HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 016 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 1, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, April 1, 2014

● (1100)

[*English*]

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

We will convene the meeting. We're here today to study the growing problem of identity theft and its economic impact. We're pleased to begin our study with witnesses from the Department of Employment and Social Development, Mr. Louis Beauséjour and Mr. Robert Frelich. That will be from 11 to 12, and then a separate panel will begin.

Mr. Beauséjour and Mr. Frelich, you have about 10 minutes for opening remarks, and then we'll open it up to questions from the floor.

You have the floor, sir.

[*Translation*]

Mr. Louis Beauséjour (Assistant Deputy Minister, Integrity Services Branch, Service Canada, Department of Employment and Social Development): Mr. Chair, members of the committee, good morning.

My colleague Robert Frelich and I are pleased to appear before the Standing Committee on Access to Information, Privacy and Ethics.

We are pleased to provide you with information that will assist you in your study on the growing problem of identity theft and its economic impact upon citizens and businesses, and the steps that businesses and law enforcement agencies are taking to protect Canadians from identity theft.

One of my duties as Assistant Deputy Minister of Integrity Services at Service Canada is to implement processes and administrative measures linked to the issuance of social insurance numbers.

[*English*]

As you may know, Service Canada is the service delivery arm within Employment and Social Development Canada. The department delivers over $100 billion in programs and services every year related to different programs, such as employment insurance, Canada student loans, Canada pension plan, and old age security. And the social insurance number is used by all of these programs.

But the use of the social insurance number is not limited to Employment and Social Development Canada. Many other federal departments and agencies, such as Canada Revenue Agency, RCMP, Canada Border Services Agency, and Department of Justice, use the SIN and the social insurance register, or the SIR, on a daily basis.

As the SIN is an important element to ensure that the right benefit is provided to the right person at the right time, it plays a central role in identity management.

Today I will explain how our practices in the issuance of the social insurance numbers and the administration of the social insurance register improved over the years to increase the integrity of the social insurance number program and to reduce the impact and the incidence of identity fraud.

The evolution of the SIN program can be broken down into four periods with respect to integrity measures put in place to protect the SIN.

[*Translation*]

The first period is what I call the early years, from 1964 to 1976. The SIN program began in 1964 as a register for two federal government programs: unemployment insurance, now employment insurance, and the Canada Pension Plan.

Shortly afterwards, its use was extended to the Canada Revenue Agency for tax reporting purposes. Since then, the SIN program has grown to become a unique identifier for more than 50 federal programs or services and is a staple in the lives of Canadians.

At that time, there was little integrity in the issuance of social insurance numbers. For example, employers were allowed to ask for SINs to be issued to employees, clients were not required to present identification, and if someone had lost their SIN, another number was issued and assigned to them.

The second period is from 1976 to 1996. I will qualify that period as a time of increased integrity of the paper-based processing of SIN issuance.

Starting in July 1976, the SIN program began requiring clients to provide identification documents to prove their identity, and applications for a SIN had to be made by the client. Employers could no longer request a SIN to be issued for their employees.

At the beginning, a large number of identity documents were accepted for SIN issuance, including secondary identity documents, such as a driver's licence. However, at the end of this period, almost all secondary documents were no longer accepted for SIN issuance, and SIN agents were using primary documents such as birth certificates and documents issued by Citizenship and Immigration Canada.

● (1105)

[*English*]

In the period spanning from 1996 to 2006, we began transitioning from a largely manual and paper-based approach to integrity towards system changes that would begin to automate integrity measures.

In November 1996, the first of such changes was implemented. An electronic link with Citizenship and Immigration's database was established, allowing for the verification of identity and status of permanent and temporary residents who arrived in Canada after 1972.

In 1998, the Office of the Auditor General began looking closely at the SIN program. I would like to take a few moments to share with you the various conclusions the office reached, because that period was a seminal moment in the administration of the SIN and the SIR.

In its 1998 and 2002 reports, the Auditor General's main findings were that the proof of identity procedure needed to be improved, that existing information sources had to be used more effectively, that the information in the SIN database was not always complete and accurate, and that there were more SINs in circulation than there were Canadians over the age of 20.

To address these issues, important initiatives were implemented with regard to the administration of the SIN and the SIR which had positive consequences on government efforts against identity theft and fraud. We implemented the dormant flag, introduced an expiry date for social insurance numbers issued to temporary foreign workers, and developed a proof-of-identity internal intranet reference website.

[*Translation*]

The dormant flag identifies SINs that have not been active for a period of five consecutive years or more—meaning that there was no income-related activity, such as filing taxes, or interaction with government programs during this period. Since then, someone with a dormant flag on their SIN file must provide original proof of identity to have their SIN reactivated, an original birth certificate if born in Canada, or Citizenship and Immigration Canada documents if born outside of the country.

This reactivation is done either in person at a Service Canada centre if they reside in Canada, or by mail if they reside outside of Canada. In addition, to better assist agents in detecting potential identity fraud and theft, the SIN proof-of-identity internal Intranet reference website was developed in 2003. Through this website, agents responsible for the issuance of SINs have access to detailed information on what to look for in identity documents to ensure their authenticity.

Building on the recommendations to make better use of different sources of information, the department signed agreements with all 10 provinces, beginning with Ontario in 2005, to develop electronic links between provincial vital statistics agencies and the Social Insurance Register. Under these agreements, we are able to validate the information found on provincial birth certificates, as well as to receive death data from provinces which is matched against the SIR. This allows us to identify records of deceased individuals, preventing further payments from federal programs from being issued.

Moreover, these agreements integrate the ability for parents to apply for a SIN for their child at the same time as they register the birth with provincial authorities.

● (1110)

[*English*]

Finally, in the most recent period, since 2006, the department put in place two important features to assist the administration of the SIN: the certified training of agents and the SIN code of practice. Through our certification program, agents are specifically trained in the issuance and administration of social insurance numbers, and since 2006, only certified agents can issue SINs to clients. The SIN code of practice, which is a public document available on our Internet site, provides standards and guidance to users of the SIN—individual Canadians, employers, or other stakeholders—in understanding their responsibilities with respect to the SIN.

[*Translation*]

For instance, the code advises employers on how to handle employee information, especially social insurance numbers. It emphasizes employers' key role in detecting and preventing SIN related fraud, as illegal employment and income tax evasion are two of the main motives for this type of fraud. In the code, employers are prompted to immediately report suspected misuse of a social insurance number to Service Canada.

We began receiving birth and death data electronically from Ontario in 2006.

The first province to have validation of birth certificate information was British Columbia in 2008. Currently, there are electronic links with eight provinces, with the remaining two planned to be in place by 2016.

We are pleased to report that our work and efforts were recognized by the Office of the Auditor General in 2009 and 2011. The Auditor General recognized the measures taken by the department to address concerns of past audits, indicating that the department achieved significant improvements on the issues that have been raised.

[*English*]

Now, I'd like to talk about the two most recent initiatives made to the SIN program aimed at increasing its integrity: the redesign of the SIN mail channel and the termination of the SIN card. Given that SIN applications by mail represented only 4% of the 1.5 million SIN requests processed in a year, that approximately 55% of these requests were rejected due to errors in the application forms, and that the mail channel's identity management measures were not as robust as those of the in-person channel, SIN requests can no longer be made by mail, except for individuals in remote areas, or by those who have extenuating limitations, or by those who are from outside the country.

The department was also aware of integrity issues related to improper use of the SIN card. The SIN card was never intended to be an identity card as it does not contain any security features or identifying attributes. However, the convenient wallet-sized format of the SIN card led many recipients to carry it in their wallet, despite the department advising not to do so. As of yesterday, individuals no longer receive a SIN card, but instead receive their SIN in a letter. This initiative will contribute to the prevention of identity theft and fraud related to the potential loss or theft of SIN cards.

[*Translation*]

The social insurance number is central to the administration of many programs. Since 1964, we have made much progress in developing a robust social insurance number program that assists departments and governments in the administration of their benefits, while protecting clients from identity theft and fraud.

