HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 025 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 29, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 29, 2014

● (1105)

[*English*]

The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)): Good morning, ladies and gentlemen. We'll convene our meeting of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Mr. Ravignat, do you have something to say?

Mr. Mathieu Ravignat (Pontiac, NDP): Mr. Chair, before we continue with the regular business of this committee, I understand that there was a reference to committee that is particularly important, and therefore the opposition would like to give notice of motion:

> That, pursuant to Standing Order 111.1(1), and subject to the order of reference of May 28, 2014, the Committee undertake a study of no fewer than 4 meetings to examine all matters regarding the proposed appointment of Daniel Therrien as Privacy Commissioner of Canada, that the Committee invite Daniel Therrien to appear, and that the Committee report its findings and recommendations to the House.

I have two other notices which I think are important:

> That the Committee invite the former Privacy Commissioner of Canada, Jennifer Stoddart, and the Interim Privacy Commissioner of Canada, Chantal Bernier, to assist the Committee in its study of the proposed appointment of Daniel Therrien as Privacy Commissioner of Canada.
>
> That, the Committee invite legal and constitutional experts, and other experts in the protection of privacy, to provide testimony regarding the proposed appointment of Daniel Therrien as Privacy Commissioner of Canada.

Whenever we get a reference to committee of this nature, it is crucial that the committee study it.

Thank you very much.

The Chair: Mr. Ravignat, I hate to interrupt you, but your notice of motion is non-debatable. You've served notice, and thank you for that.

Mr. Calandra.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): I don't mind entertaining a debate on that briefly.

The Chair: If there's a willingness of the committee to discuss the motion....

Mr. Paul Calandra: One of the proposed motions anyway.

The Chair: Notice was given for three separate motions. Do we have agreement of the committee to discuss briefly one or any of the motions? If we open this door—

Mr. Paul Calandra: Certainly I don't mind talking about one of the motions with respect to Mr. Therrien. I will prepare to amend Mr. Ravignat's suggestions.

The Chair: The chair was notified earlier of the interest on the government side to invite or to call the new Privacy Commissioner appointee, Mr. Therrien, before the committee to be vetted as per the order of reference in Mr. Ravignat's notice of motion.

I don't want to get into a debate about this right now.

Mr. Paul Calandra: We have witnesses.

The Chair: We are short of time. We're contemplating a truncated meeting because we anticipate bells and therefore a vote on a number of procedural matters that are happening in the House of Commons. We want to make the best use of the time we have.

In that light, I'd like to welcome the witnesses today as we continue our study on the growing problem of identity theft and its economic impact. We're very pleased today to have representatives from five of the major chartered banks in Canada. I'll introduce them in the order in which they've asked to appear. We'll be inviting them to make brief introductory comments and then be available for questions from committee members.

From the Canadian Imperial Bank of Commerce, we have Mr. Philip Fisher, senior director, eChannels risk management. Welcome, Mr. Fisher. Next we'll be hearing from the TD Bank Financial Group, Mr. Paul Milkman, senior vice-president, head of technology risk management and information security. Welcome, Mr. Milkman. We also have Mr. Ed Rosenberg, vice-president and chief security officer, legal, corporate and compliance group for the Bank of Montreal financial group. Mr. Rosenberg, welcome. We have Jay Stark, vice-president, internal audit services, personal and commercial banking for the Royal Bank of Canada. Welcome. From Scotiabank we have Jennifer Frook, director, shared services, fraud management office.

I'm very pleased that you could all be with us today. We'd like to make the most of the time that we have available on this pressing issue that our committee is studying, so in that same order, we will hear first from Mr. Fisher of the Canadian Imperial Bank of Commerce.

Mr. Philip Fisher (Senior Director, eChannels Risk Management, Integrated Business Control Services, Canadian Imperial Bank of Commerce): Good morning. I'm Philip Fisher, senior director of eChannels risk management, representing CIBC. I'm part of CIBC's retail banking fraud group. My particular specialty is in the area of online crime or cybercrime, but I'm able to speak on a variety of fraud issues.

First, on behalf of CIBC, I would like to thank the committee for giving us the opportunity to speak here today and to entertain any questions you might have. We'd also like to commend the committee for its willingness to study such an important issue to our industry, and to many Canadians who are impacted by identity theft every day. It's a complex subject, and your leadership is appreciated.

It is CIBC's view that identity theft is not a new or growing issue. Rather, it's an evolving issue. Identity theft has been part of the fraud landscape for some time. However, what has changed is how fraud is performed. Years ago we would have been talking about the theft of receipts, bills, a physical wallet, or telephone-based fraud. Now we talk about advanced persistent threats, merchant breaches, malware, and phishing. Advances in technology and the accompanying dispersal of personal information across the Internet has created a changing risk environment.

To help facilitate today's discussion, I think it's important to discuss what we mean when we talk about identity theft. The Criminal Code of Canada describes identity theft as knowingly obtaining or possessing another person's identity information for the purposes of committing an offence. Personal identity information is further described to include, among other things, name, address, date of birth, written signature, electronic signature, user name, credit card number, debit card number, financial institution account number, social insurance number, driver's licence, and password.

Financial institutions typically use a narrower definition of identity theft and tend to monitor and report fraud based on type. Before I explain more about these different types, it should be noted that financial institutions don't all share a common definition of what is meant by identity theft. That is one of the reasons why producing aggregate data on identity theft is a challenge.

