HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 024 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, May 27, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 27, 2014

● (1105)

[*English*]

The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)): Good morning, ladies and gentlemen.

We'll convene our meeting of the Standing Committee on Access to Information, Privacy and Ethics. We're here today to continue with our ongoing study on the growing problem of identity theft and its economic impact.

Today we're pleased to welcome a panel of three authorities in the field. Representing credit bureaus and agencies, we have Equifax Canada Company. Mr. John Russo, I believe, will be presenting on your behalf and you can introduce your colleagues when you get the opportunity.

We have, from the Forrest Green Group of Companies, Mr. Murray Rowe, president. Welcome, Mr. Rowe.

We also have, from TransUnion Canada, Todd Skinner, president, and he is accompanied as well.

What we usually do is invite witnesses to make brief presentations of five to 10 minutes each, in your case, and then we'll open it to questions to all three after the three presentations are made. In the order in which they appear, I think we'll invite Equifax Canada to begin. Mr. Russo, I understand, will make the presentation.

The floor is yours, sir.

Mr. John Russo (Vice-President, Legal Counsel and Chief Privacy Officer, Equifax Canada Co.): Thank you, Mr. Chair. Good morning, committee members.

My name is John Russo. I am vice-president, legal counsel, and chief privacy officer for Equifax Canada. To my left is our Canadian president, Ms. Carol Gray, and to my right is Ms. Tara Zecevic, vice-president of decision solutions and fraud.

We would like to start by thanking the committee for the opportunity to speak in support of your study of the growing problem of identity theft and its economic impact. We'd also like to congratulate the government for taking such a positive and proactive step to help stem the growth of identity-related crimes in Canada. Canadians truly benefit from coordinated strategies that involve government, law enforcement, industry, and consumers, and this committee is an excellent example of that. Our approach to identity theft is not about individuals stealing from others. It's about broader, deeper ways of taking advantage of a vulnerable system, which are organized, focused, and definitely global in nature.

Think about that for a moment. Think about the ramifications.

With that in mind, we have three key thoughts we'd like to address before the committee.

First, with the rising number of data breaches, the increased use of electronic delivery channels and networks, and the influence of social media in our society, at Equifax we have seen identity-related crimes increasing steadily since 1998. In fact, the number of Canadian identity theft victims increased 14% in 2013, according to the Canadian Anti-Fraud Centre. Another pertinent example we'd like to highlight today is that we estimate today that synthetic or fictitious identity fraud schemes cost Canadians potentially $1 billion a year in losses. They are real numbers based on carefully calculated cost analysis.

Second, we would like to address the types of identity theft—real and synthetic—impacting both businesses and consumers. Finally, we'd like to point out why Canadian consumers and business should be concerned, and what steps they can take to prevent future financial losses and other hardships associated with identity theft.

Before an identity-related crime can be perpetrated, the theft of personal information needs to occur to set up and prepare for the crime. At Equifax we have noticed a substantial increase in the amount of personal information lost by or stolen from a variety of sources, such as rogue or careless employees and other unauthorized access at various institutions ranging from retailers, health care providers, financial institutions, and even, unfortunately, government. Also, keep in mind the increased identity thefts stemming from data breaches. For example, at our bureau, over the past 18 months, we have protected more than 1.5 million Canadian credit files with credit alerts or credit monitoring as a direct result of data breaches, and these numbers are steadily on the rise.

Recent statistics prove that the bulk of these threats to personal information are through malicious or criminal attacks on an organization's database. Data breaches are truly becoming a treasure trove for fraudsters. Key findings published in a recent Ponemon Institute study include the following. Forty-two per cent of incidents involved a malicious or criminal attack. Similarly, data breaches due to malicious attacks cost companies in North America approximately $246 per compromised record, significantly above the mean of $200. Finally, more consumers terminated their relationship with the company that had the breach; the average abnormal churn rate increased by 15% between 2013 and 2014.

When it comes to ID theft prevention, Canadian businesses have taken a number of steps to mitigate the effects of the crime, but the electronic transfer of personal information is critical when processing financial transactions, and there are only so many steps industry can take. Indeed, thousands of personal credit reports are electronically transmitted every day, which are acquired, secured, and used lawfully by our members. Furthermore, thousands of credit applications are also processed daily ranging from bank loans to car financing.

Yet, there have been numerous cases where rogue employees, or “foot soldiers” as we call them, will take credit application information from their place of employment, and much like any trafficker, sell the personal information on those applications to organized crime.

In many of those ID theft investigations, police services report that stolen personal information is frequently found during traffic stops and other lawful searches. Simply put, there is little to no legitimate reason for anyone to possess piles of consumer credit applications, financial information, or other identity-related documentation.

I'd like to provide a little more information on identity theft statistics and trends in Canada. Since 1998, Equifax has been documenting the exponential growth in identity-related crimes. Between 1998 and 2003, Canada experienced a 500% growth in identity theft reports, where applications were submitted and damage was incurred to a legitimate Canadian consumer. From 2004 to 2005, the growth rate levelled. In 2008, the numbers climbed back up to the highs of 2003 and fictitious, also known as synthetic, identity crimes started to blossom.

What are synthetic identity crimes? Synthetic, or fictitious, identity crime occurs when information is either stolen—where components of that information are used to create a non-existent person—or information about an identity is simply made up. The perpetrator often does this by taking the personal information, such as a SIN, of someone who is deceased or not yet part of the credit granting system, like a child, to build a non-existent identity. The perpetrator then monitors progress of the fictitious identity, by pulling credit reports and conducting hundreds of thousands of dollars in financial transactions, before abandoning the identity of the synthetic person they originally created and disappearing without a trace. More concerning is the fact that we commonly see tens, or even hundreds, of fictitious identities operated by the same group at the same time. Organized crime plays a big role in this, with the proceeds of these crimes being used to finance a wider range of other global activities, possibly even terrorism.

Recently, l participated in a CBC investigative report on synthetic identity, following Project Mouse by the Toronto Police Service. To some, this may seem like a faceless, victimless crime, but the consequences are chilling. Fake names on real credit cards, real driver licences, and real passports pose a real threat to national, if not our global security. I encourage you to watch this report by Rick MacInnes-Rae on CBC's *The National*.

Without question, fictitious identity creation is on the rise, and tens of millions of dollars are being siphoned by organized criminals each year. Correspondingly, Equifax sees, on average, 1,300 fictitious consumer files being created monthly from across the country by fraudsters and other organized criminals. The fact of the matter is that criminals will not stop evolving, and our laws, our security, and our prevention tactics must change with them. Thieves are stealing real IDs or building upon fictitious identities as we speak, and this problem isn't going away without a confluence of legislation, law enforcement, and solutions from organizations like Equifax. It's what we estimate to be a multi-billion dollar business in Canada.

The financial services and credit industries continue to do their part for victims of identity-related crimes by investing millions of dollars each year to detect identity fraud as quickly as possible. Identity-related crimes have grown to a level that affects all Canadians, either directly or indirectly. Unlike 15 years ago, I am hard-pressed to find a person today who hasn't been a victim of an identity crime, had a debit or credit card skimmed, worked with an employee who was terminated for dishonest behaviour, or had credit or other applications submitted using that person's identity. I'm sure many of them are your constituents.

Finally, combatting identity-related crime is a battle that transcends politics. It starts with education and awareness from each individual consumer and every household in Canada, especially, in light of recent data breach incidents, where it is not only individuals losing information, but corporations being hacked or maliciously attacked for your sensitive information; your confidential and personal information.

Hacktivism is on the rise. According to a recent study by ABI Research, hacktivism now represents 47% of all activity around various cyber-threat groups. These hacktivist activities may not seem connected on the surface, but the release of any personal information that can later be used to gather a synthetic or real identity has a real impact on consumers. The term “data breach” has become a household term.

● (1110)

A recent North American study by Javelin Strategy and Research reports that one in every three consumers affected by a breach becomes a true victim of identity theft. This is up from nearly one in four, in 2012. Consumers and businesses should be concerned.

What steps can they take to prevent or at least detect theft and mitigate future damages?

First off, we advise consumers to check their credit file at least once every quarter to spot any abnormalities or possible fraud on their file. Our consumer slogan at Equifax is “check to protect”. You can do so for free, 365 days per year, at any one of the Canadian credit bureaus.

Second, if you are a victim of a data breach incident, ask the organization, at their expense, of course, to provide you with credit monitoring services for at least the next 12 months. From our experience, 12 months is the time period that most identity theft crimes are committed.

Finally, be vigilant on what information you are providing to institutions. Do they really need your SIN or date of birth to conduct a simple retail or rental transaction?

Mr. Chair and committee members, on behalf of Equifax, we commend you for helping to address the growing problem of identity-related crimes in Canada, and for inviting us to speak on these very timely and critical issues.

Thank you.

● (1115)

The Chair: Thank you, Mr. Russo.

That is a very chilling, sobering report. This is exactly why we've convened this study, because of issues just like this.

Next on the list of witnesses, we welcome the Forrest Green Group of Companies, Mr. Murray Rowe, president.