We are continually working with key stakeholders, such as other government departments, the provinces and territories, and the private sector, to identify what more can be done to reduce risks of identity fraud and theft. We are also regularly assessing our processes and policies to make them more secure and more robust, while providing a high level of services to Canadians.

We would be pleased to answer any questions you may have.

● (1115)

[*English*]

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

We will begin immediately, then, with the official opposition and Mr. Mathieu Ravignat.

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

Thank you to the witnesses for being here.

It wouldn't be an understatement to say that Canadians are worried about their private information and that the possibility for breaches of their private information have increased since the advent of various social media. The legislation we have in place is definitely not robust enough or even modernized enough to ensure the protection of Canadians and their private information. I think the apparatus of government is suffering a little bit from that as well.

I have a more specific question for you. In the privacy commissioner's report tabled recently, we can find the following paragraph on page 21:

> Notwithstanding the above, we would like to highlight that there may have been more personal information compromised as a result of the loss of the hard drive than was reported by ESDC to affected individuals.

Would you care to elaborate on why compromised personal information was not disclosed to individuals specifically? Why didn't the ministry choose to report this?

Mr. Louis Beauséjour: I'm not well placed to talk about all the details of that specific breach, because I'm not directly in charge of the program where it occurred. My understanding is that we were moving really fast to try to inform clients and that we didn't inform them of the key elements of information that we understood could have been on the hard drive at the time.

Mr. Mathieu Ravignat: So why do you think the commissioner has said more personal information compromised may have not have been reported to affected individuals?

Mr. Louis Beauséjour: Do you mean which information that could have been? I don't have that detail with me.

Mr. Mathieu Ravignat: Okay. It would be interesting if you could forward that information to the committee because it's pretty fundamental that Canadians know and the affected individuals know all the types of information that were lost in their cases, and that be....

The Chair: I was just going to interrupt, Mr. Ravignat, as well, but go.

We'll let you have the point of order.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): The witnesses are here to talk about identity theft. They are not here specifically to talk about the report so they wouldn't be prepared in any way to talk about the report or the breaches.

Now I would imagine we can certainly talk about issues around protecting identity, but I'm just not sure whether we're giving the witnesses.... We're putting them in a very bad position to try and talk about a report when we didn't actually invite them here for that purpose.

The Chair: Let me just deal with it as a point of order. You're challenging relevance, I think, would be the only legitimate point of order you might be raising, and I would rule you don't have a point of order. Questions of that nature are certainly relevant to the subject matter we're talking about.

But I wanted to be clear. Mr. Ravignat, are you making reference to the loss or theft of the student loan records within the—

Mr. Mathieu Ravignat: That's correct. Yes.

The Chair: —580,000 student loans or student loan information?

Mr. Mathieu Ravignat: That's correct, Mr. Chair.

The Chair: I'm going to allow the line of questioning. I don't see it as a legitimate point of order.

Answer to the best of your ability, Mr. Beauséjour.

Mr. Mathieu Ravignat: So you would be willing to forward that information to the committee?

Mr. Louis Beauséjour: The department will be forwarding that information.

Mr. Mathieu Ravignat: Thank you for that.

[*Translation*]

Although the Minister of Employment and Social Development said that he accepted the Privacy Commissioner's recommendations, as noted in the report, the half-million Canadians who were the victims of the loss of these records expect their government to take action.

What real measures are you going to take over the next few months to respond to the commissioner's recommendations?

● (1120)

Mr. Louis Beauséjour: As we indicated in the report, we have already taken a certain number of very real measures to respond to these recommendations.

[*English*]

In light of the incident we immediately reviewed and reinforced our procedure and protocol involving IT security specifically pertaining to the handling of personal information on portable storage devices such as USB keys and external hard drives.

As well we took action to strengthen training for employees regarding the proper handling of sensitive data such as personal information.

To be a bit more specific we have new stricter protocols that have been implemented. Unencrypted external hard drives are no longer permitted in the department.

[*Translation*]

Mr. Mathieu Ravignat: Were these measures in place in 2013?

Mr. Louis Beauséjour: In response to the events in 2013, we implemented them immediately. We did not wait for the Privacy Commissioner's recommendations to improve measures that were already in place at the time, in order to reinforce the protection of private information.

Mr. Mathieu Ravignat: Very well. Thank you.

[*English*]

In a digital world, it's important the loss of information be dealt with in a very rapid way because of the consequences, but it took two months for some of these cases to be revealed.

Can you explain to me why it took that long?

Mr. Louis Beauséjour: There are a number of things the department had to do. It took a bit of time before we realized the hard drive was missing. After that we did a number of searches in the building to find the hard drive. After that it also took some time to determine what was specifically on the hard drive. Those are all the different things that were between the time we found the hard drive and the time we were in a position to report.

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

Your time is up, Mr. Ravignat.

Next, for the Conservatives, is Mr. Laurie Hawn.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr. Chair.

Thank you to our witnesses for joining us.

I'd like to talk about not so much the misplaced records, because it's hard to tell, if *x* number of records are misplaced for whatever reason, what the net result is.

Can you speak about the frequency of actual breaches, of cases in which somebody has actually used someone else's SIN card or SIN inappropriately?

Mr. Louis Beauséjour: We are not aware of any misuse of the SIN following a breach involving loss of personal information.

Hon. Laurie Hawn: Are there instances of misuse of SIN other than—?

Mr. Louis Beauséjour: Yes, there is sometime misuse of the SIN. As part of our regular investigations, we do investigations related to benefits. and as part of those kinds of investigation, we may come across individuals who are improperly using a SIN to get benefits.

Hon. Laurie Hawn: Do you have a sense of numbers or the frequency?

Mr. Louis Beauséjour: Basically, if we look at the number in the last fiscal year, we had a bit more than 4,500 investigations that led to a conclusion that there was a misuse of the social insurance number. But there were investigations associated with the potential misuse of a SIN.

Most of them—I will say three-quarters of them—were related to a benefits investigation at the same time, and about 1,400 were related to potential issues raised with SIN applications.

When we do an investigation, it is not necessarily about misuse; it could be a situation in which we have a flag in our social insurance registry, as one example, that someone is deceased and someone comes to the office to reactivate the SIN or get a new SIN card. Before providing them with their social insurance number, we refer them to our internal investigator to go further in questioning the individual and getting additional pieces of identification to confirm whether or not the person who requests the SIN issuance is the right person.

● (1125)

Hon. Laurie Hawn: Would that classify as a deliberate or accidental...? Would it be that someone did it with intent or that it was not intentional?

Mr. Louis Beauséjour: These cases could be due to errors in the server, or sometimes they could be real potential fraud. If it's real SIN fraud that could lead to other types of fraud, we refer it to the RCMP for their investigation and to validate whether there is fraud or not.

Hon. Laurie Hawn: How often does it happen that things are referred to the RCMP for prosecution?

Mr. Louis Beauséjour: I don't have that information with me here.

Hon. Laurie Hawn: Is it frequent, infrequent? I know that's a subjective assessment

Mr. Louis Beauséjour: I don't know.

Hon. Laurie Hawn: How are those instances discovered? Does somebody just say that something doesn't look right here, or how do you come across these?

Mr. Louis Beauséjour: There are different ways. Informant leads that may come across it. As I said, it could be people coming to the office and not having the right piece of information that we're looking for. Sometimes they don't have permanent documents, or sometimes the document they are providing doesn't look like the right document.

Among other types, people may come to the office who have received a T4 for benefits that they never received. In that case we investigate the benefit that is part of it. We also investigate whether the SIN was improperly used.

Those would be examples of different ways that we can come across such cases.

An individual could come directly, telling us that they were in their view facing identity theft and were looking at getting a new social insurance number. In that case we will investigate the matter and will refer to the RCMP to determine whether there's real identity theft.

Hon. Laurie Hawn: Do you have any idea of the numbers or frequency of people coming to you saying, “I think I've suffered identity theft” and wanting a new one?