As I was saying, fraud types are generally based on the source of the stolen information or how it is exploited. These fraud types could include copying of magnetic strip data at point of sale or automated banking machines. Information captured in this manner is typically used to create counterfeit cards or make card-not-present purchases. This type of fraud is something the banks have not traditionally counted as identity theft because of the limited amount of information involved. Information obtained from a consumer's computer which is infected with malicious software is the type of fraud that is concerning because of the amount of information at risk and the difficulty involved in identifying the issue and remediating it.

Use of e-mail fraud, phishing, to collect personal information, is one of the frauds that's undergoing evolution. Phishing e-mails have traditionally focused on capturing online banking sign-on credentials or credit card information; however, increasingly, we're seeing attempts to broaden the types of information being captured.

Another example is theft of a person's mail. With third party data breaches, examples are merchant and transaction processors. Recent media reports have highlighted that these breaches can, depending on the merchant, involve large numbers of consumers. A stolen wallet is a simple example of lost or stolen information from the consumer, or there can be disclosure by the consumer through the sharing with third parties or inappropriate disposal of information.

Some of these issues have been around for some time and have mature and robust controls in place to identify and respond to them. Others are newer and controls are still evolving. A number of my peers will speak to this at greater length in their remarks.

Even with sophisticated fraud detection controls in place, financial institutions cannot combat identity theft alone. To effectively combat identity theft, there needs to be a coordinated effort on the part of financial institutions, consumers, and the government. Consumers play an important role in protecting themselves from identity theft. Consumers know their personal information and how they are using it, and they are uniquely positioned to identify unauthorized use.

However, consumers are not fraud specialists and need guidance and support. Financial institutions and government agencies provide essential support, educating consumers on the risks and providing consumers with the tools they need to protect themselves. Good examples of the tools available are transactional alerts and free credit bureau monitoring offered by some financial institutions. One of my peers will delve deeper into this in his comments.

The government's role in protecting consumers from identity theft cannot be understated. As I explained earlier, technology is changing the landscape in rapid and meaningful ways. Having the right legislation in place with appropriate consequences for those who would commit identity theft is a strong deterrent. Financial institutions have advocated for identity theft legislation in the past. They will continue to support the government as it seeks to strengthen controls in this continuously evolving area.

● (1110)

I have first-hand experience where this partnership works. The copying of card information at bank-owned automated banking machines, known as ABM tampering, has changed significantly over the years.

When I first started working on it, CIBC would measure ABM tampering in terms of hundreds. Now with anti-tamper hardware common on ABMs, and an increase in the likelihood of jail time for those involved in this crime, CIBC now measures these incidents in the single digits. Other banks have had similar experiences. We look forward to carrying forward this success in other areas.

In closing, I would like to thank the committee again for the opportunity to address this important issue, and I would be pleased to answer any questions you may have.

The Chair: Thank you very much, Mr. Fisher.

Second on our list is Mr. Paul Milkman from the TD Bank Financial Group.

● (1115)

Mr. Paul Milkman (Senior Vice-President, Head of Technology Risk Management and Information Security, TD Bank Financial Group): Mr. Chair, thank you for the opportunity to be here today.

As an American living in Canada for the past five years, this is my first chance to appear before a Canadian parliamentary committee, and l am very much looking forward to it.

[*Translation*]

I'm sorry I can't speak to you in French, but I am American.

[*English*]

I think Philip has provided a very good framework for thinking about identity theft.

Identity theft is a crime. The active use of stolen identity to commit financial fraud is a separate and distinct act, and it is a separate and distinct crime. However, as a bank, our prevention strategies need to be seamless since there can be a causal relationship between identity theft and financial fraud. I would also note that our interests are very tightly aligned with those of our customers when it comes to both identity theft and fraud. Banks do everything they can to prevent their customers from becoming a victim of either one of these crimes.

How do we approach prevention? We think of this as a shared-responsibility approach, where customers and banks both need to act vigilantly. At TD, we have a four-step process aimed at ensuring that customers make responsible efforts to protect their personal information. Let me touch on each of them briefly.

First, we ask customers to be careful about sharing personal information. If you're asked to provide personal information, ask how it will be used, why it is needed, with whom it will be shared, and how it will be safeguarded. Never disclose your personal identification number, or PIN, your social insurance number, or passwords. Passwords used for banking should not also be used with social media.

Second, we ask that people use appropriate security measures. Keep account statements in a safe place. They contain sensitive and personal information. Take advantage of technologies that enhance security and privacy when you use the Internet, such as digital signatures, anti-virus software, personal firewalls, and data encryption. To use a specific TD example on this point, TD offers our customers a free download of Trusteer Rapport, which prevents phishing and some Man-in-the-Browser malware attacks, as well as a one-year subscription to McAfee anti-virus software. These tools are made available for free to all of our customers, to help them protect themselves while on the Internet, not just in their banking transactions, but in all of their use of the Internet.

Third, check statements for accuracy. Check account statements or online statements to ensure all transactions and charges are correct. Access your credit report from a credit reporting agency, such as Equifax or TransUnion, once a year to ensure it is accurate.

Four, guard your cards, cheques, and ID. When travelling, carry only the identification and credit cards you need. Don't carry your SIN card. Make a list of all your cards and their numbers and store this list securely.

Taking these actions will help a customer prevent identity theft and the potential for a resulting fraud.

On the other side of that shared responsibility, banks need to be clear about what personal information we retain about a customer, how a customer can access that information, and most importantly, how we protect our customer's personal information.