Mr. Murray Rowe, Jr. (President, Forrest Green Group of Companies): Mr. Chair and members of the committee, thank you for having us,

I'd also like to recognize my associate, Bob Groves, who may advise me as we progress here, depending on your questions. I'd like to take a little different approach here today as both my colleagues at Equifax and TransUnion will focus on the macro level. I'd like to focus on a group that I think are particularly vulnerable and that would be first nations communities.

I'll give you a little background on Forrest Green. We're well versed in supporting public sector organizations. We have secret clearance. We've worked with the Assembly of First Nations and with AANDC.

Our position is that first nations communities are one of the most vulnerable to fraud and financial abuse. We submit that a lack of credit bureau data means they're more susceptible to fraud. In many cases, they don't understand the concept of how credit bureaus function. They rarely check their credit reports, and as a result, individuals I've spoken with are keenly monitored; they get a call from a collection agency....

A member of Parliament called me on Friday indicating they believed they were a victim of identity theft. They knew almost immediately because of the processes that take place. Individuals on reserve are difficult to find, and they rarely reach out and connect with credit bureaus.

On the next page I've provided some insight into a format. It's not a real credit report, and I would submit we were extremely generous when we indicated that less than 5% of first nations have viewed their personal credit report. I would submit that it's closer to 1%. Out of curiosity, can anyone on the committee who has viewed their credit report in the last year put up their hand? Okay, that's impressive. We see that close to half the members here have not viewed it, so imagine remote communities. I think they're particularly vulnerable in that regard.

We implement solutions for online authentication and we work with police services. The next page shows a screen print from the Hamilton Police Service. To avoid having to come in and show photo ID, we have a solution whereby we leverage credit bureau data to authenticate a person, so it's an anti-fraud solution. What's interesting is that when we're dealing with aboriginal communities in remote areas, many of them are low income and the challenge is that the people in remote communities should be the ones who are provided access to online services so they don't have to fly in or drive hundreds of kilometres to show photo ID. Ironically, because they don't have credit bureaus they are the ones who are forced to do these kinds of activities. I think it's important we understand that the ramifications of leveraging credit bureau data are quite profound.

The issue of identity verification is also interesting in the sense that when people are applying for low-wage jobs particularly, credit bureau data is often also used in employment searches and analytics. There's a certain irony that the people who are most vulnerable and who most require access to jobs could be discriminated against because they have poor credit ratings. I realize that's somewhat tangential, but I think there are some interesting relationships with lack of data or poor data, fraud, identity theft, and vulnerability.

I wanted to make some interesting references here to the Standing Committee on Aboriginal Affairs and Northern Development. I think when you look at some of the statistics below, it demonstrates a propensity for aboriginal communities not to trust organizations that gather data; 80% of family allotments are done outside the Indian Act, and 50% of band leasing is unregistered. This demonstrates that aboriginal communities do not trust or have not bought into the concept of sharing data.

I think if there was one theme we could have when we finish this dialogue, it would be that education needs to play a key role in what we're going to do to solve this. We need to talk and we can't just rely on leaders today. They haven't been educated. They can't tell their children how to formulate a good credit report because no one's told them, no one's educated them.

● (1120)

The last page is just further evidence supporting access to information and the challenges of not having identities, not having photo ID, not having credit bureau data. Not only does it lead to fraud, there was an interesting, a sad story, quite frankly, of a lady who had received a settlement for residential schools, had difficulty opening a bank account, cashed the cheque, brought the money home, and was robbed and murdered on reserve.

I think this demonstrates there is a vulnerability of these people, and we need to start examining some of the root causes. I don't think we should forget on this fraud issue that with a lack of documentation—this is my humble opinion—I think they are more vulnerable to fraud than people who can catch it within a week, as many Canadians do. Now, my colleagues here may debate that, in fact, it's much more rampant and difficult, but the people I know who are experiencing fraud are reacting very quickly.

Thank you very much for your time.

The Chair: Thank you, Mr. Rowe, for introducing that very important aspect to our study. I'm sure there will be questions about it later.

We go now to TransUnion Canada, Mr. Todd Skinner, president.

Mr. Todd Skinner (President, TransUnion Canada): Mr. Chair and committee, thank you very much for having us attend today. My associate with me is Chantal Banfield, our legal counsel for TransUnion Canada.

A little about TransUnion, and then we'll talk about the issue of identity theft.

TransUnion, as a global leader in credit and information management, creates advantages for millions of people around the world by gathering, analyzing, and delivering information. For businesses, TransUnion helps improve efficiency, manage risk, reduce costs, and increase revenue by delivering comprehensive data and advanced analytics for decisioning. For consumers, we provide tools, resources, and education to help manage their credit health and achieve their financial goals. Through these offers, TransUnion is working to build a stronger economy worldwide, based in Toronto, with our global headquarters in Chicago.

TransUnion is regulated by consumer and privacy legislation. Our core business is consent based, and one needs to consent to obtain a credit file. We screen and audit process our members for prospective members and legitimate businesses. We process millions of pieces of data a month and update our database on a regular basis. We recognize the importance of safeguarding information, and we are pleased to announce we were the pioneers of fraud alerts in the early 1990s.

When you define the issue of ID theft, it really falls into three categories: a data breach or a compromise, the actual potential ID theft that happens as a result of that, and the fraud that occurs after that. Compromises or data breaches are when a hard drive is stolen, such as the student loan portfolio or theft that occurred at Revenue Canada.

We're aware of these compromises through consumers and through companies. One of the problems is that companies do not always report their compromises as recommended by the federal Privacy Commissioner in "Key Steps for Organizations in Responding to Privacy Breaches".

When you look at the statistics as reported to TransUnion, there are a couple that stand out. The actual number of reported compromises in the last five years has decreased by 30%. What's alarming about that is the number of potential victims actually increased by 600%. Most would assume these data breaches happen at financial institutions, but contrary to that, that is not the case. The number of reported compromises is actually only 8% from financial institutions; 70% of the number of compromises come from the medical, service, or retail industry. If you look at other industries—government, insurance, and finance companies—the numbers are very small.

What are the implications? The implications are that the financial sector is acutely aware of the safeguarding obligations they have to their constituents. When these losses happen through breaches at financial sectors, they typically bear those costs. This is also driven in part by the OSFI requirements, no doubt.

TransUnion does servicing for many of these institutions. We are PCI compliant. We are in line with the ISO standards, and on a regular basis—

● (1125)

The Chair: Mr. Skinner, could I interrupt you briefly? Because the translators don't have a written copy of a report, they are asking if you could slow down just a little bit. Thank you.

Mr. Todd Skinner: Certainly. Do you want me to just continue from this point?

The Chair: Yes.

Mr. Todd Skinner: We are in line with the ISO standards, and on a regular basis, audit under SSAE 16 requirements.

Our data would seem to point to the lack of awareness in industries outside the financial sector and show that there's more need for education in this area, not only in the obligations emanating from a breach but also in awareness around security protocols to prevent a breach.

Awareness by breach notification where warranted will be useful. TransUnion is supportive of the efforts of the government on the part of Bill S-4. While we do not want to inundate customers with notifications, where there is a material risk of harm, there are benefits to customers receiving notification.

Here are some stats on impacts for consumers and TransUnion. The number of potential victims has increased by 600% in the last five years. The number of confirmed fraud victims is up by 100%. Many of these consumers report these frauds to the Canadian Anti-Fraud Centre—PhoneBusters—and while there has been a 300% increase in the number of fraud alerts placed, we still have work to do.

These compromises have a short-term impact on TransUnion and Equifax, increasing call volumes to our centre and requests for alerts to consumer disclosures. We've invested in technology to make that process as effective as possible and to help contribute to that 300% increase in the number of fraud alerts placed on consumer bureaus. What we're doing is helping to reduce the numbers of frauds, and we're pleased that it's not increasing at the same rate of potential victims.

Who pays? The cost is borne entirely by the consumer unless the companies or government bodies that have caused the compromise are willing to step up and pay for the damages that are created. We believe that the burden and those costs should be borne by the companies that compromise the information of the consumer. Not all companies take on this responsibility and agree to pay for these solutions to reduce potential harm to the consumer in mitigating risk.

What should be done? First is notification to the Privacy Commissioner. TransUnion is supportive of the amendments under PIPEDA in this regard in Bill S-4. Where a loss of sensitive financial data has been confirmed, both bureaus should be informed. Where a loss of sensitive financial data has been confirmed, fraud alerts should be placed on both bureaus—at a minimum—to reduce the likelihood of ID theft. As an example, we serve our clients differently, and if a breach has occurred and somebody notifies Equifax, that fraud could still be committed if they go to a financial institution that is serviced primarily through TransUnion. In many cases, both bureaus should be notified.

With respect to synthetic identity, my colleague John Russo talked about synthetic identity and its impact on the Canadian market. In defining the issue, it really is about recreating an identity to commit fraud. In the synthetic fraud, there is no one to complain. There is no constituent to talk to. It is a cost that is borne by many indirectly. In regard to public security, CBC has reported on a few stories, and John referred to the billion dollars in losses that Canadians absorb through different fees and costs. Every consumer pays for synthetic fraud.

How do we work towards a solution? We work with police authorities to report such suspected activities. We take this information, put it into our fraud database, and report it to financial institutions.