Mr. Louis Beauséjour: I do not directly, but I would suspect that the maximum number we have.... As I said, there are about 1,400 people we have identified as having only issues related to the SIN. I will guess that this probably means a higher number for it, but I will have to get back to that question and figure out whether we have those specific statistics.

Hon. Laurie Hawn: That's 1,400 that were referred to the RCMP for further investigation. Is that my understanding?

Mr. Louis Beauséjour: These would be the cases that we would refer to the RCMP, when people say they are facing identity theft. We do not investigate identity theft. We investigate all the questions around the issuance of a new SIN, a new SIN card. We also investigate to ensure that the benefits are going to the right person.

Hon. Laurie Hawn: I understand.

You don't allow it by mail anymore and maybe I missed this, but can somebody apply online for a SIN card?

Mr. Louis Beauséjour: No, we cannot apply online. People have to come at the office to get a SIN card. Now, parents can apply for the social insurance number at birth as they register the birth of their child. It's a new program that is now being implemented in all provinces. That's the only way.

Hon. Laurie Hawn: I just had a new granddaughter on Sunday so we're going through that as we speak.

Again, this may be outside your lane, but are you aware of the level of penalties for identity theft or misuse of SIN cards? I guess my question is if you are, do you think they're adequate? Or should they be looked at ?

Mr. Louis Beauséjour: I'm not aware .... I know that there is a penalty for people misusing the SIN as it relates to the program. I don't have the details here. I can get back to you about that.

● (1130)

The Chair: I'm afraid that concludes your time, Mr. Hawn. Thank you very much and congratulations, Grandpa.

Next for the Liberals we have .... Actually once Mr. Andrews is back in the room, technically he is the committee member but we'd certainly be flexible enough to welcome the honourable member from Prince Edward Island, Mr. MacAulay.

Hon. Lawrence MacAulay (Cardigan, Lib.): Thank you very much.

I'm a substitute on the committee but I did listen to your presentation, enjoyed it very much and thank you very much for being here.

You indicated that the SIN card is no longer issued as a card because it was so convenient to carry. What I gather from that is this great concern that people actually are not concerned enough about their own identity at times and this is why this was done. I'd just like you to elaborate a bit on that.

Mr. Louis Beauséjour: People are not always aware of the risk of carrying with them a number of different identity attributes in their pocket. We do our best to increase awareness about the importance of protecting these kinds of information. As part of SIN code of practice, on the website we specifically identify what people should and should not do with their social insurance numbers.

It's one reason we decided not to produce the card anymore. People will still get their social insurance numbers when they come to the office but when they show up at the office, they receive the social insurance number on a piece of paper. That would be the only thing that we give to them.

Hon. Lawrence MacAulay: Thank you very much. Not to go back to the HRSDC breach but situations like that, I'd just like you to comment. The information was on small hand-held devices. Do you think that's a problem, possibly, that personal information should not be held on devices like that? I'd just like you to comment on that.

Mr. Louis Beauséjour: Clearly, we think that they should not because we changed the way we do our business. Right now, when this type of personal information has to be put on this kind of device, it will have to be encrypted to ensure that the information is protected. One of the first measures that we put in place at the time when we lost the hard drive was to ensure that those devices would not be used anymore and any devices that could be used on the system are devices that are encrypted.

We also implemented the data loss prevention system where we can control what could be copied from the system to a device. We also monitor the devices that are linked or put in any computer within the department.

Hon. Lawrence MacAulay: Breach is related to stolen identity. Could you just elaborate what effect that would have on businesses with any idea what percentage of breaches that take place are connected with that? Possibly not even with theft but loss, but most likely theft I would have to think....

Mr. Louis Beauséjour: I cannot comment on the overall impact of identity theft or on the economy. It's not something we are looking at.

Hon. Lawrence MacAulay: I'd like you to elaborate. It looks like, and it's easy to understand, it's a game of catch-up. Who is doing the catching up is sometimes hard to know. But when you put in the certification training of agents and the SIN code of practice... would you elaborate a bit on the SIN code of practice?

Mr. Louis Beauséjour: Yes, the SIN code of practice is an element where we provide advice to employers, stakeholders, and individuals of what they should do or not do to protect personal information.

One example for employers is that we would recommend they don't use the social insurance number as the employee identifier on their system, and also we would recommend to only put the social insurance number in letters if required, like for a T4. But for other kinds of communication, we would recommend that they don't communicate the social insurance numbers. That would be an example that we put in the code of practice, just to increase their awareness around the importance of protecting the social insurance number, in particular.

● (1135)

Hon. Lawrence MacAulay: Okay.

The SIN is used to identify people. If it hasn't been used in five years, you indicate that something clicks in, in order to.... Is that to investigate what's taken place? Also, is it used in order to detect income tax fraud, or these types of things? I'd be interested to know.

Mr. Louis Beauséjour: I cannot speak about income tax fraud. I think CRA would be a better place to determine the techniques to identify that. But clearly for us, we put the dormant flag because when people are leaving the country—most of the time it's because they are not in the country or they could be active in a war zone—there's an issue of not knowing where they are any more. There's always increased risk as time passes that if that person wants to reactivate the SIN, it could be misused. and because of that, it's one of the things we implement. We begin to put what we call a dormant flag. It's a flag which is on the SIR to indicate that.... In that case, we require that the individual who wants to reuse their social insurance number come to the office to reactivate their social insurance number. That will give us additional assurance that it is the right person who wants to reactivate their SIN. It's to ensure that the right person receives the right benefit.

Mr. Robert Frelich (Director, Enterprise Identity Services Divison, Service Canada, Department of Employment and Social Development): The dormant flag is one of the things that allow the agents to look at additional SIR records, and if it hasn't been used in a long time, it's one of the extra factors they look at when they're agreeing to reactivate a SIN. If there's something that doesn't fall right, if you have an individual who, for example, doesn't correspond with the documents or any of the facts of the situation when they're coming in, then you'll refer it to our national identity centre for investigation.

The Chair: Thank you, Mr. Frelich, and thank you, Mr. MacAulay. That concludes your time, sadly.

We're going to move now to the Conservatives, Pat Davidson. You have seven minutes, Pat.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thanks very much, Mr. Chair.

Thank you, gentlemen, for being with us today on this extremely important venture that we're starting studying.

I just had a couple of things I wanted to ask about from the remarks that you made.

The first one goes back to Mr. MacAulay's question about the dormant status of the SIN card. You say that if it hasn't been active for a period of five consecutive years or more then it can have this dormant flag identifying it. Then you say it's for taxation and those types of things that it's being used for. But then you also said that a child can have one issued at birth. So how is that SIN card used? Kids don't file taxes. What would they be using theirs for? Would theirs always become dormant and have to be reactivated?

Mr. Louis Beauséjour: I will need to follow up specifically on what the process is for. But the reason parents would like to have a social insurance number at birth is to be able to contribute to the student savings account and be able to get the grants associated with it. Basically, that is one of the reasons.

Mrs. Patricia Davidson: So if an RESP is in place, the card is being used.

Mr. Louis Beauséjour: Yes, because it's considered as program use.

Mr. Robert Frelich: Through our vital events linkages with the provinces and territories, when they get a birth certificate from the province, the newborn registration is marked in their SIR record as having been issued as part of the newborn registration process or SIN at birth.

Mrs. Patricia Davidson: Okay. Thank you.

One thing that most of us as MPs deal with is the falsified email communications that go out to our constituents. Often they use email that mimics such official government agencies as Canada Revenue Agency or Service Canada.

Just recently I had to communicate to constituents about this issue, with the phishing scams that were taking place. Could you elaborate on how or whether your departments try to educate the public about these scams?

● (1140)

Mr. Louis Beauséjour: For many years we had information on our Internet site to indicate that Service Canada will not reach clients that way. More recently, we took further steps. We put it more up front, on the first page of the Service Canada website, to ensure that people are aware that they could face phishing scams. It refers them to a more detailed page concerning what they should not respond to and gives examples of potential phishing scams.