On retaining personal information, banks use personal information in order to establish the identity of customers. In order to provide a product or service to a customer, or to help with any money-laundering or other types of defence, we need a name, address, birthdate, occupation, and some sort of identification. For certain products, such as home loans, we may need to collect other personal information. We may also obtain information about customers from third parties, including credit reporting agencies, but this will only happen with the customer's consent.

Individuals can access or update the information that banks have at any time. There are also several privacy preferences available to customers, such as choosing not to be contacted by direct marketing officers or choosing not to participate in customer research surveys.

Specific to protecting customers' information at the bank, banks make significant investments to maintain strong security standards to protect our systems and customer information against unauthorized access and use. For example, our systems have been designed to ensure that the personal identification number, password, or other access codes are always held private and confidential. For your protection, your access codes are known only to you. Our employees cannot gain access to them and they will not ask you to reveal them. All our suppliers and agents, as part of their contracts with TD, are bound to maintain your confidentiality as well, and they may not use the information for an unauthorized purpose. We also require them to prove that they are operating with appropriate controls and defences.

● (1120)

In the online environment, banks have specific measures in place. At TD, these would include comprehensive threat intelligence, access management controls, transaction logging and analysis, secure firewalls, constant monitoring to proactively identify unusual customer account activity, phishing and spam protection, and the highest levels of encryption available to ensure that data can only be decoded and read by the customer or by our system.

In conclusion, the twin issues of identity theft and financial fraud will always be a concern for both banks and their customers. We will always be in a battle with criminal elements that want to steal data and use it for their benefit, but I can assure the committee that in terms of technology information risk management, Canada's federally regulated banks operate at the top global standards for information security and identity theft protection.

Thank you.

The Chair: Thank you very much, Mr. Milkman.

Moving right along, we will go to the BMO Financial Group and Mr. Ed Rosenberg.

Mr. Ed Rosenberg (Vice-President and Chief Security Officer, Legal, Corporate and Compliance Group , BMO Financial Group): Good Morning, and thank you very much, Mr. Chairman.

On behalf of BMO Financial Group, l am pleased to join today's discussion on identity theft, and more specifically on how Canada's banks protect our customers, employees, and assets from harm against fraud and other criminal conduct.

It is timely to appear here today so shortly after the wrap-up of fraud prevention month at the end of March. In March, BMO joined other financial institutions, consumer groups, law enforcement agencies, and our partners in the Canadian Bankers Association to raise awareness about fraud and crime reduction.

BMO takes identity fraud and all criminal activity very seriously. We believe each of our employees has an important role to play in fraud reduction. At BMO, our corporate policies are designed to prevent, detect, and respond to suspected criminal activity. Our work in corporate security is the product of a nearly 200-year history of protecting our clients' information while providing them with convenient access to their accounts.

The protection of our clients' information means responding to evolving and complex criminal activities, such as fraud, corruption, cybercrime, and acts of violence. We provide all of our employees with clarity in their roles and responsibilities for individuals and their respective corporate groups to be engaged in the management of criminal risk.

Just two months ago we organized a number of activities that raised awareness, including hosting anti-fraud sessions with employees across our organization, ensuring that anti-phishing brochures were available for our customers in our branches, providing fraud avoidance tips on our bank statements, and getting our message out over Twitter and Facebook.

Our staff, serving across our lines of business and ranging from our customer service representatives in our local branches to our commodities and futures traders, are our front line in our fight against fraud. We work with them to develop programs to prevent and detect criminal risk in such areas of responsibility as managing internal controls on cash, credit and transaction processing, client and financial information management, and regulatory monitoring and compliance.

Our corporate environment continuously evolves with considerable innovation of our internal controls and processes. Our criminal risk environment changes daily, and the banks are organized to respond to it. We try through authentication to validate information and documentation; however, the quality and security of documents can be inconsistent across jurisdictions, and there are few reliable ways to universally authenticate documentation.

We have zero tolerance towards criminal activity and have practices in place to manage our response to any activity that takes place.

A part of those efforts is to identify individuals conducting financial fraud. As an industry, we invest millions of dollars and dedicate hundreds of employees to the prevention of, detection of, and response to criminal behaviour. As well, we collaborate on initiatives, in some cases organized as an industry by and through the CBA, to identify criminals and work with law enforcement to prosecute them.

Banks have highly sophisticated security systems and experts in place to protect customers' information and to protect them from being the victims of financial fraud. Each bank, as noted above, heavily invests in the identification of fraudulent activity. The adoption of chip and PIN standards alone has cost the industry millions of dollars to reduce the risk of card fraud in Canada.

However, as the environment changes daily, organized crime turns more and more to new technologies and has migrated and exploited other avenues. Industry forums and collaborative tools are in place to share fraud patterns and preventative controls. Through the CBA and other forums, we liaise with a multitude of parties to enable the protection of the industry. These could be ISPs for cybercrime, insurance for common fraud, or law enforcement to share trends.

We also do this internationally. As of two weeks ago, I met with my peers from more than 30 banks internationally to discuss the risks we face, the manner in which we can protect our institutions and customers, and how to best collaborate and expend our efforts.

Mr. Chairman, it's clear that the protection of the credentials you and I and members of the committee each establish as part of our unique digital identities is a team effort between the individuals who hold them and the vendors whom they trust with them.

At BMO we are proud of the Canadian banking sector's strong record of ensuring safe and convenient access to our clients' financial information.

On behalf of BMO, I'm pleased to be here today, and I would be happy to answer any questions you may have.

