receive confirmation that it was patched, that's in place. I mentioned in my opening statement that it used to take 48 hours to put such patches in place. That has been decreased to 24 hours or less, in terms of what we're doing globally.

We're also refining any existing industry best practices, procedures, and standards. We want to be above industry best practices. I didn't mention that the chief security officer now reports to our interim CEO, so the corporate governance structure has changed at Equifax in terms of accountability. We're centralizing that security rather than having a decentralized system country by country. We're working with all those individuals. We've appointed a chief transformation officer as well to get some better transparency from a security and IT perspective not only in Canada but also globally, so that this incident won't occur in the U.S., in Canada, in Argentina, or anywhere else we operate.

In regard to your second question, on the reputations of affected consumers, Toni's team works individually case by case with each individual consumer. We have call centre representatives who are able to alleviate any consumer concerns or frustrations in terms of walking them through what has transpired, if anything, with their information. We have protections in place that have been used in incidents a lot larger than ours to afford Canadians protection. Again, our number one priority is the Canadian consumer. I've heard from neighbours, friends, family. This affects everybody's reputation. We have 10,000 employees globally. It affects them as dearly as it does the Canadians who were impacted.

At the same time, we want to ensure that Canadians are afforded the best protections there are in the market, based on the regulatory situations in each country. There's a different regulatory situation in the U.S. from that in Canada. We want to make sure we apply those to each country individually to best represent those individuals.

● (1700)

[*Translation*]

Mrs. Sylvie Boucher: Do I have any time left, Mr. Chair?

[*English*]

The Chair: You have four minutes.

Mrs. Sylvie Boucher: Okay.

[*Translation*]

That's what I'm wondering. The criminals or the people who got this information will not necessarily use it today or tomorrow, but they might use it in 2018, for example. How will Equifax help to ensure that consumer data is 100% protected?

It's all well and good, but wherever consumers go, they're asked to have the Equifax file. We consult Equifax and everything is supposed to be great.

This is what worries me about your answers. I have the impression that you waited to see what the United States was going to do before taking the ball here in Canada. You have put things in place, but what are you going to do now and in the future to protect more and more consumers? How are you going to make sure that consumers' personal data will never be made public?

[*English*]

Mr. John Russo: With regard to the impacted data, our core consumer and credit database, the daily transactions we do with banks, the information we sell to the banks, was not impacted at all here in Canada. Again, the 18,000 was with regard to payment, process, and data that resided in the U.S. where there was a transaction between a consumer and our U.S. merchant.

In terms of the timeline, I just want to clarify the Canadian portion of the records that were impacted came to light on or about September 4 or 5, with all the experts and everybody working around the clock. The Canadian pieces came to light late in the game, in the investigation. When we found out my timeline on the 7th, we notified all the appropriate commissioners. We contacted our clients. We did what we could from a Canadian perspective to best serve those Canadian constituents, and at the time we didn't even know how many there were. We worked with our incident response team and our leadership team in Canada to make sure we got the correct information, that we worked with our teams south of the border to ensure we had all the tools at our fingertips. Once we had that information, we provided the consumers with the protections in place, the monitoring they could subscribe to affording them protection of their identity, and you heard the features of that product.

To ensure this doesn't happen again, just to summarize, we've enhanced our vulnerability scanning, our patch management processes and procedures. We've reduced the scope of sensitive data retained in our back-end databases. We've also increased restrictions and controls for accessing data housed within critical databases. We've deployed additional web application firewalls. The list goes on in working with internal and external experts. It wasn't that we didn't have good systems in place, but we want to be better.

● (1705)

The Chair: Thank you, Ms. Boucher.

Next up is Mr. Weir, and then Mr. Erskine-Smith.

Mr. Erin Weir: The Privacy Commissioner has initiated an investigation into the Equifax breach. I'm wondering if you could speak to that investigation, and how you're working with the Privacy Commissioner.

Mr. John Russo: Our team is working with the commissioner's office, along with our external counsel, Ms. Bernier. We've had regular meetings with them since the initial phone call within the first 24 hours when we were notified on September 7. We've worked with them. We've worked with all the privacy commissioners across Canada. The investigation is ongoing. We're, again, compiling our answers to the questions they had and working to answer them in a fulsome manner so they can complete their investigation in due course. We've been very transparent. Again, accountability and transparency drive our corporation, and we want to make sure we're doing the best for the consumers and the best for all our clients.

Mr. Erin Weir: That's good.

The Chair: Thank you, Mr. Weir.

Next up is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: I have a few small questions.

There was a preliminary report released in relation to the internal investigation. Is there a final report that's public?

Mr. John Russo: In terms of the Mandiant report?

Mr. Nathaniel Erskine-Smith: That's right.

Mr. John Russo: It's a confidential report.

Mr. Nathaniel Erskine-Smith: I see, so even though 145 million Americans and 19,000 Canadians have their data made more public, the investigation of that internally is not going to be made public.