But we are constantly playing a proactive role, in terms of putting it up front in our main Service Canada page, to ensure that people are aware that they could face those kinds of scams.

Mrs. Patricia Davidson: Would an individual basically have to go on the Service Canada website to access that information? Is it not available elsewhere?

Mr. Robert Frelich: Actually, one of the contexts in which we've had to deal with attempted phishing scams is the government's Job Bank website. We have put up a number of messages there that say, among other things, that Job Bank will not ask you for your financial information, will not ask for money, and that this is the only validated job site.

The Canadian Anti-Fraud Centre provides a website with things to look for, such as phishing scams, how to prevent fraud and identity theft, among other things.

Mrs. Patricia Davidson: I realize that there probably isn't too much business being conducted by paper mail these days, but if it is in fact, do notices go out that way as well to constituents?

Mr. Louis Beauséjour: I will have to check. I don't think we systematically put an insert in with mailing information about potential phishing scams, but I will look into that to see whether we're doing something on a more systematic basis. My understanding is that we don't do it. In fact, as I said, these days the Internet has become the vehicle of preference to communicate information.

Mrs. Patricia Davidson: Okay.

We all know that it's extremely important to protect the privacy of Canadians. Certainly, as a government we need to protect the privacy of those who are being served by such government departments as Service Canada or Revenue Canada, or any of them.

The Privacy Commissioner made it clear that specific breaches declared as material breaches should be made known to the department.

Can you clarify what a material breach, in your opinion, would be, and how an example would be qualified as a material breach or a more minor type of incident that perhaps wouldn't warrant the specified report to the Privacy Commissioner's office?

Mr. Louis Beauséjour: In fact, this would not be my opinion, but there's an agreement we have in terms of the three characteristics of what is considered a breach that needs to be reported to the Privacy Commissioner.

It's that the information is directly related to personal information that is sensitive, such as financial or medical information, or to a personal identifier such as the social insurance number. It's that there is a risk of identity theft or fraud. And it's if the incident may cause damage to the career, reputation, financial situation, security, health or well-being of the person.

This is the criteria that are used to assess if it is necessary to report the breach to the Privacy Commissioner.

● (1145)

The Chair: That concludes your seven minutes. Thank you very much.

Mr. Andrews was late getting in and has asked permission to interject briefly with one small question. Is there willingness of the committee to allow Scott that latitude?

Some hon. members: Agreed.

The Chair: Go ahead, Scott, and then we'll go to the NDP.

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

I just had an opportunity to go through your testimony.

Are there any restrictions around other organizations asking to use the person's SIN for a way to identify them as a customer or as another...? An outside government agency may use someone's SIN as part of identification purposes for you as a customer, or for another purpose. It's outside of an employer-government relation. It's an outside organization using the SIN. Are there any restrictions on any companies doing that?

Mr. Louis Beauséjour: There is the entity that can use the SIN as an identifier through, I think, the Treasury Board Secretariat, and there are legal limitations as to who can ask and who we can ask to provide the SIN. It's the “don't” part that we advise the client on; don't give your SIN to people who ask for it except if they can legally do so and propose any other means to confirm your identity. People can provide viable licences or there are other kinds of means that they can use. But they should not provide the SIN except if the entity that requires the SIN can legally do so.

The Chair: Thank you, Mr. Beauséjour.

Thank you, Scott.

Next, the NDP are going to divide their time, and we have only time for their five-minute round, and then one more Conservative five-minute round. Then we're going to give some time to change the witness panels, because our next presentation has two 10-minute presentations and it's a shortened period.

Mathieu, you wanted to begin?

[*Translation*]

Mr. Mathieu Ravignat: To start, I would like to present the following Notice of Motion:

> That, pursuant to Standing Order 108(3)(h)(iv), the committee invite the Privacy Commissioner of Canada to discuss her findings in the investigation into the loss of a hard drive at Employment and Social Development Canada.

Thank you, Mr. Chair.

[*English*]

The Chair: So you're just serving notice of an intent.

[*Translation*]

Mr. Mathieu Ravignat: Yes.

I will now give the floor to my colleague, Mr. Giguère.

Mr. Alain Giguère (Marc-Aurèle-Fortin, NDP): Good morning, Mr. Beauséjour.

In your document, you say that the department does not recommend using the social insurance card. However, I looked at my social insurance card, and on the back, it says “Sign your card. Keep it with you.“ Now, you are saying that you don't recommend that people keep it with them. And yet, when you issue this card, you clearly ask them to do so. I see a serious contradiction here.

Mr. Louis Beauséjour: Your card was probably issued a number of years ago, because the new cards say on the back not to keep it with you. It simply shows that, over the years, we realized that we had to change our social insurance number protection practices, given the risk of identity theft when people kept it with them.

I cannot tell you how long ago the cards were changed. Recently, the 50th anniversary of the social insurance number was celebrated. As of this year, the social insurance number has existed for 50 years.

Mr. Alain Giguère: This is a question that is exactly in the same vein as that of my colleague.

I really enjoy your rhetoric, but we are currently proceeding with a supposedly democratic reform which will mean that voters are not allowed to show up with their voter card, but are being asked to show up with their social insurance card so that they can vote.

On the one hand, the Minister of State for Democratic Reform tells us not to use the voter card anymore, but to use the social insurance card instead. On the other hand, you have just informed us that this card will no longer exist. It would be worthwhile for departments to talk to each other from time to time.

It is impossible to use a card for voter identification if it is a going to be phased out soon. There is a problem here.

● (1150)

Mr. Louis Beauséjour: Since the card will no longer exist, this becomes an issue. We will have to follow up on that. I do not know what happened.

Mr. Alain Giguère: You say there is always a risk. That is obviously the case. When a wallet is lost, the social insurance card and other relevant information is also lost, especially the information on a driver's licence. However, 500 000 wallets are not stolen every year in Canada.

As for your department, in one fell swoop, the private information of 500,000 individuals was lost. The scale is not the same. On this front, the Information and Privacy Commissioner indicated that, among all federal departments, only 4.4 % of incidents involving lost information were reported to her.

Don't you think that your priority should be to better secure your internal data transmission networks, rather than tell Canadian citizens to be careful of pickpockets?

I do not believe that 500,000 wallets are stolen every year in Canada. The main source of danger is not that citizens loose their wallets, but that their identity could be stolen. The problem with your department is that it is not always a good custodian of the information that it maintains and protects.

Mr. Louis Beauséjour: As I just mentioned, protecting the private information entrusted to us is our main concern through the entire department. We are constantly trying to improve.

Following the events that you mentioned, we implemented different protection reinforcement measures and we are constantly looking for new ways to reduce the risks associated with the losts of private information.

[*English*]

The Chair: Thank you, Mr. Beauséjour.

Thank you, Mr. Giguère.

That concludes your time, sadly.

Next, for the Conservatives, we have Jacques Gourde.

This will be our final round of questioning.

[*Translation*]

Mr. Jacques Gourde (Lotbinière—Chutes-de-la-Chaudière, CPC): Thank you, Mr. Chair.

I would also like to thank Mr. Beauséjour for the information he is provided to us today.

Personally, I really liked the social insurance card. It gave me a link with the Government of Canada. I asked for my card when I was 16 years old, and I remember that I received it with pride. For me, the card was also a reminder.

Soon, the department will send us our social insurance numbers on a piece of paper. Individuals, especially young people, have a tendency to put letters with their things and to loose them easily.

The department must expect that it will receive many calls to receive that number again. How are you going to be able to offer this service to Canada's entire population?

Mr. Louis Beauséjour: When the social insurance number is issued, we will ask the client to quickly memorize his or her number and to keep the letter that we have sent in a safe place so that he or she can refer to it as needed.

Over the next few months, we will evaluate the situation in order to measure the effects of withdrawing the social insurance card. We don't believe that the effects will be very serious, but we will conduct a very close follow-up with those who communicate regularly with us to obtain their social insurance number repeatedly.

Mr. Jacques Gourde: When are you going to stop issuing the social insurance card?