The prevention of these crimes requires better technology to ensure that identity cards are not easily replicated and that they cannot be authenticated. If we really want to attack this issue, it also requires the sharing of information between government agencies and the financial sector. The lack of sharing creates silos, and fraudsters take advantage of that.

Today, there's no automated method whereby the private sector can get confirmation as to whether or not a particular piece of ID has been issued by the government or whether that actual ID belongs to the individual who claims it's theirs. TransUnion and Equifax can help by being the conduit to financial institutions, as we already provide, for example, identity verification for AML or KYC. Both of these have been noted in the RCMP paper, the “National Identity Crime Strategy”.

In closing, TransUnion is supportive of the initiative to crack down on identity theft by, first, reporting of breaches through Bill S-4 and notification to both bureaus where a data breach of sensitive financial information has been confirmed, and second, ensuring that companies responsible for the breaches bear the burden and the cost for data breaches, not consumers. Third, on the lack of education and awareness outside of the financial sector in the area of data security and safeguarding, TransUnion is supportive of the data breach notification where circumstances warrant as a key to raising that awareness. Fourth, we are also supportive of a focus on and attention given to synthetic identification, allowing for the sharing of information from government to financial institutions for fraud and ID theft prevention, and investing in security measures for identification cards that are relied upon by the private sector for AML purposes and fraud prevention.

● (1130)

Mr. Chair and committee, thank you very much for having us here today.

The Chair: Thank you very much, Mr. Skinner. That was very interesting.

Now we'll go to questions from committee members. We'll begin with the official opposition, the New Democratic Party, Charmaine Borg.

[*Translation*]

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair.

Hello. I want to thank you for being with us today. Your testimonies have been very interesting.

My first question is to Mr. Russo.

You stated that we always have access to our credit file. However, it is sent through the mail, which still takes a while. If you wish to get your file for free, that's how you need to do it. But if we want access to our file online, we need to pay. Why? Could we do the opposite and get free online access to our credit report? If you ask me, that would be easier for consumers.

Ms. Chantal Banfield (Vice-President and General Counsel, TransUnion Canada): In Canada, since the birth of credit agencies, the law requires us to have offices in certain provinces. Thus we have an infrastructure that allows a consumer in Nova Scotia, for example, to go to a TransUnion Canada office to get a credit report. Because of these legal requirements, we must have an infrastructure that supports the offices we need to have in various places in Canada.

Furthermore, as Mr. Skinner stated, we are investing in telephone technologies such as interactive voice response systems. For example, people will no longer need to send proof of identity through the mail, they could simply go through an authentication process over the phone and receive their credit file through the mail.

You have the example of the United States. In 2005 or 2006, the Fair and Accurate Credit Transactions Act was passed. Under its provisions, American consumers have the right to consult their credit file once a year and the selected means is online access.

For our part, we already have an infrastructure that we need to support since the beginning of the 1990s, when these laws were adopted in most provinces. Things have evolved slightly differently here.

Ms. Charmaine Borg: Mr. Russo, I will also give you a chance to respond. I suppose your answer will be essentially the same.

[*English*]

Mr. John Russo: Yes, I'll respond. I'll just add a few nuances to Ms. Banfield's message.

First, in Canada, at Equifax you can receive that via a walk-in centre, as Ms. Banfield noted. You can also receive your credit report over the phone in a couple of days, again with the IVR process, as well as over the Internet for a small charge.

As Ms. Banfield noted, in the U.S. it's one file per year per individual. After that you have to pay. Here you can access your file every day, 365 days a year, and the infrastructure we built accommodates that, the mail-in requests and everything. We bear those charges in terms of the letters, envelopes, and stamps that have to go to these individuals as part of the verification process and the security processes that go into place to make sure that we're sending the right credit file to the right person.

I won't reiterate what Ms. Banfield said. She gave you a brief history of the legislation.

Thank you.

● (1135)

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

My second question is about an issue raised earlier by one of the expert witnesses. This person pointed out that implementing a credit freeze after identity theft could prevent fraud. In fact, most of the time, when someone steals another's identity, they request credit cards and go on a spending spree.

Would that be possible in your case? Have you thought about putting in place a credit freeze system?

[*English*]

Mr. John Russo: That's an excellent question. We discussed this about 10 years ago when the legislation was coming out in Ontario with regard to Ontario's Bill 152, where you could put an alert on your file to say, “Please contact Ms. Carol Gray before granting credit.” She could provide her cellphone number so you could access her right away to make sure you were dealing with the right individual.

Why the Province of Ontario at that time shied away from it was because consumers wanted real-time authentication. They want real-time access to credit. Let's say you have a credit freeze on your file and you have an emergency, let's say a car accident, and you have to pay certain charges to fix your car, or you have another unfortunate situation where you need access to funds, access to credit. That freeze would totally put you out of the game in terms of accessing that credit in a real-time fashion. It would slow down the whole access to funds, especially in emergency situations.

You see in the U.S. that some of the states have shied away from that and are actually moving away from the credit freeze concept.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Would you like to add something, Ms. Gray?

[*English*]

Ms. Carol Gray (President, Equifax Canada Co.): If I could add, I think there are multiple approaches to the solution and there's unfortunately no one-size-fits-all or silver bullet. So in addition to what John was saying, there are real-time monitoring services that don't inhibit the consumer from getting access to credit, but would alert them in a real-time environment should their consumer report be accessed without their knowledge and they could take immediate action.

[*Translation*]

Ms. Charmaine Borg: Thank you.

As I only have a minute left, I will quickly ask a final question.

Mr. Rowe, you have shown through examples that in the end, very few people requested access to their credit file.

I would like to know if you have the percentage of Canadians who made that request.

[*English*]

Mr. Murray Rowe: Pardon me. I wasn't sure if you said Russo or Rowe.

[*Translation*]

Ms. Charmaine Borg: In fact, anybody can answer.

[*English*]

Mr. Murray Rowe: Sorry. Could we go back a little bit there? I was trying to follow.

Ms. Charmaine Borg: I'll say it in English and we'll skip the translation part.

I'm wondering if you or either Equifax or TransUnion may have information about the percentage of Canadians who actually ask for their credit report.

Ms. Carol Gray: I don't have the exact statistics because while we track the number of inquiries or consumers who ask for it, some of them could be duplicates over the course of a year. I would say it's very safe to say 25% to 30%. At the high end it would be 30% of consumers over the course of a year, so there's a lot of room for improvement.

That would vary dramatically by demographic. Elderly people would tend to access it less frequently than younger people who are establishing credit.

The Chair: Thank you, Madam Charmaine.

Would anybody else like to risk an opinion on that?

Mr. Todd Skinner: From a TransUnion perspective, the percentages would probably be similar to what Equifax has for a delivery of reports to consumers.

Mr. John Russo: Our files from our members are accessed 150,000 times per day, so in terms of members accessing information about you and me as individuals, it's 150,000 times per day. In terms of trade line updates, to give you some background, there are 50 million trade lines updated per month at Equifax.

● (1140)

The Chair: Mr. Rowe, briefly, please....

Mr. Murray Rowe: There's very little information on aboriginal communities, particularly first nations. Part of what we're trying to do is research this and gather the data so that we can have better empirical discussions. I doubt any of my colleagues or I could even comment from an aboriginal perspective exactly what the percentages are. I think they would be a fraction of what the rest of society would be.

The Chair: Thank you very much, all of you.

Next, for the Conservative Party, is Laurie Hawn.

You have seven minutes, please, Laurie.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr. Chair, and thanks to all of our witnesses for being here.

I'd like to start with Equifax. Do you offer identify theft protection products and how much does that set somebody back?

Mr. John Russo: We do. There are two types of protection that we offer. There is a credit alert you can put on your consumer file across Canada for $5 plus applicable taxes. That stays on your file for six years unless you ask to have it removed.

There are also credit monitoring services, as I mentioned in my speaking notes, in regards to programs, where you have real, 24-7 access to your information. You're alerted when there's a change on your file, perhaps an application made in your name, perhaps a change of address because somebody's trying to change your address and mail your information to another address, and other instances like that. So there is the credit monitoring as well as the credit alert.

Hon. Laurie Hawn: At the risk of sounding like a commercial for Equifax, people who don't have that would presumably be less protected than those who do.

Ms. Carol Gray: That's correct. There are optional add-on services to the basic package, everything from out-of-wallet and lost wallet insurance, and so on.

Hon. Laurie Hawn: For Mr. Rowe from Forrest Green, for first nations and a lot of the programs obviously that they participate in, the challenge is cultural, which leads to challenges in confidence and so on. Do you have any stats on first nations victims? We're talking about very low participation in the process. Are there any stats on victims within the first nations?

Mr. Murray Rowe: I don't have any data on that. We've been looking quite aggressively and in fact we're trying to get a bit of a focus on this. I think part of what has to happen is that there's a culture on reserve, in particular. For example, we talked earlier in my presentation about 80% of many of the transactions they don't register with the federal government. They don't pay income tax. There are many different challenges of registration and the concept and benefits of it.

I think one of our goals, quite frankly, is that we're trying to now gather that information so that we can report back to organizations such as yours with more clarity. We're actively involved in this. We're doing it hopefully at a grassroots level. We don't want this to be pushed down onto the reserves. It takes longer, but our approach is to have it led by first nations and have chiefs and councils support these types of dialogues.