● (1125)

The Chair: Thank you, Mr. Rosenberg.

For RBC, the Royal Bank, we'll go to Mr. Jay Stark, vice-president.

Mr. Jay Stark (Vice-President, Internal Audit Services, Personal and Commercial Banking, RBC): Good morning. My name is Jay Stark. I represent RBC in my former capacity as vice-president of fraud management, a position which I held for 11 years.

RBC is committed to providing our clients with secure financial services. We've a proud history of innovation and excellence in fraud management. Thank you for inviting RBC to address the committee today. We applaud both the committee and the government on this identity theft study.

Identify theft is a serious crime leading to substantial financial losses, significant inconvenience and loss of sense of security to consumers, funding further criminal activity, concealment of criminal identities, and it may assist terrorist activities.

You've heard from my colleagues and past witnesses. The definition of ID theft differs among industry participants, as does the understanding of fraud; however, we can all agree that ID theft is an important subset of financial crime. Previous research and testimony has undoubtedly shown that identity theft is a complex topic. Similar to the differing opinions on definition and quantum, there is no shortage of opinions and vendor solutions to address the issue. A timely, effective, and efficient response requires the application of a variety of fraud strategies against a proven framework. This is an area in which I believe my colleagues at the table and I can best assist the committee.

A successful framework must optimize relationships among what I call the four fraud management pillars. The first is consumer impact or inconvenience. The second is fraud losses. The third is cost, both to the banks and to society. The fourth is risk management.

The framework called the fraud value chain must balance the following key fraud management strategies: intelligence, for example, using negative data, linking criminal events, and sharing trends and best practices; prevention—consumer awareness and education, and chip and PIN are good examples; detection—sophisticated analytics and industry partnerships; investigation, including prosecution and asset recovery; and regression or root cause analysis.

Each of these fraud strategies has decreasing marginal returns. For example, it is practically impossible to prosecute all participants in a large organized debit scheme, nor would it be practical to prevent fraud by reducing withdrawal limits to $10 or freezing credit bureaus, for example, to disincent criminal activity. Further, strategies lead to fraud migration. For example, the implementation of chips and PINs led to substantial increases in cross-border and card-not-present fraud.

The most powerful fraud strategies in the past decade have been industry initiatives, and more importantly, advancements in detection analytics, including both the sophistication of analytics and the application of enhanced data in quality and breadth. Combined with elements of other available strategies, detection analytics allowed differentiated outcomes and optimized the overall fraud management program.

The framework and the strategies have been very successfully applied to a wide range of fraud schemes, including debit and credit card lending and cheque fraud. In fact, despite a growing portfolio and the increased sophistication of criminal activity, RBC enjoyed the lowest fraud loss experience in over a decade in absolute terms last year. At RBC we spend significant time and resources in reviewing, testing, and enhancing our strategies to address financial crime, including identity theft.

Unfortunately, my time is limited. We would be pleased to work with the committee and to provide any additional assistance as you continue to study this important issue. I look forward to your questions and comments today and working together in the future.

Thank you for the opportunity to present.

The Chair: Thank you, Mr. Stark.

Last but not least, from Scotiabank, we welcome Jennifer Frook, director of shared services, fraud management office.

● (1130)

Mrs. Jennifer Frook (Director, Shared Services, Fraud Management Office, Scotiabank): Good morning. My name is Jennifer Frook, and I'm the director of the fraud management office at Scotiabank. In my role I am responsible for the assessment of fraud and the reporting of fraud risk across the global Scotiabank group. This includes the proactive identification of fraud prevention practices and technologies to mitigate the bank's exposure to fraud loss. A large part of our ability to prevent fraud and protect our customers depends on our work with other stakeholders. I am also the current chair of the CBA's fraud specialists group.

I appreciate the opportunity to speak to this committee about an issue we all take very seriously, one that has a direct impact on our customers, our industry, and on the economy. This is a critical issue for the bank, given how important customer confidentiality and security is to banking. Without the trust of our customers that their information and identity is secure, we cannot perform our role.

To address the committee's interest in identity theft, I will focus my opening remarks on the following points related to fraud and identity theft: training and education, prevention, detection and mitigation, and last, collaboration.

An important part of preventing fraud is ensuring our staff has the proper training required to protect our customers from identity theft and other forms of fraud. Scotiabank has rigorous training programs in place for our employees, with customer-facing roles such as those in our branches, contact centres, and bank card security operations. Employees are required to go through a comprehensive onboarding training program, as well as to take annual refresher courses. Equally important is empowering our customers with the information and awareness necessary to help them protect their information and ensure that any time they are faced with a security concern, they know exactly what to do.

In terms of fraud prevention, we have instituted a number of security measures to help ensure the integrity of our customers' information. Several examples of that follow.

In Canada, 100% of retail credit cards and active debit cards, as well as all Scotiabank ABMs, have been converted to chip technology to support enhanced security against lost, stolen, and counterfeit card fraud.

Our debit cards are equipped with Interac Flash technology, which uses secure chip processing technology to protect customers against various skimming and counterfeit fraud. Many of our retail credit cards are equipped with a similar Visa payWave functionality. Scotia InfoAlerts are e-mail and/or text messages that provide an additional layer of protection and help our customers monitor activity on their accounts.

We also offer customers free software, as my colleagues have alluded to, at their institutions, to help them protect their information. We have partnered with McAfee, and offer all Scotia online customers 12 free months of McAfee AntiVirus, which helps customers protect their machines against viruses online and network threats. We also offer free Trusteer Rapport software, which helps to protect against malicious software, or malware.