Mr. Louis Beauséjour: We stopped issuing social insurance cards last Monday. We don't yet know what effect this will have on the network, but we are monitoring the situation.

Mr. Jacques Gourde: I can predict that you are going to have huge problems because currently in Canada, people move more often than they used to. Often, during a move, papers get lost. Young people also move frequently.

I think that you have unintentionally created a monster. I don't want to discourage you. I think members' offices will have more work to do, because people are going to call us to find out what to do to get a new social insurance number. I think that you will have to implement an emergency team because, in a few months, this is going to start.

● (1155)

Mr. Louis Beauséjour: I have made a note of it. As I said, we are going to monitor the effect that this will have on the network. I would imagine that at that time, if there are measures to be taken, we will look at which ones are appropriate.

Mr. Jacques Gourde: You are asking people to memorize their number. At a certain age, it becomes more difficult to remember numbers. Not everybody can easily memorize numbers.

I think that what you are saying is a relatively weak argument to explain this decision.

Mr. Louis Beauséjour: As I said, the individual will be able to refer to the document they have at home. It is clear that this will be an important document that must be kept in a safe place.

The same recommendation is made for the card or the document. It's always been recommended over the last few years not to carry the social insurance card. Therefore, be it the card or the letter, it's exactly the same thing: it must be kept in a safe place.

People have to ensure that they can find it again. It's clear that there is a risk, but this risk has existed for many years. For years, it's been recommended that people not carry their social insurance card with them. Hopefully, they have been following this recommendation, because it puts their identity at risk.

Mr. Jacques Gourde: Have you calculated the number of times that a Canadian has to write their social insurance number on a form throughout a given year?

Mr. Louis Beauséjour: No, I don't know how many times they have to do it. Clearly, there are a certain number of programs that require it. Of course, every time someone finds a new job and has a new employer, they have to provide their social insurance number.

Also, for all federal government programs that offer benefits, the individual must provide their social insurance number. Everything hinges on where the individual might be in their life cycle. Some have the same job for many years and rarely have to give out their social insurance number, whereas others have to do it frequently.

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Thank you, Mr. Gourde. That concludes your time. That's perfect.

Thank you very much, Mr. Beauséjour and Mr. Frelich, for joining us today. It's been very helpful.

We're now going to suspend the meeting briefly while we get a new panel of witnesses. I'd like to suggest that committee members take this opportunity to get themselves some lunch. We'll reconvene in about five minutes.

● (1155)

(Pause)

● (1200)

The Chair: We'll ask our witnesses now to start their presentations.

I understand that we have representatives here from two departments, the Department of Citizenship and Immigration and the Department of Industry. Both would like the opportunity to make brief, five- or ten-minute opening remarks. We'll certainly provide that.

But we should also be aware, committee members, that we need five or ten minutes at the very end of the meeting to give the clerk some direction on future witnesses. So we may have a limited number of speaking opportunities for questioning the witnesses.

Having said that, we're going to welcome, from the Department of Citizenship and Immigration, Mr. Lu Fernandes, director general of the passport program integrity branch.

Mr. Fernandes, I understand you'll be giving the briefing on behalf of your department. Please go ahead, sir.

Mr. Lu Fernandes (Director General, Passport Program Integrity Branch, Department of Citizenship and Immigration): Thank you very much.

Mr. Chair and committee members, thank you for the invitation to appear before you. We are pleased to contribute to your efforts to gain a better understanding of identity theft in Canada.

My name is Lu Fernandes. I am the director general of the passport program integrity branch at Citizenship and Immigration Canada. I'm accompanied today by Peter Bulatovic, director of the investigations division of the passport program integrity branch.

With more than 5 million applications a year and approximately 23 million valid Canadian travel documents in circulation, our passport is truly one of the most recognizable symbols of Canadian citizenship around the world. We share the concern that these documents should only be issued to Canadian citizens who are entitled to hold them.

[*Translation*]

By way of background, I should note that effective July 2, 2013, the Minister of Citizenship and Immigration Canada assumed overall accountability for the Passport Program. This includes issuing, refusing to issue, revoking, withholding, recovering, and providing instructions on the use of Canadian passports. The minister is also responsible for providing guidance to missions issuing passports abroad and supervising all matters relating to Canadian travel documents.

On that date, the delivery of the domestic services under the Passport Program came under the responsibility of the Minister of Employment and Social Development Canada, while the Department of Foreign Affairs, Trade and Development continues to provide passport services to Canadians abroad.

[*English*]

This move to CIC places the passport issuance at the end point in the continuum of services provided by a department that facilitates access to those who wish to visit, study, work, immigrate, and ultimately become Canadian citizens. It also places the domestic delivery of these services in the hands of the government's service delivery arm, Service Canada.

● (1205)

[*Translation*]

As we continue to modernize the Passport Program, these changes also provide opportunities to take advantage of existing technology investments, such as the CIC Global Case Management System, and leverage the extensive network of Service Canada offices across the country.

I would now like to spend few minutes speaking about the direct responsibilities of the Passport Program.

[*English*]

July 1, 2013, marked the launch of our electronic passport, or ePassport, as well as the inauguration of Canadians having the choice to apply for a five-year or ten-year validity passport. The new ePassport meets the latest international norms set out by the International Civil Aviation Organization, which represents the gold standard for travel documents.

The electronic chip embedded in the ePassport adds an additional layer of security to guard against identity theft. The chip stores the information found on page 2 of the passport, including the bearer's photo, providing border control personnel with an additional tool to validate the passport holder's identity. By accessing the information on the chip and comparing it with the information on page 2 of the book, a border agent can ensure that the information or photo has not been modified.

The design of the visa pages in the ePassport provides another layer of security, making the book more difficult to counterfeit. The pages are made up of unique pairs of vignettes that depict recognizable themes, places, and persons in Canada's history. The different images on each page, along with a variety of visible and invisible security features, make it very difficult and extremely expensive for counterfeiters to reproduce a book or substitute a page.

[*Translation*]

The Passport Program's commitments to protecting the security and integrity of Canadians travel documents is crucial to maintaining their international acceptance and facilitating extensive visa-free travel for Canadians worldwide.

Supporting the integrity of the documents themselves is the Passport Program's strict regime for determining identity, eligibility and entitlement to a passport. First-time passport applicants 16 years of age and over are required to submit an application form along with authenticated photos, proof of Canadian citizenship, supporting identity documents and a guarantor declaration.

[*English*]

Individuals who are already in possession of a Canadian passport can use the simplified renewal process. This involves a shorter application form and requires the applicant to submit their previous passport and new photos. Proof of citizenship, supporting identification, and guarantor support are not required as the passport program already has this information on file.

Before a passport is issued, various processes are applied to authenticate identity. The passport program uses a combination of trained officers and technology to verify applicant identity.

At the time of application, personal information, photos, and signatures are manually compared with information provided in previous passport applications, documentary evidence of citizenship, and supporting identity documents.

Facial recognition software is used to compare photos of every applicant against the database of all passport holders to counter attempts at identity fraud.

Other automated verifications include comparison of personal information with the program's central database and against the program's watch-list.

Where the applicant's identity is in question, additional verifications may be completed, such as guarantor, reference, and occupation verifications, validation of citizenship and identity documents, or Canadian Police Information Centre, CPIC, queries. In fact, there is a daily electronic exchange with Correctional Service Canada to obtain details about federal offenders.

[*Translation*]

The Passport Program works closely with other government departments, law enforcement and intelligence partners for the refusal and revocation of Canadian passports when necessary.

For example, travel documents are canceled for persons who are incarcerated or have other mobility restrictions. An individual who is charged or convicted of a serious offence, or who owes child support can have his or her passport revoked and can be refused passport services.

● (1210)

[*English*]

The passport program also has the capacity, within the passport program integrity branch, to conduct administrative investigations to determine ongoing entitlement to a passport or entitlement to future passport services.

Individuals who have been refused a passport or whose passport has been revoked may challenge the decision taken by this program through judicial review before the Federal Court.