Hon. Laurie Hawn: That leads me to a second question I have. Is first nations involvement in the whole process, in terms of educating the people—training staff, getting people involved—is your organization...?

Mr. Murray Rowe: It's not yet, but we have spoken with more than 20 bands. It's a long process. It's expensive, but we believe it's one of the fastest-growing demographics in the country. Ostensibly, there are somewhere between 500,000 and one million individuals who are invisible to the credit bureaus. This is staggering. I don't know any other group, other than maybe new immigrants, that have some of these challenges.

Hon. Laurie Hawn: I think it's safe to say that with the whole high-level of non-registration and so on, there may be a variety of reasons for that. But if we can convince first nations—and it will take time—that they're obviously better in the system than outside the system....

Mr. Murray Rowe: Exactly.

I think land reform, quite frankly—and I mentioned this to the chair earlier—is one of the most exciting things coming down the pipe. The concept of individuals owning, or at least even leasing land.... It would be compliant with subsection 89(1.1), so we're talking about something that is possible, and it's within the Indian Act. I think to be unable to unleash billions of dollars in wealth and allow first nation communities to build equity in their homes and then to even be able to bequeath it to their children and grandchildren is incredible. Right now, they are prohibited from participating, in most cases.

We did an informal survey of five bands, and in some cases interest rates are 300% higher for aboriginal communities. By the way, this is even after ministerial loan guarantees take place, which means 100% backing from the crown. I don't understand some of the issues taking place. I think there is a systemic problem within the banking community and with the way the credit bureaus are gathering and distributing information, which I think we need to examine with aboriginal communities.

One of our goals is to better understand the problem and to get feedback directly from chiefs and councils, and we're aggressively doing that.

But this is not a short-term fix. We're talking about trying to change things and there is no quick win on this.

● (1145)

Hon. Laurie Hawn: Nothing is, but I appreciate that. It was a very pertinent comment and I hope that will make it into the report somewhere.

Ms. Carol Gray: Chair, maybe I could offer a suggestion just so that we are grounded in facts.

We could undertake a study, and if we know what the postal codes are for the reserves, we could identify the number of consumer reports of individuals who live on those reserves. We could take it to a more granular level—no fewer than 15 households, though—without permissible use of the data. We could undertake that study and it may shed some light. If you know the number of people on the reserve today, we could tell you how many have a report and provide some other statistics around that.

Hon. Laurie Hawn: Would you suggest that as a recommendation for this committee to move forward on?

Ms. Carol Gray: I do.

Hon. Laurie Hawn: Yes, okay.

Mr. Murray Rowe: I'd like to make a little point on that.

I think this is far more complex than what is taking place. One of the challenges is that credit bureaus base their information on Canada Post addressing standards. Canada Post doesn't address on reserve. We have some fundamental issues that are taking place.

I love your approach. I compliment you on thinking of this, but I think the dialogue about what is taking place.... I think we have to work hand in hand with many of the committed individuals at Aboriginal Affairs and Northern Development Canada because we have some core issues. On reserves, there are no street numbers. There are no registered streets.

I think we need to step back. We need to look at things like P.O. boxes that are frequented by aboriginals, and first nations in particular, so those are some of the things we're working on. I think it's a very exciting time, but if we can get some support from the committee, that would be much appreciated.

Hon. Laurie Hawn: Thank you. That was helpful.

The Chair: That wraps up your time just about perfectly.

For the Liberal Party, go ahead, Scott Andrews.

Mr. Scott Andrews (Avalon, Lib.): Thank you, Mr. Chair.

Welcome, guys. It's a very interesting panel we have this morning.

I want to go back to Laurie's question about credit alerts and credit monitoring, just to dive into both.

I'd like TransUnion to jump in on it too, because I think you mentioned as well that you have a fraud alert system, so I assume they're similar.

Is it fair to say that TransUnion and Equifax are the front line when fraud is about to happen to an individual? Would you say that you guys would be the first ones to be able to flag that an individual's credit is being used fraudulently? Is that a fair statement?

Ms. Carol Gray: I would say if it relates to credit, yes, but there are data breaches on data outside of credit where we wouldn't be the first line of defence. But if it is information that is contained on the consumer file, we are often seen as the first line of defence.

Mr. Todd Skinner: Prior to joining TransUnion—I've only been with TransUnion for 75 days—I spent most of my career in financial services. I think the front line of fraud prevention resides in the hands of the folks in the financial services sector, and the retail sector when they get that data. How do they store that data, how do they protect that data so that there isn't a breach and it doesn't get in the hands of fraudsters?

I think in terms of a second-line protection, when either Equifax's or TransUnion's credit bureaus are accessed, that's where the products that we have as Equifax to identify fraud, to create awareness of potential fraud, really kick in to help solve this problem. So the way I would characterize this is that if the front-line financial services and retail are one, we're probably one and a half, because there are ways that we can connect with consumers. But the typical fraud happens through those institutions first.

Mr. Scott Andrews: I think what you just said is that in most of those institutions, fraud happens if there's a breach of data, if there's some sort of activity that would be, I guess, criminal in nature.

Mr. Todd Skinner: Yes.

Mr. Scott Andrews: Okay.

Ms. Tara Zecevic (Vice-President, Decision Solutions, Equifax Canada Co.): I was going to add that it's not always a data breach. Sometimes it's rogue employees, or it could be dumpster diving. There could be less-sophisticated to the more-sophisticated data breaches. There are various ways that data could be compromised.

● (1150)

Mr. Scott Andrews: Okay, on the costs for those alerts, the credit monitoring, the consumer has to bear that particular cost. Is there a way that we can change the legislation? You referred to the legislation's saying we have to provide a mailed copy. Should we look at changing the legislation to give the consumer more free credit monitoring, for example, if we took away some of the legislation restrictions on mailing and that sort of thing?

Have either one of you thought about what changes need to be made to the legislation so that you could do more on the free end of things that wouldn't cost you as much?

Ms. Chantal Banfield: I can tell you that every time there's been a reform in the consumer reporting acts in the various provinces, that is one of the things we've advocated for. Basically, in this day and age, do we really need to have an office outside of our core headquarters, because if we didn't have that infrastructure we could invest in other areas—being able to provide information electronically, for example. So we have tried that, but unfortunately we have not been successful. I think my colleague, Mr. Russo, will tell you the same thing, that we've tried that across the various provinces.

Ms. Tara Zecevic: I just want to add that we'd like to see some reform. It would also be in terms of the penalties to organized...and crimes. I know that these identity theft crimes oftentimes are viewed as white-collar crimes, and we'd very much like to see stiffer penalties to criminals in this sector or area.

Mr. John Russo: I agree with Ms. Banfield's statements in terms of not only provincial reform but also in terms of privacy reform. We have canvassed that, but not to much success.

Mr. Scott Andrews: You mentioned these foot soldiers, Mr. Russo, taking people...from their employment. How big an issue is that? We had the RCMP in, and they didn't refer to that at all.

I'm wondering if you could just elaborate a little bit on that particular aspect. I think that was the first that we heard about it, and it's a real concern.

Mr. John Russo: Yes, and I heard the same things when we were working on the CBC investigative piece, that the Toronto Police Service saw it as a big issue, but for some reason the RCMP didn't see it being as big an issue. I'm not saying one is better than the other.

But what really interested me when I started seven years ago at Equifax was the synthetic identities and synthetic crimes, because we knew they were starting to blossom. I would look at the various reports, working with local law enforcement in the various provinces, even in terms of some of the fictitious names they would come up with, such as “Robert Consumer”. At that time there were 100 or 200 reports that we'd be able to identify, working jointly with police, as being fictitious. That was seven years ago. That's increased exponentially every year, and we're up to 1,300 or 1,400 files on average per month using fictitious identities for non-existent people. We see it on the file. This individual ends up busting out, and they think they can leave the country and not pay their bills, but really they just open up a new identity.

We've even seen it in our walk-in centre. We have a walk-in centre just below my office in Toronto. You'll get an individual coming in with a driver's licence, and on the front they're a male, 35 years old, and when they swipe their driver's licence, it's a female reader on the back. So of course we notify law enforcement of that.

To us it's a real problem, and it's a billion-dollar problem.

Ms. Tara Zecevic: The only thing I would add is that oftentimes it's very difficult to quantify the numbers, because, as John mentioned, with these fictitious identities they build up their credit profile over time. Then there's a term that industry uses called “they bust out” when they have an all-time high with their credit. Oftentimes it's very hard to measure that, and sometimes they'll get classified in collections. In that case it's really hard to measure when, in fact, it's not a collection issue; it's a fraud issue.

Mr. Scott Andrews: Does the RCMP have enough resources? Are they really focusing in on that? Or are you somewhat frustrated with the police, that maybe they're not paying enough attention to this? Do you have any comments regarding the law enforcement side of the problem?

The Chair: Could we have a very brief answer, please? Your time is actually up, Mr. Andrews.

Mr. John Russo: Jointly, we could always do more.

● (1155)

The Chair: That's the kind of brevity we appreciate around here, thank you.

That concludes our first round of questioning.

No, it doesn't, actually. Mr. Calandra and Ms. Davidson will share a round.