In every channel and for every product we offer, there are a number of fraud controls in place to detect suspicious activity. These controls are multi-layered and dynamic. All of this is aimed at letting the true customer in and keeping the fraudster out.

We are also continuously testing our technologies and systems as well as repeatedly monitoring and reviewing our customer activities for any unusual or suspicious behaviour that could be fraudulent.

Naturally, despite our best efforts, our customers' credentials and other personal identification information is compromised and can be stolen. When banks are made aware of such compromises, we take appropriate measures to protect the customer and mitigate losses, such as notifying the customer that their card and/or account was compromised, blocking the stolen credential, and replacing it, when possible, with a new one, such as replacing a compromised credit card or resetting the customer's online or mobile log-in password.

We monitor account activity for fraudulent or suspicious transactions. We update customer profiles to include notes that this customer has been the victim of an identity theft, so that front-line employees are able to ensure enhanced know-your-customer policies are performed when authenticating customers on their account. Of course, we indemnify the customer for his or her loss, and make the customer whole.

Banks also collaborate and voluntarily report to the Privacy Commissioner any material or systemic breaches of personal information.

● (1135)

Identity theft is evolving, fast moving, and ever changing. We do our best to ensure that we are keeping on top of it by tracking and assessing the fraud associated with it and constantly developing new protective measures.

I should also say that since the act of identity theft nearly always takes place outside of the banking environment and is beyond our control, we need to work with other stakeholders to manage it. We provide information on our own internal tracking of fraud to a number of institutions and stakeholders, such as Visa, American Express, Interac, law enforcement agencies, and the CBA. These groups also compile information from other financial institutions and provide industry metrics and benchmarks from which we can measure our own mitigation of various types of fraud, many of which were enabled by some sort of theft of a customer's personal information. For example, the CBA fraud specialists group has a mandate to work together on fraud prevention and share information and best practices.

Allow me to conclude there, and to simply say, once again, that as a bank we are committed to doing our best to ensure the safety of our customers personal and financial information.

I look forward to your questions. Thank you.

The Chair: Thank you, Ms. Frook.

Thank you to all of our presenters for their testimony today.

We still anticipate that we may be interrupted at some point by bells and subsequent votes, so we won't waste any time getting to questions.

The first round of questions goes to the official opposition, the NDP.

For seven minutes, Mr. Ravignat.

Mr. Mathieu Ravignat: Thank you to the witnesses for being here today.

From your presentations, I get a sense that the magnitude of the problem is not particularly fully understood, as well as your important role. I think most Canadians would agree that banks have a crucial role to play in ensuring that identity theft doesn't happen.

We've heard from researchers who have attempted to contact banks in order to get information on cases of identity theft and on practices you have in place to ensure that it doesn't occur. They've had very little response, and very little data has been shared with them.

I understand that you're in the business of making profit and you have to be careful about being competitive with your fellow competitors, but it seems to me that more transparency, more openness with greater access to cases of identity theft as well as your practices would help researchers, as well as parliamentarians, wrap their heads around an increasingly serious problem.

I'd like to ask why you are not sharing this type of information with academia. If you are, perhaps that would be reassuring, and it would be interesting to know.

Whoever would like to contribute their point of view, feel free to jump in.

The Chair: If more than one responds, please keep the answers brief, as we only have seven minutes for the questions and the answers.

Mr. Ed Rosenberg: I'll take the question. Thank you very much, sir.

On behalf of my peers, one of the questions we have been faced with is regarding the academics who have approached the institutions. None of us has been able to determine who they've approached within the institutions and how those requests were not met.

The other thing is that we would be willing to undertake a study of this, and as a group, go back, define it, and try to quantify it, again through our partner at the CBA. But it will take us some time.

Last, if I may speak on behalf of my institution and the others, we don't believe that crime is a competitive advantage. We do work together, and we actually do want to stop it. We work with our industry partners, as you've heard my peers articulate, on the best strategies through education or other measures to inform the public, as well as stop the impact of identity fraud, let alone identity theft.

Mr. Mathieu Ravignat: You are, at a minimum, aware that academics are attempting to contact your institutions in order to get information to study the issue.

Mr. Ed Rosenberg: As of this week, we are.

Again, I'm accountable for fraud within the bank itself. None of my staff, and no one within my chain of command, has ever been approached, so we're unclear as to where that request actually went.

Mr. Mathieu Ravignat: That's peculiar.

We've heard from first nation individuals and bands that indicated the issue of identity theft is linked to a lack of access to information by many first nations people. Some bands have complained that banks are taking advantage of this particular situation, particularly the lack of credit bureau information, to create consumer credit that is way beyond what is acceptable. There are numerous examples of first nations individuals being charged interest rates 300% higher than non-natives.

Are you trying to tackle some of the issues inherent with dealing with first nations? Is there a consultation process in place by your institutions in dealing with a population that is much more vulnerable to identity theft than others?

● (1140)

The Chair: Mr. Milkman, are you interested in responding?

Mr. Paul Milkman: Yes. I'm not sure whether we'll be able to answer it closely. As retail institutions our branch strategies, especially in areas with predominantly first nations populations, do offer different types of training and different types of materials to attempt to help with the problem. But I think most of us would probably say it's not so much our area of the business, and we'd be interested in getting back to you with some information on what we would do differently.