The passport program continuously reviews its policies and procedures to ensure they meet evolving standards and program integrity requirements. We are committed to leveraging technology and working with other government departments, provincial vital statistics agencies, international partners, and law enforcement agencies to counter attacks against the passport program and limit any opportunities for identity theft and fraud.

Of course, Canadians must do their part in guarding against identity theft by keeping their travel and other important documents safe and by protecting against unnecessary disclosure of personal information.

[*Translation*]

I hope that these remarks have given you some insights into the Passport Program identity authentication and fraud prevention activities.

We would now be pleased to take your questions.

Thank you.

[*English*]

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

We'll hold off on the questions, though, until we have our other briefing and presentation from Mr. Michael Jenkin, the director general of consumer affairs in the Department of Industry.

Mr. Jenkin.

Mr. Michael Jenkin (Director General, Office of Consumer Affairs, Department of Industry): Thank you, Chair.

Thank you for the invitation to speak to you today regarding identity theft.

As you mentioned, I'm the director general of the office of consumer affairs, which is a part of the strategic policy sector at Industry Canada.

[*Translation*]

I would like to discuss a number of the activities and initiatives that the department is involved in with a view to protecting consumers in regard to identity theft.

[*English*]

I will begin my remarks by touching upon the Personal Information Protection and Electronic Documents Act, and describing how this law helps to protect Canadians from identity theft. Secondly, I'd like to briefly discuss certain elements of Canada's anti-spam legislation, a law for which a number of federal actors are responsible. Finally, I'll touch briefly on certain information initiatives with which my office has been involved, including initiatives to help with public awareness in connection with the implementation of the anti-spam legislation.

First, I'd like to turn to the Personal Information Protection and Electronic Documents Act, or PIPEDA, as we call it. This law sets rules for the collection, use, and disclosure of personal information by private sector organizations, such as banks or phone companies, in the course of commercial activity. While the Minister of Industry is responsible for the law, it's the Privacy Commissioner of Canada, operating at arm's-length, who is responsible for enforcing and administering the act. As such, I would defer to the Privacy Commissioner for any issues respecting application of the law. That said, I will take a few moments to provide a brief overview of the act and how its requirements help to address identity theft.

[*Translation*]

The rules are based on 10 international and recognized principles for how organizations should best manage the personal information of their clients and customers. Many of these rules help protect consumers against threats like identity theft.

[*English*]

For example, the act requires that organizations only collect the information they need and retain it only for as long as necessary, to make sure that they are not maintaining databases of personal information that are not necessary and that would be vulnerable to loss or theft.

The act also requires that organizations put in place appropriate security safeguards to protect the personal information they hold against unauthorized access, loss, or theft. Such security measures, including the use of passwords or encryption of consumer data, help prevent the loss of personal information that is being used in identity theft.

In response to the first parliamentary review of PIPEDA, the government has committed to amending the act to create a new requirement for organizations to notify individuals if their personal information has been involved in a potentially harmful data breach. These amendments would ensure that consumers are informed when their personal information has been lost or stolen and would give them the information they need to protect themselves against identity theft, fraud, financial loss, or other forms of harm. The government remains committed to making these amendments, along with other changes recommended by Parliament in the first review.

I will now turn briefly to Canada's anti-spam law.

● (1215)

[*Translation*]

The law prohibits sending commercial electronic messages without consent. It also prohibits the installation of software on an other person's computer without consent. Together, these new prohibitions address nuisance spam messages.

[*English*]

Major concerns that the new law is intended to address include phishing messages, which are designed to lure recipients to counterfeit websites and trick them into revealing personal information, such as usernames, passwords, and account information; malware, which involves the installation of software on a person's computer, smart phone, or other digital device without their knowledge or consent—these types of spyware and viruses can secretly collect personal information that is then used in identity theft activities—and finally traffic rerouting, which involves secretly redirecting a person's online searches to a malicious destination where attackers can collect personal information for the purposes of carrying out identity thefts.

Most of the act will come into force on July 1 this year. Once the law is in force, it will help to protect Canadians while ensuring that businesses can continue to compete in the global marketplace. On January 15 of next year, sections of Canada's anti-spam legislation related to the unsolicited installation of computer programs or software will come into force. And then, the act's private right of action provisions will come into force on July 1, 2017. CASL will be enforced by the Canadian Radio-television and Telecommunications Commission or CRTC, the Competition Bureau, and the Office of the Privacy Commissioner.

The CRTC will enforce the law in respect to violations related to sending commercial electronic messages, altering transmission data, and installing computer programs without consent.

The Competition Bureau will investigate and take action against false and misleading representations and deceptive marketing practices.

The OPC will investigate the collection of personal information through illegal access to computer systems and electronic address harvesting.

[*Translation*]

I should note that a key element of the government's approach is preventing problems from occurring in the first place, and a key way to do that is to ensure that Canadians understand how to protect themselves. With this in mind, the government has set up a website, called www.fightspam.gc.ca, or www.combattrelepourriel.gc.ca.

[*English*]

In English it is www.fightspam.gc.ca.

The website includes information about the law itself and provides a number of information resources to Canadians. The website will also serve as the online home for the spam reporting centre, through which Canadians will be able to report on commercial electronic messages that have been sent without consent and commercial electronic messages with false or misleading content.

[*Translation*]

I would note, in addition, that a web-based advertising campaign has begun that will inform Canadians about the July 1 coming into force, and invite them to visit www.fightspam.gc.ca. You will find the introduction page from that website in your folders, as well as an image of the “Mobile Protection Tool Box.”

[*English*]

My own branch, the office of consumer affairs, has been involved in preparing communications efforts in respect of CASL. You will note in your packages, in your information kits, a series of infographics. The first, *Worried it's SPAM? 5 Things to Look for*, is geared to consumers to provide them with the basic information they need to avoid being taken in by fraud artists. It does so by setting out a number of common techniques used by spammers to obtain consumers' personal information. The infographic was printed and has been distributed to a large number of stakeholders, including other federal departments, provincial governments, with which we work quite closely on the consumer side, and community organizations.

The next three infographics in the kit, *Does Canada's New Anti-Spam Law Apply?*, *4 Tips for Contacting Clients Electronically*, and *3 Things to Think About When Sending Messages*,were created to help small and medium-sized enterprises know the basic requirements of the legislation and avoid being mistaken for spammers. These infographics, along with *Worried it's Spam?*, the one I just referred to, have been posted on the fightspam.gc.ca website and shared via the Industry Canada Twitter account.

● (1220)

[*Translation*]

Finally, an additional item in your packages is called the I.D. theft checklist.

[*English*]

In English, it is *Identity Theft: A Checklist*.

[*Translation*]

The list was prepared in collaboration with provincial and territorial officials and was distributed widely in recent years.

[*English*]

In conclusion, as I have noted, the government has taken a number of legislative measures aimed at protecting Canadians from identity theft. At the same time, an important part of the puzzle is awareness and education to ensure that Canadians have the right information they need to protect themselves.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Jenkin. That's very helpful.

Given the time limitations, we're going to do our first round of seven minutes per. That would be the official opposition, Conservatives, Liberals, and Conservatives, and then we'll call it a day. We need to do some in camera future planning as well.

Beginning without delay, then, we will go to Mr. Ravignat, for seven minutes, please.

[*Translation*]

Mr. Mathieu Ravignat: Thank you, Mr. Chair.

I would like to thank the witnesses for being with us today. It was very kind of them. It is always important for Canadians to have a chance to hear them.

My first question is for the representatives of the Department of Citizenship and Immigration.

In response to a question on the *Order Paper* from my colleague, Mr. Charlie Angus, you indicated that there had been 174 breaches of data that had affected 246 Canadians between 2002 and 2012. We haven't heard any more details on that subject. I was wondering if you could tell us more about the nature of those breaches of data.

Mr. Lu Fernandes: Thank you for the question.

[*English*]

As the person responsible for the passport program integrity branch, I am not able to answer the question you referred to. I am not certain if that's passport related or is with Citizenship and Immigration Canada.