Mr. Calandra.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): Thank you, Chair. Thank you, witnesses.

Let me first state that I know that you do good work, so forgive me on some of my questioning.

Just to confirm, legislation forces you to mail a free credit report to people.

Ms. Chantal Banfield: No, what I was referring to is that the legislation requires us to have offices in some of the provinces, so we have to have a walk-in centre.

Mr. Paul Calandra: Okay, I get that. But what does that have to do with the fact that a consumer wants a credit report and doesn't necessarily want it mailed to them? How is that the consumer's problem that you have to maintain an office when we want access to our credit report, and we want it free, and we want it online? Why do I care that legislation forces you to have an office? That's just the cost of doing business for you.

Why is that my problem as a consumer?

Ms. Chantal Banfield: I think the issue we have there is that over time we've built an infrastructure that's already in place, so in order for us to change it and invest in other technologies, we still have to bear the burden of those costs. So, for example, we've invested in IVR technology—and I know that Equifax has invested in IVR technology—so you can get a copy of your report by phoning in the centre, authenticating online, and then getting a copy of it by mail. It's processed overnight and it's mailed the next day.

Mr. Paul Calandra: Yes. Again, it's always by mail. I can pay and have it immediately as a consumer, but I have to pay the $26. Somehow I have to wait for the mail because you guys have to have offices in different provinces. Well, boo hoo, too bad. Get out of the business if you don't like it, I guess is the reality.

The problem is that the consumers are having a difficult time. When you guys make a mistake, whether it's your own fault or not, or somehow a mistake is made, it impacts consumers, and it's not easy for a consumer then to fix a mistake that has happened—sometimes by no fault of their own, by somebody else's criminal negligence, or whatever—and the only way for us to do that for free is to wait for you to mail something out to us, or pay. That is obviously causing a big dilemma, because things have changed over the last 10 years, so your business model, presumably, should change to follow.

Ms. Carol Gray: Maybe I could also add that what we want to have is one channel that is universally acceptable and can be accessed, and that is the mail. Not everyone has access to a computer, and when you discover that you think you might be compromised, you probably have access to a phone. So notifying us immediately over the phone, and getting your report within 48 hours, is a very good solution because if we put everything on the Internet, what about the folks—and particularly those on reserves—who may not have access to the Internet? So really, the mail—that's the free one—does provide universal access. But I do hear what you're saying, and it's a matter of an evolving business model for us to add alternate channels in a cost-effective way.

Mr. Paul Calandra: I hear what you're saying, but it strikes me as a business that is just finding every excuse not to provide people with the information that they need. You're probably one of the only businesses ever to come before us and say they have to rely on the mail because more people have access to that.

Honestly, right here, I have access to this. Maybe I'm different, but most people have access to a cellphone. I'd hazard a guess that most people on reserve have access to a cellphone that can give them Internet access as well, and they can download the report for free if you would allow them to do it.

All I'm suggesting is that as things are changing, as identity theft has become more of a problem, there is nobody out there really to protect consumers. You work, obviously, for businesses and not necessarily for the consumer. When a consumer has a problem with what you have done, or the information that you have gathered, through no fault of your own, it is a hard job to change that and we have to pay if we want to change it immediately.

I would suggest that is one of the problems.

But is it another problem that more and more businesses are asking for credit reports? Part of your system of how you judge consumers is based on the number of reports that are being generated. If I want a cellphone, Rogers, Bell, or whatever, will pull a credit report on me, a soft inquiry or whatever they call it.

More and more businesses, for less and less significant matters, are asking you for your information, which impacts consumers in the sense that their credit scores are then impacted, and that's a score that you generate.

Would another answer not be, in order to avoid more people having access, to limit the amount of transactions businesses can ask you to pull a report for?

● (1200)

Ms. Carol Gray: Maybe I can clarify a few things.

First of all, a business needs to qualify to become a member of a bureau to access the report. They have to have a legitimate reason and the proper security protocols in order to access consumer reports. That's number one.

Number two, every time an inquiry is done on the consumer's report does not necessarily affect the consumer's credit score. The scores are calculated in different ways for different purposes . Each credit granting body will use scores in different ways. For example, not all the telecoms report all of their information to the credit bureaus.

Many of the lenders don't even use that information in their credit granting decision. So it's not—

Mr. Paul Calandra: But if they pull a report, does that not impact the score that you give?

Ms. Carol Gray: Not necessarily.

Mr. John Russo: Not necessarily. There are soft inquiries, as you mentioned, or hard inquiries. If it's for credit adjudication, that would impact your score. If an inquiry is just for account management or some other purpose, that would be a soft inquiry.

Ms. Tara Zecevic: John, just to add to that, like inquiries are also lumped together. So for instance, if I'm looking to purchase a home and I'm applying for a mortgage, and within a period of time, if I'm going to multiple lending institutions to apply and get the best rate for that mortgage, that's put together as one inquiry. Also, inquiries are only one of the variables that are used in the calculation within the score.

Mr. Paul Calandra: Yes, but doesn't the number of people who are accessing, either soft or hard inquiries, whatever you want to call it....That then gives more people access to the information that you have collected, right? Which then opens the door for more potential identity theft.

So if I call Rogers to get a cellphone and they say they have to check my bureau, that gives another person on a telephone an opportunity to access my information, just to get a cellphone, when I might already have three or four other accounts with Rogers for my TV and have great credit.

In summary, who stands up for the consumers? I don't think it's you guys because you work for business, and that's fine. But who stands up for us when you make a mistake? Why should it be so difficult for us to fix a mistake that you make, or businesses make, which you are just bringing forward on their behalf?

Ms. Chantal Banfield: I'd like to just address one of your questions with regard to the dissemination of information because of the fact that multiple credit reports may be requested.

You mentioned telcos. Typically, this is the way that telcos will handle that. The agent on the phone actually doesn't see the credit file. The credit file goes in a repository of information that is secured. It's in a bunker. You need to swipe and fingerprint in order to get in there, and the agents on the phone only get yes or no.

Mr. Paul Calandra: Yes, but somebody—

Ms. Chantal Banfield: They get a decision. So the access to information is very tightly controlled. I don't want you to get the impression that anybody can just see a credit file.

Mr. Paul Calandra: I guess my impression would be that if I already have three other accounts with Rogers and they're all really good, why would they have to pull even a soft inquiry? I mean, why would you allow them to do it?

The Chair: As interesting as this is, I'll have to interrupt. You're well over time there, Paul. I think you set a new record for being over time, actually.

That concludes our first round of questioning. I'm going to take a liberty and ask one question from the chair. It's not along quite the same lines, although it does strike me that when a business calls for a credit check, you don't mail the response to them. You don't ask them to wait 48 hours for it to arrive in the mail.

Two of you mentioned that you support in a qualified way the duty of notification that's contemplated in the legislation pending. Under what circumstances would you think a consumer would not have the right to know that their identity had been compromised? Why is your support for the duty to notify qualified in any way?

Can either of you answer, just briefly?

● (1205)

Ms. Carol Gray: The response is not qualified by a reluctance to have the information accessible in a timely fashion by the consumer. It's part of an evolving business model. It's a matter of making the investment in order to change the channels of access.

The Chair: Okay. Maybe this will come up in other questioning.

Mr. Ravignat, you have a five-minute round.

Mr. Mathieu Ravignat (Pontiac, NDP): Thank you, Mr. Chair.

Although it may be surprising, I share many of the same concerns that my colleague across the way brought up. I also share his cynicism. There's just something bizarre about having to wrestle basic information about yourself that's held in companies who seem to want to render that somewhat inaccessible or difficult to get to. I know that there have been improvements.

At any rate, that won't be my line of questioning. I'd rather talk about the aboriginal situation.

I have two first nations in my riding. I'll be very quick, but maybe I'll illustrate my point with a story I was told by an Algonquin friend on Kitigan Zibi. He decided to buy a boat for his mother, because his mother went out every season to go fishing in a particular place that was quite far. He made a pretty good salary, and one day he came back and bought a boat. He presented it to his mother by surprise. She just kind of looked at him, clueless, so he said to her that this way she could get to her fishing hole quicker. She said, “Well, why would I want to be fast?”

I think the story illustrates that there is a certain headspace that we're all in around this committee, including yourselves, and we're dealing with a fundamentally different way of viewing the world. To integrate these individuals into a system that they may not, in fact, want to participate in.... I don't think we can simply say it's an issue of education. I think it's an issue of choice as well. I think there are individuals who very well know what this system represents and what it means. Communities and individuals are consciously deciding not to participate in it.

One of the reasons would be, well, what will be done with that data? Some of you are in the business of selling that data. Selling data on first nations people is a historical problem, because their data, whether it be cultural, linguistic, artistic, or otherwise, has basically been stolen and made into consumer goods in order to make profit for non-aboriginal companies.

I understand, though, the assumption on the basis that this is good, that this is something that needs to be done. That's why I applaud Mr. Rowe's references to the importance of deep consultation and deep conversations with aboriginal people about this and how that tool can actually be used by the communities by themselves, if they desire to, in order to develop their communities or what have you.

Having said that, Mr. Rowe, it's clear that you've done consultations. I'd like to know what themes come up, what concerns come up, from aboriginal communities about integrating themselves in the entire credit system.