Mr. Mathieu Ravignat: That would certainly be appreciated. Maybe you can discuss with your various organizations that this is indeed a problem. I have two first nations in my riding and many of my colleagues do as well. The first nations are being gouged and there are high rates of identity theft in these communities. We need to respond.

I'd like to come back to my previous question, but from a consumer perspective perhaps.

There's tension between keeping financial information that you need to be competitive and your products in house and educating the public and the relationship to identity theft in that context. How are you providing tools to consumers to make sure they have access to what they need to prevent their identity from being stolen? I'm not talking post-identity theft; I'm talking prevention. It's not necessarily the responsibility of government to do it.

Mr. Philip Fisher: I'd be happy to address that.

First of all, CIBC would not view the security and integrity of their clients' information as being a competitive advantage or anything that we would want to compete with anybody regarding it. We would view that as an expectation on the part of the customer that their information is protected.

I think it's important from an education tools perspective. We keep the client informed as to what's happening with their account. CIBC, through its online banking service, has a variety of transaction alerts. You can go in and see when your personal information changes, when your PIN changes, when your password changes, when any large transactions are performed. We even offer free credit bureau monitoring. We do that because we think it's important for the client to know what's happening with their account and for them to know it real time. Clients who subscribe to those services would get an e-mail or an SMS telling them what's happening with their account in real time so they could intervene and ask any questions they might have of the organization.

The Chair: We'll have to leave it at that, Mr. Fisher. Thank you very much.

Your time is up, Mr. Ravignat.

For the Conservative Party we have David Anderson. Welcome to the committee, Mr. Anderson.

Mr. David Anderson (Cypress Hills—Grasslands, CPC): Thank you, Mr. Chair. It's good to be here today.

When you're talking about things like return e-mails and SMS texts and those kinds of things, is it gained at the password level? Is it gained at a failure to log out of a site and someone can access through that? Is it gained through phony websites? Over the last while, one of your banks has been sending me something that is obviously not from you, and I'm wondering when you run into these problems where the access point usually is.

● (1145)

Mr. Philip Fisher: There is actually a variety of them. You have listed quite a few. The core is that we see a considerable number of phishing e-mails; we see malicious software on the clients' computer —that is one I would highlight as highly problematic—and we see clients providing their information to third parties and then see disclosures happening there. But I think each of these ebbs and flows.

If you were to ask me about phishing, I would tell you that the number of phishing incidents over the years has increased, but the number of clients who actually fall victim to them has declined over the years. When I first started doing this, I did a rough calculation which said that for every phish that went out, I would see 40 clients provide their information. Now I see one to about half a client, on average, who provides information to those sources.

You held up your mobile device. This is one of the challenges. People with a large screen can see the visual aspects that are saying something is wrong with this, but when you shrink it down to a mobile device, it becomes significantly more difficult to pick out those cues that might tell you that something is actually wrong with it.

Mr. David Anderson: I don't know much about this, but often you go back to the e-mail address. That is really the only thing that, to my mind, gives it away, because there are some pretty attractive-looking website presentations out there.

I want to ask what percentage of crime is related to what you would call petty attempts to get information and what percentage would be much more due to organized crime. I think Ms. Frook talked about its being evolving, fast-moving, changing, sophisticated technology. Is it increasingly organized crime, or is it still people who are hacking from home and who are fairly smart at being able to punch through those systems?

Mr. Philip Fisher: Certainly the card-based fraud, such as the copying of debit and credit cards, is the area in which you tend to see the larger organized crime groups involved. But when you get into phishing and malware, the barriers to entry for fraudsters to get in are considerably lower. You can go onto the Internet and buy a kit that will help you phish a bank. You need very little technical capability. You buy this kit; it does all the work for you, and it sends it out.

You will start to see more individuals appearing in some of those types of frauds, because it is a do-it-yourself kind of thing compared with the larger-scale organized crime and debit and credit card types of fraud.

Mr. David Anderson: Okay.

My financial institutions are regularly sending me their online agreements. They keep changing. They keep shifting around. They're almost indecipherable for an average person to read anyway, but one thing that seems to be fairly common in them is that they seem to lessen institutional responsibility each time I get one of those, and to increase my responsibility.

Do you hear from the public that they're frustrated with that kind of thing? It looks to me, when I get them, as though there may be some change in technology, but it's typically because it looks as if the financial institution is trying to absolve itself of a responsibility rather than improve my protection.

Is there any comment from anybody?

Mr. Philip Fisher: I can continue, if you'd like.

Certainly, looking at some of those electronic access agreements is somewhat intimidating for consumers. But from a bank's perspective, we try to understand that our clients are not technology experts and are not information security experts, and so we try to keep expectations of them fairly low. We want you to have anti-virus, and we want you to try to protect your computer, but we understand that this is difficult for some clients to do.

We review these cases on a case-by-case basis. We would look at one and ask whether we are erring on the side of the client: are we giving them the benefit of the doubt?

The Chair: Mr. Fisher, I'm going to have to cut you off.

Mr. Anderson, you can tell that the bells are ringing.

With the unanimous consent of the committee, we might extend this for 15 minutes or so. These are half-hour bells, and we're in the same building.

Is it the will of the committee to continue for 15 minutes?

Some hon. members: Agreed.

The Chair: Okay, we have agreement.

Carry on, Mr. Anderson. You have about two minutes left in your seven-minute round.

Mr. David Anderson: Thank you, Mr. Chair.