[*Translation*]

Mr. Mathieu Ravignat: Fine.

Following a question in the *Order Paper*, we were told that it was impossible to obtain the number of breaches of data within your department.

In your opinion, is there a particular reason for the lack of information on this subject? Are there shortcomings in terms of the way in which your department apprehends these data breaches? Could you provide us with details on this subject? For example, is there a system that manages cases of data breaches?

Mr. Lu Fernandes: With all due respect, I cannot answer any more questions that have to do directly with the loss of data.

[*English*]

I can speak specifically to the passport program and passport program integrity.

Mr. Mathieu Ravignat: Well, then, within passport integrity, is there a system in place to manage the loss of sensitive data?

Mr. Lu Fernandes: In terms of responding to losses of data, it would be the regular processes and policies that would be in place to inform the Privacy Commissioner's office and/or the individual, depending on the situation.

Again, I am responsible for the integrity of the passport program itself and the security of the document and the security of the issuance and entitlement process.

● (1225)

Mr. Mathieu Ravignat: My next question would be for Mr. Jenkin.

The work you've done on spam is interesting. It's some of the only work I know of that the government has done to renew its protection of privacy information. The act hasn't been reviewed since Facebook and Twitter were created. It seems to me that you might have some interesting input to give as to the modernization of the protection of privacy legislation and framework that we have.

Would you like to comment on how you would see a more robust set of rules in place to protect the privacy of Canadians in a digital world?

Mr. Michael Jenkin: With respect, Parliament has already done a review of the act and has delivered its views, and the government will be responding to those shortly. I think we need to get that process of reform under our belts before we look at new threats or new problems or new issues with respect to identity theft.

It is a very fast-moving area, and it is difficult to keep up sometimes with a phenomenon that literally.... This is a problem one gets generally with fraud issues more broadly; that there is constant innovation going on to try to find new ways to compromise people's identity and to use it for ill gain.

Right now, I think what we would like to do is get this next phase of the work completed and then address what the future issues would be that both Parliament and the government think are important.

I could list off, and I'm sure you could as well, a number of potential problems that are emerging. One of the problems with this area is needing to allow a certain amount time whereby we can see how these things settle out and determine the longer-term structural problems we need to address when faced with a highly innovative and constantly changing environment like this.

So as I said, right now I think the key priority is to get on with the government's own intentions to reform the act and to provide Canadians with more opportunities in that context to protect themselves.

The Chair: Your time is pretty much up; there are about 10 seconds left. But I would like to clarify, perhaps, Mr. Jenkin's response.

The PIPEDA act is up for review. It was due to be reviewed about two years ago. It was reviewed once about seven years ago, and the government's response to that review was Bill C-28, which died on the order paper, and Bill C-12, which died on the order paper. So if there was a government response, none of those elements was ever implemented; the act was never amended or changed.

I don't want Mr. Ravignat to think that a review led to amendments to the act. It did not.

Or did you mean something else?

Mr. Michael Jenkin: No, I simply meant to say that the government is on the record to say that it will be reviewing the act in due course, and that date is yet to be determined. But the government is on record to say that it is intending to amend it.

The Chair: And this committee is on record as having written the minister asking for that review to take place.

Next, for the Conservatives, we have Mr. Zimmer.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you for appearing before our committee today.

My first question is for Mr. Fernandes.

I wanted to ask how Canada's passport program ranks globally. Are we the best? Are we the worst? Where do we rank in terms of what you're here for, and that's security? Where do we rank in the world system?

● (1230)

Mr. Lu Fernandes: Thank you.

I'm very pleased to say that among our equivalent five nations or partners, as we call them—these would include the United States, the United Kingdom, New Zealand, Australia, and ourselves—we are in the range of where those organizations are with regard to the document itself. We have a very secure document, in the world rankings, and it's an excellent book as far as the security of the document itself goes. It allows Canadians access to approximately 140 countries visa-free.

That's because of the document, but also because of the entitlement process and how we ensure that there is security in the identification of the individual and in the entitlement decision that is made to give somebody a Canadian passport. The proof really speaks in the visa-free status to so many countries around the world that Canadians have access to.

Mr. Bob Zimmer: The department has issued the new ePassport. We've just seen it over the last number of months, I believe. Can you explain the difference between the new ePassport and its different security items or security offerings and what we had before?

Mr. Lu Fernandes: Certainly, I'd be happy to.

The ePassport is an increased and enhanced level of security in the book itself, with the chip that is embedded in the back cover. The chip includes the information that is found on page 2 of the book, including the photograph.

So biographic information and the photograph are stored inside the chip. The additional security that this provides for border agents is that they can access the chip, take a look at the information, and ensure that it is in fact exactly what you would expect to see in the book on the second page. With the individual standing there in front of them, they have a third point of reference: the individual, the photo, and the photo on the chip. That would provide the additional levels of security. That's what the e-chip is about.

As to the book itself, if you don't have a new ePassport yet, your current book has on the visa pages a number of maple leaves in sequence through every single page. The new book has vignettes on every single double set of pages.

If I may have your indulgence for a second, you can see, where I am pointing, the ultraviolet features on the pages themselves. Every single page has embedded visible and invisible security features that provide additional layers of security that you won't find in the types of security features that are in the current book.

Mr. Bob Zimmer: My next question, or last to do with passports—I'll have some more questions for Michael in a minute—is this. We have had credit cards stolen or lost or whatever, and the process we go through is that we phone the bank and say that our card has been lost or stolen, and they reissue a new card with a new number. If somebody takes our passport or our passport goes missing, what similar types of security offerings do you have that can protect our identity and protect our person from misuse?

Mr. Lu Fernandes: The lost—and/or stolen, in many situations—replacement process is quite different from the credit card process. We have about 66,000 lost and stolen passports reported to us annually. Canadians domestically and around the world report lost or stolen passports. Often, it's that individuals have forgotten where they put them, have just misplaced them, or in a move have no idea which box they might be in, and they report them as lost.

Once that information reaches us in the passport program integrity branch, we automatically and immediately cancel the book. We also then, within a 24-hour period, notify our partners that the book has been declared lost or stolen and has been cancelled in our system.

We advise the CBSA daily of that information. We also advise the Canadian Police Information Centre, CPIC, which is managed by the RCMP so that all police organizations have access to that information. On a daily basis it's updated. It's subsequently updated from CPIC to Interpol, and that's through the RCMP linkage with Interpol. So around the world that information is passed along into the Interpol database.

This all happens immediately, within a day. As a result, when an individual misplaces a book and says, “I can't find my book, I must have lost it” and then comes back to us and says, “Sorry, I found it”, we advise them very clearly that they cannot use the book, because while we might be able to change the status of the book as being in the hands of the holder, all of our partners have already been informed that the book has been cancelled.

So they cannot use that book, or they will risk, if they do use it, being stopped at a border. Then they have to come back in and do a whole application for a new book.

Thank you.

● (1235)

Mr. Bob Zimmer: Chair, do I still have some time?

The Chair: No, I'm sorry, Mr. Zimmer, you're out of time. Thank you.

Next, then, for the Liberals, is Mr. Scott Andrews.

Mr. Scott Andrews: Thank you.

I may get back to that question, if I have time, but I'd like to ask a couple of other questions.

Do you keep statistics on how many people you catch applying for a passport who are not who they say they are? What kind of statistics might you have on people who apply for a passport and you catch for not being who they say they are?

Mr. Lu Fernandes: Last year, we refused or revoked approximately 1,370 passport applications. Of those, about 1,000 were refused or revoked for reasons of criminality. These would have been for individuals who were incarcerated and who, from their point of incarceration—prison or jail—would have applied for a passport, or individuals who, subsequent to being incarcerated, had mobility restrictions applied. The great number of these 1,370 or so cases—1,000 of them—are from this group, this population.

Out of the total number, we have about 70 individuals who were refused or revoked passports on the basis specifically of identity fraud.

Mr. Scott Andrews: Okay. What happens to those 70? Are they referred to the RCMP, or what is the process for those cases? And what is the most common reason or what documents or whatever else are these people using to try to steal this identity? They are providing you with documents to prove who they are.