Mr. Murray Rowe: That's a great question.

We were at a conference in Toronto recently with several chiefs, Chief Roxane, from Temagami, for example. We had an in-depth conversation. When we were chatting with them, they were initially very hesitant about working with us. It was funny, because when you talk about cultural differences, I was told not to show up in a suit, not to wear a tie. But I thought that was interesting, because my culture is to wear a suit and tie. I don't necessarily need them to change their culture, but I'm not changing my culture. If I always wear a tie, I'm not going to be false to who I am. I think that kind of honesty and those kinds of conversations and behaviours are needed.

We started off with and had very direct and sincere conversations with them. One of the conversations that came up was about Pic River, for example, where they have a huge demand for housing on the reservation. One lady ended up getting a personal loan for 24%. All the banks that were at the conference were pursuing the first nation communities, and they were saying, “We really want your business”. One of the chaps, Moses, who was the housing manager, went up and said, “What is this all about? How can you expect someone to pay a 24% interest rate?”

But, to be fair, the challenge to many of these institutions is that things like ministerial loan guarantees require incredible labour and reviews and bureaucracy in order to secure and in order to allow banks to feel comfortable with moving ahead. The interesting thing is that the number one comment I get is, “I want to be able to build wealth and help my children and grandchildren, and to pass that on”.

Diane Francis recently wrote a new book. It was about kind of a partnership between Canada and the U.S. I'm not so keen on that concept necessarily. But one of the things she talked about was how, in 1776, Congress, by removing lands from the crown and pushing it into allowing home ownership, really kicked off the greatest wealth-creation engine in the history of the world.

It's fascinating. People can look back. We're talking about something hundreds of years old: personal ownership of land. We see wealth in the United States certainly in non-native communities. I think, quite frankly, a lot of natives are sitting back and saying, “Why can't I own my land? Why can't I have financial independence? Why are we prevented from doing this?” But I think it's flipping now to understanding that, quite frankly, banks are global, and they're looking to process loans efficiently and to have reasonable risk.

I think if we can build the files, we can reduce fraud, which is part of the mandate of this committee, but in addition, we can unleash billions of dollars in mortgages for the financial institutions. But let's have it be competitive. Let's have it be at non-native financing rates. I think what's motivating the aboriginal communities is the thought of passing on to their grandchildren and their children property wealth, of having financial independence, and quite frankly, of having autonomy instead of getting a handout.

There's $14.1 billion flowing onto reserve. That's great, but I think a lot of reserves are moving towards financial independence and are looking at changing the paradigm.

● (1210)

The Chair: I'm afraid you're out of time, Mr. Ravignat.

Mr. Rowe, thank you.

Next, for the Conservative's five-minute round, is Mr. Zimmer.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you for appearing before committee today. I have just a couple of questions.

I think a lot of us, as regular Canadians, have this perception of a hacker being a 17-year-old kid who's pretty good with computers, and that's the person who's stealing our identity and just having some fun with it.

Who are these new fraudsters? Put a face on who organized crime is. Is it organized crime in Canada? Is it the Hells Angels? Can you put a face on it for us, if you wouldn't mind answering as well as you can?

Mr. John Russo: In terms of hacktivism, there are different organizations. There are nation-states attacking other states. There's organized crime. You have gangs of individuals who prey upon consumers and their personal information to create these identities or steal their information. There are one-offs; people happen to find a person's wallet or identification and create these one-off crimes. There's not one group per se, in terms of the hacking or in terms of who's going out and seeking this information. There's a multitude.

● (1215)

Ms. Tara Zecevic: I might just add that what we're also seeing with organized crime is that different crime groups who would compete in certain areas are actually collaborating. There could be some groups who are actually good at obtaining the identities. There are other groups of organized crime who are good at creating the plastics, and then there's another group who may actually go to the ATMs and pull out the cash, if that's the particular scheme they're after. There have been numerous cases where we're seeing that kind of collaboration, and they're treating it as a business. If only they put their means to legitimate ends, they could do some great things, but they don't. We're seeing this organizational collaboration globally.

Mr. Bob Zimmer: Would it be gangs who are doing it? Would it be the Taliban? Who are we talking about? I'm assuming we have two groups, domestic and foreign, right? You said nation-states.

What is the predominant one that you see attacking and wanting our identity, let's say, the majority?

Mr. John Russo: The majority here in Canada are Canadian organized criminal activities emanating from Canada.

Mr. Bob Zimmer: Okay.

Would it be organized crime like gangs in Vancouver, and one stealing the cards or information?

Yes, okay. I just want to know what is predominant.

You talked also about terrorist organizations being involved in this. Can you list some examples of which terrorist organizations have been doing it in terms of using stolen identity to finance their regimes?

Mr. John Russo: I couldn't provide that information to you in terms of which terrorist organizations. When we work with law enforcement, and our security departments work in terms of—

Mr. Bob Zimmer: You just know that it's happening.

Mr. John Russo: We know that it's happening.

Mr. Bob Zimmer: Okay.

We heard from former presenters about when our children are born and issued a SIN number. Mr. Russo, I think it was you who said that those are the ones that are hijacked. We heard earlier too that, because they go unchecked for many years, by the time you realize what happened, it's too late.

Can you take us through the chronological picture of what happens? When it's stolen, what kind of things would it be used for? What would that number be used for in terms of it being put on.... I'm not trying to give the criminals a leg up on how to do this, and I don't want you to. Should we look at our kids' credit report at 10, then 15, and then 20? Is it something we should be on—

Mr. John Russo: Unfortunately, minors don't have credit reports in terms of protecting those.

For example, at Equifax, we have a stolen SIN database where we could enter minors' information, a SIN number, that has been compromised. When a fraudster tries to use your daughter or son's information, and they're under age, that would trigger the institution to say that this SIN number has been stolen or lost by an individual. Since children don't have a credit file, it's a lot tougher.

Building the identity—and Tara working with fraud and the associations who deal with fraud can elaborate—simply put, they start with the SIN, which gives a concrete basis to the identity or the fictitious identity. With that they apply, let's say, for a cellphone and they get the hardware. Then they post it on Kijiji or something and meet you near a subway to sell that hardware. They do that over and over again. These identities are faceless crimes and they don't exist. They start simple and build up that credit, perhaps go to a bank and get a small loan, or get credit cards. They work using one or two pieces of identity. When your child applies for their first credit facility years down the road, all of a sudden they find out that their SIN number has been compromised and used over and over again.

Mr. Bob Zimmer: Thank you.

The Vice-Chair (Mrs. Patricia Davidson (Sarnia—Lambton, CPC)): Thank you, Mr. Zimmer.

We'll now move on to Madam Borg, please, for five minutes.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

I would like to come back to Mr. Calandra's questions. It's a little difficult to understand. However, I understand that there are financial constraints.

I do not know if you can answer my question now or if you can write in your response later, but here is what I want to know. If I make a request to obtain my credit file, how much would that cost in terms of the resources for your respective organizations?

[*English*]

Mr. John Russo: We can get back to you with those numbers in terms of what it costs.

A voice: That would be the same for both of us.

[*Translation*]

Ms. Charmaine Borg: I do not know if we have a process by which you can transmit that information to the clerk, but if it were possible, it would be interesting. Thank you very much.

Another concern was raised by certain witnesses in academia. They stated that they had trouble getting data or information about certain things. I know that it's not necessarily in your mandate to document all this, but have you already participated in research projects? Can you share data with academics? I mean demographic data or data on recurring problems for example.

● (1220)

[*English*]

Mr. Todd Skinner: I think from TransUnion's perspective—and I suspect from Equifax's perspective as well—we'd be up for sharing the information with an individual body. The issue goes back to how do we prevent as much fraud as possible? We're trying to get to the government bodies that issue identification and have them share that information through us, as a conduit, to really try to prevent as much fraud as possible. I'm not sure what the conduit should be to deliver that information, whether it's this committee, or on a one-time basis, but what does that look like going forward? Sharing information to have a better understanding of how big the issue is.... We're very much supportive of that.

[*Translation*]

Ms. Charmaine Borg: Thank you. We were told that could be a potential solution. Obviously, if everybody involved worked together, the results would be better.

You said elsewhere that between 25% and 30% of Canadians requested access to their credit file. I think, for my part, that online access would be easier, but are you thinking of other ways by which to encourage consumers to request access to their credit report?

[*English*]

Mr. John Russo: As an example, we go out in terms of Junior Achievement and work with schools in educating young Canadians so that when they do turn of age and are able to access credit they're aware of what the report is, and they know how to read the report and what impacts their score. So we've been doing a lot of work in terms of Junior Achievement and laying the foundation for young Canadians.

[*Translation*]

Ms. Charmaine Borg: Mr. Skinner or Ms. Banfield, would you like to add anything?

Mrs. Chantal Banfield: We have a lot of information on our website. We have worked among others with police services as well as many agencies in order to publicize it. We also run campaigns in schools.

I think Canada's privacy commissioner could include more consumer-oriented information in her toolbox. I believe many consumers consult the commissioner's website particularly to get information when they have been the victim of fraud or another such problem.

Ms. Charmaine Borg: Thank you.