My question is about one of the small things in those agreements. How realistic is it to have people changing their passwords every 90 days, when they have a dozen different places that they use passwords? You're not allowed to use the same one, so you're expected to keep different accounts and change passwords regularly. I just think that for some people that's okay, but for many people it is a real source of frustration.

How do you deal with that frustration?

Mr. Philip Fisher: Certainly from CIBC's perspective, we do not require you to change your online banking password every 30 days. We understand that it is difficult for clients to remember their passwords. Even within our own site you occasionally need multiple passwords or personal verification questions.

From the perspective of evolving online banking, CIBC is moving to a two-factor authentication system that we're going to launch next month. We're going to take away some of the personal verification questions and we are going to start sending clients SMS messages with one-time use codes for use when they want to do a higher-risk transaction and when they really need them, putting the security where it needs to be at the moment that the client needs it. We will try to make it such that they don't have to remember all of these things.

● (1150)

Mr. David Anderson: I probably only have time for one more question, but I want to know the difference between the U.S. and Canadian protection. Some of the technology to me really seems to be lagging in the United States. I think we're ahead of it in a number of areas here. Here you get the magnetic strip cards. Down there you get a failure to be able to transfer money electronically. How does that contribute to or how does that prevent this kind of identity theft and fraud?

Mr. Paul Milkman: TD, obviously, has a very large presence in the United States and is the largest foreign-owned retail bank operating in the United States. What we would see is that there are variations in the protections between the two countries. We would say that chip and PIN, in particular, have been a huge advantage to the Canadian consumer. Frankly, seeing some data from both sides of the border, we would say we've seen techniques like skimming at ATM machines literally migrate south of the border because of the superior control of the Canadian environment. We would say there are other areas where I think large institutions in the U.S. and Canada are working very hard to accelerate their efforts. Transactional data analytics, that is, gathering information on what a normal transaction in our bank looks like, is something that both are working on very hard. You would say there's a set of shared problems that we're all working on. There are certainly, currently, some advantages in Canada over the U.S.

The other thing that's different, I believe, in Canada is that the banks and some other key industry players, like the telecommunications firms, are working more closely with public safety. The possibility of either a legislative change or even an interpretational change of existing legislation in Canada will most likely allow Canada to leapfrog the U.S. in making progress at a national level. The public-private partnership here is a bit more accessible. In the U. S. we're seeing signs that they're likely to continue to lag in terms of really forward-looking legislation on privacy and on security itself.

The Chair: Mr. Milkman, I'll have to stop you there.

Thank you, Mr. Anderson.

For the Liberal Party, Mr. Scott Andrews, for seven minutes.

We'll probably have time for you to do your round of questioning. I'm pleased because all three parties will have had an opportunity. Then we'll release our witnesses with thanks, adjourn, and go and vote. I'll ask the committee members to come back for 10 or 15 minutes. We need to discuss future business and witnesses for next Tuesday.

With that, Mr. Andrews, for seven minutes.

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

Mr. Fisher and Mr. Stark, I think you both mentioned that the definition of identity theft is not consistent. Do you want to elaborate on that, as we're looking at identity theft? What is the definition that we should be drilling down on?

Mr. Jay Stark: One of the key examples would be credit card and debit card skimming. Some people will look at debit and credit card as covering identity theft in that case. A lot of the banks don't look at that. We look more at things when credentials are stolen, or it could be paperwork, or it could be credit bureau data, and an application is made to a bank in the name of another party. That would be identity theft. But the big problems we have are really the grey areas.

In my opening remarks, I wanted to present the whole of financial crime, then we would split out, to the best of our ability, what we agree on for identity theft, and then show the grey areas, so the committee could look at it and make their own opinions.

Mr. Philip Fisher: From CIBC's perspective, we tend to monitor fraud at a much lower, more granular level. Some of it's operational and organizational, where we have, say, a team that's responsible for identity theft. We have a dedicated identity theft team. They have a defined set of duties and responsibilities that they have for certain types of frauds, which may be different from how another organization would split it up. When we talk about trying to get information up to an identity theft level, the challenge we have is making sure that we get those apples to apples, and the same types of information are being put in the same categories. Then what we're providing is obviously meaningful, right?

● (1155)

Mr. Scott Andrews: For me, in the last couple of days on the committee, it's been trying to compartmentalize individuals who actually are people. I don't think anyone talked about synthetic identity theft. I had that from our last group. There are ones that affect actual people and then ones that are synthetic identity theft. How big is the synthetic identity theft issue in the bank?

Mr. Ed Rosenberg: Let me take that.

Again, I think what Philip was articulating is that we look at fraud very differently. Both of those, be it a fictitious person or a real person, will manifest itself in identity fraud, if you want, or fraud on our shores. However, we would view them as significant risks.

Synthetic ID is a big concern for us. One of the challenges we have is to ensure that when we authenticate a client and validate the transactional activity that they're doing, we have some mechanism we can actually reconcile to, for example, to say that this is Mr. Andrews and these are Mr. Andrews' transactions, and therefore we will allow, conduct, the transactions for him.

It's difficult for us. Synthetic ID is a big concern because we have no control over the establishment of the ID, the production of that ID, but we deal with the manifestation when it's presented to us to conduct those transactions.

They're both very big topics for us. To quantify them would require a deeper dive into our respective systems to pull out the number.

Mr. Scott Andrews: That leads into my next question because, Mr. Fisher, you mentioned free credit monitoring. We had the credit agencies here. I think they're the front line, and they'll say, “No, we're kind of the front line, but the banks are the front line.” Who is the front line on raising the red flag?