Of the 19,000 Canadians, how many people have opted into the 12-month free subscription?

Mr. John Russo: So far we have about 1,700 Canadians. Toni has an updated number as of this morning.

Mr. Nathaniel Erskine-Smith: Is that the number of Canadians affected who've opted in to the program so far?

Mr. John Russo: The initial mailing, just to set the level, was 8,000. Of those 8,000, over 1,600 people have subscribed to that. The second mailing in regard to the 11,000 went out within the last few days, so we're seeing an uptick in terms of people starting to subscribe to that. It was 22%.

Mr. Nathaniel Erskine-Smith: You've undertaken to provide this committee with the number of Canadians affected in the United States, as well. Will you also provide this committee with information about the number of affected Canadians in the United States who have opted in to this additional protection program as well?

Mr. John Russo: We'll make our best efforts to.

Mr. Nathaniel Erskine-Smith: Thanks.

Are there any reports of identity theft? Has there been any identity theft reported to Equifax either in the United States or in Canada?

Mr. John Russo: To the best of my knowledge, not to my knowledge. Toni can speak to consumer relations.

Ms. Antonietta Di Napoli: I only have information based on Canadian consumers, and we have not had any complaints in regard to identity theft or fraudulent activity from the impacted Canadians who we identified.

Mr. Nathaniel Erskine-Smith: To follow up on a previous question of mine, on March 8 or March 9, DHS notified Equifax in the United States of a data vulnerability, and there was an internal audit run in some fashion by internal security officials. They found nothing, to your knowledge, and you're going to get us information if there has been. There was no follow-up with DHS.

Was there any follow-up from senior officials at Equifax or senior management as to their own security team to say, “So you just did one sweep, didn't find anything, but DHS just said it was a problem,” or was there just radio silence between March 15 and the end of July?

Mr. John Russo: Our former CEO, Rick Smith, was told about the suspicious activity on July 31.

Mr. Nathaniel Erskine-Smith: Right, but if you're in a senior management position, and DHS has told you there was a problem.... You're going to get us information as to whether you followed up with DHS, but was there any internal follow-up after that March 15 sweep, or was that sufficient to satisfy concerns of senior management?

Mr. John Russo: I am here in my capacity as Canadian CPO.

Mr. Nathaniel Erskine-Smith: Fair enough.

Mr. John Russo: I wouldn't have that knowledge. I wouldn't be privy to that information. Sorry.

● (1710)

Mr. Nathaniel Erskine-Smith: It occurs to me, DHS notifies Equifax of a security vulnerability, there is one sweep done, and then.... I should also add that I have information here that says, "Equifax did not take advantage of DHS' Automated Indicator Sharing program that enables the exchange of cyber threat indicators between the private sector and government" and a patch was not adequately installed as it ought to have been.

When you add up all these factors, would you characterize that as negligence on behalf of your parent company?

Mr. John Russo: I would not characterize that as negligence.

Mr. Nathaniel Erskine-Smith: Well, allow me to characterize it as negligence. You have that negligence and where there are damages that might flow to Canadian consumers, ought not Equifax make these Canadians whole and ensure that no Canadian experiences any damages, any loss at their own expense as a result of the negligence of Equifax?

Mr. John Russo: We're taking steps by monitoring the dark web to ensure that this information is not being traded, not being compromised. Again, we're offering the premier product to ensure Canadians have protections in place. We have the call centre available to answer any questions or concerns that Canadians may have. We're taking all the best steps and practices and working in tandem with the OPC with their guidance to make sure that we're doing the best thing for each individual Canadian consumer.

Mr. Nathaniel Erskine-Smith: Can you provide this committee with—in writing, I expect you don't have it today—the detailed steps Equifax is taking to monitor the dark web? I'm not entirely sure what that means.

You mentioned Home Depot as an example, and in response to Mr. Baylis's questions, you said that the 12-month offer of additional services is sort of a standard in relation to these breaches, and you pointed to Home Depot.

You may also be aware, though, of course, that Home Depot settled a class action suit against them in relation to that privacy breach, so you would fully expect, I would assume, to set aside some funds for a class action suit and to make sure Canadians are made whole through that process.

Mr. John Russo: We manage the litigation process with our litigation counsel.

Mr. Nathaniel Erskine-Smith: I ask only because you had said that Home Depot is a good example. Home Depot paid hundreds of thousands of dollars to Canadian consumers as a result of that data breach, and there had been no identity theft there either.

This committee is considering recommending giving the Privacy Commissioner new powers, including the power to levy fines where companies have failed to protect privacy adequately.

What do you think of that potential recommendation?

Mr. John Russo: Actually, we've worked with the former department of industry Canada and with the Canadian Marketing Association and other associations in regard to those regulations and guidance. We've worked with the OPC in terms of better protecting consumers, giving consumers control of that information.