Ms. Zecevic, would you like to add something?

[*English*]

Ms. Tara Zecevic: I just wanted to add that I currently sit on the board as well for Credit Canada Debt Solutions, so we are working with consumers when they are in debt situations.... How do we help them consolidate? Education and financial literacy are big components of that.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Do I still have time?

[*English*]

The Vice-Chair (Mrs. Patricia Davidson): You have two seconds so I think we'll call it.

Ms. Charmaine Borg: Thank you.

The Vice-Chair (Mrs. Patricia Davidson): The next is Ms. O'Neill Gordon, please.

Mrs. Tilly O'Neill Gordon (Miramichi, CPC): Thank you, Madam Chair.

I want to thank all of the witnesses for being with us today. You certainly have given us lots to think about.

My first question is to Mr. Russo. In your notes you write, “The fact of the matter is, criminals will not stop evolving, and our laws, our security and prevention tactics, must change with them”. Can you tell us here today what are some of the changes we need to make? What are some ways we need to help people out there have a better idea of what's going on around them?

It's not just really for Mr. Russo. Any of you can answer because you all have good ideas. But there have to be changes as this is evolving around and we need it.

Mr. John Russo: To start, Bill S-4 is a good initiative in terms of giving consumers a little more power proactively to know when their information's been compromised. So mandatory breach notification, something that many U.S. states have already.... Hopefully this bill does pass the third time around in terms of creating that notification so that when individuals have their information compromised, lost, or stolen at an organization they're aware of it. Most times institutions may bury their heads in the sand and not do anything, or if they're not subject to any fines or penalties, they're less likely to do anything. That's one key in terms of legislative changes.

Carol.

● (1225)

Ms. Carol Gray: Just building on what John was saying, the stiffer penalties, I think, are important because there is a perception that this is a faceless crime. It's benign. There are no real victims at the end of the chain. But there are, and as we've talked about, the costs are huge. The fines should bear, of course, correlation to what the costs are to society.

Mr. Todd Skinner: I think the last point I would make is that we talked about a lot of the breaches happening in small or medium-sized enterprises and they make up a large percentage. There really is assistance that should be offered there around the education of what happens and helping them understand from a security protocol what they need to do to ensure those breaches don't happen. I agree with John and Carol that there needs to be some legislative change and impact that goes with that.

Mr. Murray Rowe: I do a lot of work with police services and I find them very committed to solving these problems. But one of the things that might be helpful.... If you anemically fund a problem, you're going to get poor results. So, wouldn't it be interesting if you could actually track the number of officers and the actual funding that is provided to organizations like the RCMP? You can have people who are committed to making this work, but if you're cutting the department, you're going to have poor responses.

So instead of being prescriptive—asking detailed...and telling the investigators who are very professional already, “Why don't you look at some of the root issues?” I think funding is one of the key factors in this. If you have more crimes that are being investigated, then you're going to allow it to take place. In New York City when they talk about the broken windows theory that Giuliani and others have implemented on even some of the smaller crimes, it's amazing how the crime rate dropped. Maybe we could start implementing that on some of the lesser issues. But get empirical, measure the dollars that are actually spent instead of just asking, “Are you committed to making this work?”

Mr. Todd Skinner: Can I just add one more point? I think as you try to attack this problem there are really multiple solutions to get there. But I would just say that an ounce of prevention is worth a pound of cure. When you think of the number of breaches actually decreasing but the number of potential victims increasing. Technology is catching up. It's how we store information on data. That data is becoming cheaper. How many items we store on that technology is getting more expansive. So, instead of it being 100,000 records, it's a million records, then it will be 100 million records.

I just advocate that trying to solve this problem of identify theft on the front end saves a lot of time and effort on the back end, and allows us to take the funding and resources we have solving white-collar crimes to really get them focused on things that make a difference in our communities. So, try to move as much as we can to the front end to solve this problem.

Mrs. Tilly O'Neill Gordon: Another question I had was...and you have since then mentioned about education and how we can educate more people. I know you're going into the schools but right now we have a segment who did not get it when they were in school, and those people are very vulnerable too. I don't know how we can get the message out. I hear about two types of protection. I wonder how many.... Even my own family wouldn't know that this is even available. This is important news that should be out there. There's another thing about a certain amount to obtain a credit freeze. These are things that, I don't know.... That's where I'm coming from, from that end as to where we can help these people out.

Ms. Tara Zecevic: Yes, that's where I had mentioned earlier Credit Canada Debt Solutions, a not-for-profit organization. You'll see their billboards on buses and in various mail-outs. They have commercials out and it's to help those consumers around financial literacy if they need information. They have counsellors who will work with Canadians to help them, if they've strayed off the wrong path, to get back on and make sure that they feel in control and empowered.

● (1230)

The Vice-Chair (Mrs. Patricia Davidson): Thank you very much.

Did you have something that you wanted to add, quickly?

Ms. Carol Gray: I think there's also more opportunity for the bureaus to work with financial institutions in partnership to get more of that communication out.

The Vice-Chair (Mrs. Patricia Davidson): Okay, thank you.

Mr. Ravignat, please, you have five minutes.

[*Translation*]

Mr. Mathieu Ravignat: Thank you, Madam Chair.

It is perfectly normal for your businesses to want to make a profit; there is no harm in that. However, a problem arises when there is a contradiction between wanting to turn a profit and wanting to protect consumers and the interests of Canadians. One of the solutions is to legislate, but businesses could also take initiatives, create a code of ethics and values, and implement best practices.

I have heard that this is done already to a certain degree, but there is still a contradiction between billing for certain basic services in the case of identity theft and wishing to eradicate the identity theft problem.

What is your financial incentive in seriously addressing the problem of identity theft?

[*English*]

Mr. John Russo: I'll answer that.

Firstly, to clarify, if you're a true fraud victim, there's no cost to put a fraud alert on your file at Equifax. So if you're a true fraud victim you can do that for free. I believe that's at TransUnion, as well. So we're not charging people who have been victimized. If you want to take proactive steps, there's legislation, as I mentioned, in Manitoba as well as Ontario, where you can go proactively and put an alert on your file to ask that you be contacted at a certain number before granting credit.

But there does exist a dichotomy between making business function and the ability to earn a living, in terms of the businesses we're in as well as consumers trying to get access to information. At the same time, there are costs associated with it. I go back to the U.S. example where they are entitled to one file per year, per person, at any one of the three bureaus there. There are three bureaus in Canada, Experian being the third one.

In Canada you can access your file for free 365 days a year, so you don't even have to subscribe to a monitoring product. I always tell people to call or mail—call is easier—and you can get your file for free 365 days a year. So, in terms of a monitoring product, I give you that information and access to it.

[*Translation*]

Mr. Mathieu Ravignat: Nevertheless, there is also a contradiction between promoting that possibility and the promotion of monitoring tools. In other words, if you sell a monitoring product, you will not inform the people that they have free access to their reports.

[*English*]

Mr. John Russo: I think the awareness is there among Canadian consumers that they have access to their file, and they can do it via IVR, through our website, or through a walk-in centre. So that information is there. It's on our Equifax.ca website, informing consumers. If they want, like you say, that real-time instantaneous access, it's for a small fee.

Ms. Carol Gray: I think also it's a matter of giving consumers choice. The monitoring does provide an additional level of protection. Like many consumers, I subscribe to that service because I also like to know what my credit score is. That comes with the service. I also like to know that I have protection if I lose my wallet. So, it's just giving the consumer choice, and then it's our obligation to lay those choices out to the consumers and ensure they're informed when they make their choice.

Mr. John Russo: What I don't think.... Maybe we could have Mr. Skinner in this.

Mr. Todd Skinner: I think one other point I would add is that it's not just about monitoring, but it's about management, understanding your credit, and understanding what happens within your credit file. So as balances go up and down, how does that impact the score?

Credit monitoring, although it is monitoring your credit, is really a tool to help you manage your credit as you go through life and make purchases, whether an automobile or a mortgage. It helps you manage through that process.

● (1235)

Mr. Mathieu Ravignat: Selling these monitoring products, if you had to approximate how much of that is part of your profit margin, is it minor compared to other activities?

Ms. Carol Gray: Very minor.

Mr. Mathieu Ravignat: Is it a covering-cost kind of service, or does it actually generate revenue?

Ms. Carol Gray: It generates revenue, but it's a very small revenue stream.

Mr. Mathieu Ravignat: It's a very small part of what business you conduct then. That's interesting.

Thank you. I think that was it.

The Chair: I'm afraid that's your time, Mathieu.

Next, for the Conservatives, Laurie Hawn.

Hon. Laurie Hawn: Thank you very much, Mr. Chair.

I have one very specific question, and then I'll pass it to Mr. Calandra.

Just going back to the discussion about having a child's SIN number registered. We just took out an RESP for our brand new granddaughter recently. I'll have pictures later. If her SIN number gets compromised somewhere along the way, is there something that will pop up somewhere in the system because there's a recognized SIN number attached to an account? Would that be flagged somewhere in the system?

Mr. John Russo: At Equifax you could call to have that information put into our database if it was compromised. You could do that proactively if you were aware that it was compromised or used.