On the free credit monitoring that you mentioned, Mr. Fisher, I just want to dive a little bit into the role of the credit agencies and the relationship with the banking industry.

Mr. Philip Fisher: For the free credit bureau monitoring, we have a relationship with the credit bureau. Our clients can go onto our site and they can sign up for this service. Then when the credit bureau gets an inquiry on the client's account, what happens is they pass the information back to us, and then we ultimately send it on to the client to investigate.

We'll tell the client which merchant was inquiring on their credit bureau file, what type of hit it was, and when it was done. There is even contact information available for the merchant who was doing the inquiry.

In this particular case, we would be fronting for the credit bureau.

Mr. Jay Stark: We've actually established a relationship with the credit bureaus, and particularly with Equifax, where we screen all the credits using both analytics and negative databases. So I think it's a joint effort among the credit bureaus and the banks.

Mr. Scott Andrews: One other thing you mentioned was about cheque fraud, Mr. Stark. Can you elaborate a little bit on cheque fraud with identity fraud? Are they separate?

Mr. Jay Stark: I think to Mr. Rosenberg's point, we need to spend a little bit more time and go through the whole cycle.

We see some manifestation of identity theft in the cheque space. Somebody might take over an account—an account takeover. What I worry about more is where the funds are going, so where the frauds are going. We follow those frauds and we mark those frauds. We see a number of instances where people will come in with false identities to set up corporations, for instance, and be beneficial owners, or they'll be directors. Those ones are a little bit more problematic because they will now be laundering funds.

We spend a lot of time looking at that. We also spend time looking at the account takeovers of somebody's particular account.

Cheque fraud is pretty prevalent, whether it has a piece of identity theft or not, or whether it's just a straight-out fraud. We call it a first party fraud.

The Chair: Thanks you very much, Scott. I'm afraid that wraps up your time pretty much.

I think we have adequate time to get to our votes, but first there is one point of clarification I'd like from your testimony, Ms. Frook.

There is a growing sense that the public has a right to know if their personal information has been compromised. There is talk about a duty of notification in legislation that's pending. In your testimony you said that it is your policy to notify the individual, and not the Privacy Commissioner and not the credit bureau, if their identity has been compromised or if there is fraud taking place in their account.

Our understanding is that it's not the case. My credit card can be compromised and you'll fix it and make me whole, but I will never know about it.

Is it the policy of your bank that you tell every victim of identity theft that their personal information has been compromised?

● (1200)

Mrs. Jennifer Frook: In the specific case that you mention in terms of a credit card fraud, when we at Scotiabank are made aware of a number of our customers who have been the victim of a compromise, we do reach out to our customers. We explain that we believe their credit card has been compromised and that we are going to take proactive measures to protect them from having fraud on their accounts.

The Chair: What about on an individual basis? You said when it's a group. Obviously, if it was a big issue, as when CIBC had all their trouble, the public knew about it, but what about as an individual?

Mrs. Jennifer Frook: Even in individual cases, again speaking specifically to your comments about debit and credit fraud, we at Scotia would never reach out and just cut off your access to credit. We would attempt to notify you. We very much like some of the technology we have available where we can reach out to you with electronic means. You don't have to wait for that telephone message at home; we can alert you immediately.

The Chair: That doesn't quite answer the question—

Mrs. Jennifer Frook: I'm sorry. I apologize—

The Chair: What I'm trying to get at is, is it the view of the five major chartered banks that you would support the duty of notification that's being contemplated in the legislation that's going to be coming down the pike? This means you would have to inform the victim that their personal identity has been compromised. Is it your practice currently? Would you support it being codified and mandated in legislation?

Mr. Paul Milkman: It is TD's practice today to notify all individuals who have been compromised, or we suspect have been compromised. For all material or larger systemic things, we would also notify regulators, the Privacy Commissioner, etc., but on an individual basis, to answer your specific question, it is our policy to do that today.

Ms. Jennifer Frook: Scotiabank would echo that.

The Chair: I think we're pretty well out of time, folks. We're going to suspend the meeting. If there's interest, perhaps there are others who would like to respond to the same question. It is a top of mind issue with a lot of Canadians, and it's something we're going to be wrestling with, with legislation.

Mr. Rosenberg.

Mr. Ed Rosenberg: I believe we generally are supportive of the model and the legislation that's before the House. That's the first statement.

On the second one, the individual basis, most of our systems aren't geared to identify fraud at the individual level. I think Mr. Fisher articulated that we rely upon our customers to review their own transactions. In fact, they become the first line of defence for us. Then it becomes a one-on-one relationship with the customers, and through that dialogue, if they are a victim of identity theft, there are steps that we lead them through to protect them, and it's the bank's obligation to do that.

The Chair: Mr. Stark.

Mr. Jay Stark: I would echo TD's comment.

We notify the individuals, and we would notify the Privacy Commissioner if there was a relevant or significant breach. We do have a joint committee of compliance and fraud, and a number of other parties that would actually look at that and make sure that the appropriate parameters have been put forward to ensure that the Privacy Commissioner is told.

The Chair: Mr. Fisher.

Mr. Philip Fisher: CIBC shares the same views as the other witnesses.

The Chair: Okay, that's very helpful.

Thank you very much, folks. We're going to suspend the meeting. We'll thank our witnesses and excuse them. We will reconvene here right after the vote for roughly a 10-minute planning meeting, in camera.

- _____ (Pause) _____
-

[*Proceedings continue in camera*]