Mr. Nathaniel Erskine-Smith: In relation to that ability to levy fines, we're considering new powers for the Privacy Commissioner. The U.K. information commissioner, as an example, has the ability to levy fines, and has done so in a case against Sony.

In this case, with Equifax having not acted appropriately and adequately, I would say, in protecting Canadians' privacy, there would be the potential, presumably, to levy fines if the OPC had such powers.

Would you support the OPC having such powers to levy fines?

Mr. John Russo: We're open to working with government on all new guidance and all new regulations.

Mr. Nathaniel Erskine-Smith: All right.

Thanks very much.

Mr. John Russo: You're welcome.

The Chair: Thank you, Mr. Erskine-Smith.

I have a few questions of my own.

As one of the members who travelled to Washington, I have a question. We know that the Privacy Commissioner oversees the data once it has been breached. The Privacy Commissioner gets involved.

Which Canadian equivalent oversees the data traffic? The U.S. Department of Homeland Security does so, and Mr. Erskine-Smith has referred to this many times. What is the Canadian equivalent? Who oversees the data and possible breaches for Equifax Canada?

Mr. John Russo: From a security standpoint?

The Chair: Yes.

Mr. John Russo: Do you mean law enforcement?

The Chair: Yes.

● (1715)

Mr. John Russo: We've been working with the RCMP and the FBI globally in regard to this incident, answering any questions they may have. The majority of the impacted individuals were Americans. In terms of the 19,000 Canadians, we've been answering any and all questions from the RCMP and other law enforcement.

The Chair: It goes along with what different members have said, that for the 145.5 million Americans and 19,000 Canadians, the data has apparently not been used yet, but the concern is that there's this big bomb that's about to go off and what others are going to use the data for. We've heard that Canadians have not been affected by this that you've seen. Have you heard of any issues in the U.S. that have arisen from the use of the data of those 145.5 million people? Has it been used yet, and if so, what has it been used for?

Mr. John Russo: To the best of my knowledge, I have not heard of any cases. Maybe Ms. Di Napoli has heard something in regard to her conversations with U.S. operations and consumer relations. At my office, however, as chief privacy officer for Equifax Canada, I have not had a reported case in which somebody has claimed, as a result of this incident, as a result of being impacted and mailed to in regard to the 19,000, that they've been impacted negatively and had their identity stolen.

Ms. Antonietta Di Napoli: Much like Mr. Russo, I have not heard of any instances where the impacted Americans or Canadians were impacted by any fraudulent activity or identity theft.

The Chair: I have one last question.

What were your revenues for Equifax Canada for 2016?

Mr. John Russo: I think the revenues were approximately $250 million for Equifax Canada.

The Chair: It kind of goes along with the question that has been asked here.

Someone's stolen identity can be life changing. We know that. I think that if I asked you for an estimate of what it would cost any individual in particular if their data were breached, again, it could be life changing. They might not be able to buy a house. They might not be able to buy a car for many years. As a result, many traumatic events could happen in their lives.

I would suggest that $50,000 is a little light on providing Canadians with the reassurance that you're going to take care of any breach. Again, as Ms. Shanahan said, you're responsible for this data. You're responsible for taking care of this data. I think you should be, at the very least, recovering all costs, if not extras, as a result of this particular data breach, which we all know, as Mr. Erskine-Smith has referred to, was your own fault. You've admitted to it. You've apologized for that.

As a committee, our time is done. I would challenge you to do the right thing and to make sure that Canadians are made whole again if they are affected by this. The concern is that we're not sure when this is going to affect Canadians, but let us hope Equifax will step up to the plate.

Thank you for appearing today and hearing some tough questions, Ms. Di Napoli and Mr. Russo.

Mr. John Russo: Thank you, Mr. Chair and committee.

Ms. Antonietta Di Napoli: Thank you.

The Chair: We're going to suspend for five minutes and then we have some committee business to do.

● (1715)

(Pause)

● (1720)

The Chair: We'll bring the meeting back to order.

We have a motion from Mr. Erskine-Smith before us that most of you have seen.

Mr. Nathaniel Erskine-Smith: I expect that you all have the motion before you. It's fairly straightforward.

The nominee for the office of the Commissioner of Lobbying of Canada was tabled last Thursday in the House, I think. The idea is to bring Ms. Bélanger before us for an hour to question her and go from there.

Hon. Peter Kent: We had passing contact with her in her current capacity a few weeks ago. I think it's very worthy and I understand she may well be available.

Mr. Nathaniel Erskine-Smith: That's my expectation.

The Chair: Just for the record, is she available? I believe she is.

The Clerk of the Committee (Mr. Hugues La Rue): Yes. I've reached out to her and she is available on Wednesday.

The Chair: Okay. Is there any further debate?

I'm going to move to the vote.

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

The Chair: Now we'll go in camera.

[*Proceedings continue in camera*]