Hon. Laurie Hawn: So, I could call any of the agencies and ask them to register this SIN number, and that wouldn't be foolproof, I guess, but it would be one bit of protection.

Mr. John Russo: It would help.

Mr. Todd Skinner: One thing we haven't talked about that we've talked about internally is the creation of a child SIN, creating a database where rather than registering when the compromise happens, potentially registering that child SIN at the point of RESP, and then both of us having information so that we can actually prevent the fraud. The use of SIN for children has always been on the lower end of risk when you consider all the other things, but that's an opportunity to get ahead of the problem.

Hon. Laurie Hawn: Yes. You have a SIN number there that might not be used for 15 or 20 years, so it seems to me those SINs would be very attractive for those who want to abuse them.

Mr. Todd Skinner: Yes, that's certainly something I think we could collaborate on as an industry.

Hon. Laurie Hawn: Thank you.

Mr. Paul Calandra: Sorry, I know I was kind of hard on you, but I do appreciate the hard work you do. This is a bit of a challenge, for us and for you.

Mr. Skinner, you said that sharing information is important. You talked about it costing a lot of money, and said that governments and agencies should be sharing information more. But doesn't that cut both ways? When you make it difficult to share information, that's when fraud becomes more difficult for the consumer to catch.

Mr. Todd Skinner: The intent of sharing information is to help us prevent as much fraud as possible. I think this would be the same for Equifax. We have multiple layers of fraud detection as it relates to financial services. Whether it's the device you're logging in to, the information you put on your application, or the authentication questions we ask you, the more information we have and store in our data warehouse, the better we're able to prevent the problem from happening.

In terms of sharing that information—this goes back to the point Carol raised—there are very strict requirements that we have in terms of who we share information with, and the background checks that we do on those organizations when we do share information. When we present the information to those institutions, it's not just a flat file of that credit bureau. It could be an answer of yes or no. So I understand the double-edged sword you're referring to.

We take data management very seriously, both organizations. So the question is, at what point do you stop sharing? The view, based on the amount of data we have and the amount of fraud that exists out there, is that there's still much more work for us to do, and access to that information to prevent fraud becomes incredibly important.

Mr. John Russo: For example, one pertinent point is the amendments to PIPEDA, in terms of Bill S-4, doing away with the investigative bodies. That would help both organizations in terms of working with all members of the financial industry to prevent fraud. You wouldn't be limited to those who have subscribed and been approved as investigative bodies. That would be information sharing that could be shared amongst the bureaus and the financial credit granters.

● (1240)

Mr. Paul Calandra: I'm more interested, though, in the sharing between the consumers and.... You earn money from the financial institutions because you help them protect their investments, you help them ensure that people who are borrowing money are a good risk. But it strikes me that as things have changed...and obviously, identify theft has become a really big problem in the last little while.

One of the big problems we see is that consumers, rightly or wrongly, whether they believe it or not, feel they have limited access to the reports you're keeping on them, and that this is actually helping to increase identity theft. It's not until someone gets rejected for something because of something on their report that they have knowledge of the fact that something has happened with their identity.

Wouldn't having easier access to the reports you're keeping on consumers...? I know that would be a change in your business model, but wouldn't our having easier access, quicker access, and more frequent access to the things you have on us also help you in your quest to stop identity theft?

Ms. Carol Gray: I think that if you come more to the root of it, it's—as we've all talked about—education and awareness.

The issue of access isn't really an issue in consumers' minds if they don't even think to access their consumer reports.

Mr. Paul Calandra: Isn't that a problem, though? That's a problem.

Ms. Carol Gray: That comes down to education.

Mr. Paul Calandra: And when they do, you charge them.

Ms. Carol Gray: No, we don't always charge them. It depends on —

Mr. Paul Calandra: By and large....

I just went on the Equifax website and looked at “free access to my credit”, and it was free for 30 days and then $14.95, no mention of anything.... That was just in the couple of seconds I was looking at it. It might be buried in your website somewhere else.

Isn't that also part of the problem? You're collecting information from individuals. The decisions that you're making are based on what people are giving you. I know it's not you out there saying that this guy's got bad credit. It's based on what the consumers do and we have a responsibility ourselves. I get that.

You're not making these decisions. This is the information that people have uploaded to you and you're putting that on a file, but then they don't have access to it. For some reason or another, consumers feel they don't have access to it, and when they want to access it they have to fill in a form and send it by mail, go to one of your offices that you don't like having, or call on the telephone and wait for it to come to mail, or pay $23 to make sure they're not getting screwed by somebody who stole their identity. Even then, they have to fill in a report, send it back to you, and you get to make the final decision.

How is that something that consumers look forward to?

The Chair: Mr. Calandra, I think we'll have to leave that as more of a comment than a question because you're over time. Perhaps if there's a minute at the end there can be a closing comment to address that issue.

I'm afraid I'm going to have to go on to the next questioner now, and it's Scott Andrews for the Liberal Party.

Mr. Scott Andrews: Don't worry, Mr. Chair, I'm going to carry on in the same line of questioning, because I too can't get this in my head.

Mr. Russo, you say if you're a true fraud victim, it's free. Well, you're already a victim. Isn't this about trying to prevent becoming a victim? The part that I don't get, I think you said earlier...and I assume TransUnion, we're picking on you, but I think it cuts two ways here.

For credit monitoring services you said it's $5.

Mr. John Russo: For an alert, it's $5.

Mr. Scott Andrews: It's $5 for an alert. For what period of time?

Mr. John Russo: It's for six years.

Mr. Scott Andrews: It's for six years.

So it's $5, less than a dollar a year. It takes a dollar to buy a stamp, for Christ's sake. Why couldn't...? I assume an alert is just some algorithm in the computer program that.... Hold on a second. Explain to me how an alert would be triggered, and why wouldn't you want to alert the consumer regardless?

Mr. John Russo: There's a difference in alerting the consumer, which is credit monitoring, and there's an alert for the member who pulls the file.

The $5 alert is legislated in Manitoba and Ontario, and we offer it across the country. When an institution pulls that file they're mandated to receive it in an automated fashion. They would get an alert from Equifax that would read something like, “Please contact John Russo at this number before granting credit.”

Under the legislation, they then have to take reasonable steps to make sure they are dealing with John Russo and not John Fraudster, who is impersonating me. That's mandated by legislation.

Mr. Scott Andrews: That's an alert. That's not monitoring.

Mr. John Russo: That's an alert. That's not monitoring. That's the $5 alert.

The credit monitoring, which is for less than a cup of coffee a day, is a proactive, paid-for service. Unless they are a victim of a data breach and the corporation is paying for it, a consumer can pay for it on a monthly basis to make sure that anybody accessing their file—I always use the example that it's like a fingerprint, if I touch your file or I access your file it leaves a fingerprint. Soft and hard enquiries, you know if anybody has accessed your files. Because you get that real-time alert, you can say, “Wait a minute, I don't deal with this bank. What are they doing looking at my file”? You can call Equifax. You can call the bank. You can call whoever has been accessing your file.

● (1245)

Mr. Scott Andrews: I know you make people pay for that monthly fee. I think a lot of the members on this committee think you should be doing that at no cost to the consumer. I think that's where our frustration is coming from, because when you say, “Let the company pay for it if you're a victim of a data breach”, often we don't know we're a victim of a data breach until it's much too late.

Ms. Carol Gray: The monitoring service is a high-cost service to us. We're accessing millions of trade files that are downloaded to us every day. We have to load them, read through them, and identify if someone wants to be monitored. The computer cost charges are a high-cost service. That's why we charge for it.

Mr. Scott Andrews: Todd, do you want to jump in?

Mr. Todd Skinner: When you look at credit monitoring I would go back to the point I made earlier, that it's not just the monitoring aspect of it. The credit monitoring tool as it's sold has an education process to it, a management process. Again, I have my credit file. I get my email that says there's no news, but I still access it to see what's happening, if balances are changing, scores are changing—the things that make a difference from a credit monitoring perspective.

I would agree with Carol, that it seems because it's computerized and it's automated...but when you're processing hundreds of millions of transactions on a monthly basis it's not inexpensive. Then there's the call centre to support those customers. Often, when fraud alerts come in...and I know we talk about creating online access. The other thing I would emphasize is that when you have a customer call in about a fraud, all this information may be on the website, but they still need to talk to somebody. They want to talk to somebody on the other side to help them feel better about what's happened, as opposed to feeling they're in the dark.

There is a component of.... We're underwater on the fraud alerts. I know it's $5, but when you're talking to somebody and you're trying to walk them through what's happened and what they should be looking for, we lose money on that process.

The Chair: Scott, I hope you weren't building up to some huge closer question there.

I'm afraid that concludes our time, and we've concluded the rounds as well. I'm glad everyone got two opportunities.

We are just going to thank our panel of witnesses from Equifax, Forrest Green, and TransUnion for making a very important contribution to our study on identity theft.

Thank you to all of you.

We should advise committee members that this Thursday is going to be a very interesting panel. We have representatives from the Toronto Dominion Bank, the Royal Bank, CIBC, BMO, and Scotiabank, without the Bankers Association. If you think these guys got a rough ride, you can anticipate what next Thursday will be like.

Anyway, thank you to everyone. That concludes our meeting.

The meeting is adjourned.