Do you understand my two questions there?

Mr. Peter Bulatovic (Director, Investigation Division, Passport Program Integrity Branch, Department of Citizenship and Immigration): Yes.

In many cases, they have stolen the actual documents of an individual, be it a citizenship paper, a birth certificate, or a health card. They've actually stolen those documents and used them to apply for a passport.

Mr. Scott Andrews: And what is the process for those 70 individuals, when you catch them doing this?

Mr. Peter Bulatovic: What happens in that process is that the application is stopped at the time the person applies, and we commence an investigation of the individual. The individual is advised that he or she is under investigation and is notified by a letter advising them that we cannot proceed with the passport application.

At the point when it comes to the identity theft part, in many cases that's the last we hear of the individual, obviously, and so the investigation stops at that point.

Mr. Scott Andrews: Is it reported to the individuals trying to pass off that identification that the pieces of information are stolen?

Mr. Peter Bulatovic: No, actually they are not advised, because the difficulty we have is that we don't know exactly how the documents were stolen. We don't know how the individual came into being in possession of those documents. In fact we don't know if the documents were linked to a friend of this individual whose identity was stolen. So it's a very grey area for us.

● (1240)

Mr. Scott Andrews: Would you refer that to the RCMP—this attempt by someone to represent someone they're not?

Mr. Peter Bulatovic: We would.

Mr. Scott Andrews: Do you know what the RCMP does with that once you...?

Mr. Peter Bulatovic: You would have to ask the RCMP that. It's a matter of whether they have the capacity to investigate single identity thefts.

Mr. Scott Andrews: Then at the end of it, you realize it...these 70 people and you pass it off to the RCMP and that's the end.

Mr. Lu Fernandes: Actually in a number of these cases where there is in fact an administrative investigation that happens within the branch, we can conclude the investigations ourselves. The most serious cases of identity fraud or theft we would refer to the RCMP.

Mr. Scott Andrews: How often do you revoke a passport that has been issued, once you realize the person got it using identity that wasn't theirs?

Mr. Peter Bulatovic: That would be the case for the 70 that the director general Lu Fernandes referred to.

Mr. Lu Fernandes: Those would be part of the 70 that we would have come across.

Mr. Scott Andrews: Okay, but how many actually got a passport and how many did you stop in their tracks?

Mr. Lu Fernandes: I'm sorry, I don't have the breakdown of that number.

Mr. Scott Andrews: Okay. You say the common part of this was that people had stolen the documents to present to Passport Canada. Do you come across people trying to pass off forged documents to Passport Canada to try to obtain a passport?

Mr. Peter Bulatovic: Yes. During investigations we do.

Mr. Scott Andrews: Is that common?

Mr. Peter Bulatovic: Forgery is quite common.

Mr. Scott Andrews: How do we protect against that? Is there anything that would help us protect against that?

Mr. Peter Bulatovic: From our perspective, one of the big investigative tools we use is facial recognition. When someone applies for a passport, the minute they apply for a passport their picture is run against all the pictures we have in our database. That's probably the first line of defence, if you want, in terms of passport fraud. In many of these cases, for example, the individual is applying using an identity that we already know. So we know that this person is trying to obtain a passport using a valid identity that we already know.

In other cases, especially with first-time applicants, we carefully look at the documentation and if we think there's something not right there.... For example, someone whose criminality is known to the police universe could be on our systems lookout list, so we may get a hit on the systems lookout list and we will look at that. In that instance, the passport application is not processed initially but instead comes to the investigation division for a second look.

The Chair: You have 30 seconds, Scott.

Mr. Scott Andrews: You mentioned about 1,370 and you said 1,000 were the criminal aspect and 70 were the other one. What were the other 300? Do you have a little breakdown?

Mr. Lu Fernandes: I do. About 225 were for entitlement fraud or passport misuse. Allowing somebody else to use their passport, for instance, would be an example of that. Of the total number, 36 were for citizenship issues, so the individual was not in fact a citizen of Canada.

Mr. Scott Andrews: Thank you.

The Chair: Everybody has concluded.

Thank you, Scott.

Next and finally will be Tilly O'Neill Gordon for seven minutes.

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

I want to thank all of you for taking time to be with us today.

This is my first time on this committee, and I look forward to the information and what this study will bring forth. Your presentation here today certainly gave us lots of information. It's information we often think about but I guess we never follow up to see just how it all ends up.

It certainly is of great benefit to all of us here today to know that Canada ranks so highly on the stage of security and with other countries as well. That was a key factor to hear as well.

Someone already asked this, but I was just wondering. You talked about the capacity within the passport program integrity branch to conduct administrative investigations to determine ongoing entitlement to a passport or entitlement to future services. You mentioned some of the many reasons an individual can be refused a passport. You talked about incarceration and other ideas. But once they have lost their passport, how long will they have lost it for? How do they go about getting it back, or do they ever get it back?

● (1245)

Mr. Peter Bulatovic: I can answer that question.

The withheld service period that is usually imposed on individuals is five years from the date of the incident. We take administrative investigations very seriously.

We know there's a charter right to travel. Canadians have a charter right to travel, so even while they're on withheld service during that five-year period, we let the individual apply for a one-time passport to visit a relative in another country for urgent, compelling, compassionate reasons. They can have as many of those as they want during that withheld period of service; they just can't have a permanent passport for a five-year period.

We're quite cognizant of the fact that individuals still need to travel, and we do approve urgent, compelling, compassionate passport applications, but usually it's a five-year period of withheld service.

Mrs. Tilly O'Neill Gordon: I was happy to hear you say as well that with this new ePassport the security is so much higher. Is this the only kind of passport that's going to be distributed now? Everyone who applies from here on in will be getting an ePassport?

Mr. Lu Fernandes: Yes. The ePassport is the only passport that's available to Canadians as of July 1, 2013. The only difference is the choice in terms of the validity period of the passport: either a five-year passport or a ten-year validity passport.

Mrs. Tilly O'Neill Gordon: Yes. So now do they have to go into an office and apply? Because a lot of people would not have.... Or do they apply on their own computers?

Mr. Lu Fernandes: You can actually go to the website, the Passport Canada website, and fill out a form online, but currently you have to print it and then either take that form to an office or mail it in to Passport Canada, or take it into one of our Service Canada receiving agents or Canada Post.

Mrs. Tilly O'Neill Gordon: So they wouldn't absolutely need a computer or computer skills. They could go into an office and still have their service that way.

Mr. Lu Fernandes: Absolutely.

Mrs. Tilly O'Neill Gordon: I was just wondering what's best for Canadians to do to combat these phishing messages, the malware, and the traffic rerouting, because we certainly are seeing that happen more and more every day with these great technical things that we have in technology now. I'm wondering what more we can do as Canadians to prevent this.

Mr. Michael Jenkin: Well, in your package here, we have a number of suggestions about what you can do to protect yourself online, particularly with things like phishing tactics and so forth.

The biggest piece of advice, I think, is to be very careful. The fundamental issue is this: don't reveal personal information online unless you understand very carefully who it is you're dealing with. If it's someone who you know and trust, then that's one issue, but certainly most respectable businesses and institutions do not request that you send in valuable personal information cold, online.

Unfortunately, criminal practitioners in this area often do prey on these kinds of emotional appeals. For example, the typical kind of stratagem is an email that you would receive that would look very official, from a bank, for example, saying that there's been some problem with the security of your account and asking you to contact them online. When you contact them online—or even in some cases, phone them, but certainly contacting them online—you're asked to present personal information. Banks never do that.

So really, it's about being extremely careful about situations in which you provide your personal information. You do that only in circumstances where, for example, you're applying legitimately for a piece of identification, or a credit card, or some other situation. But the point is to be very aware of out-of-the-blue, unsolicited inquiries and entreaties to engage with somebody, in the course of which you're asked for some kind of sensitive personal information. That's when you always need to be careful.

In other words, if you initiate it yourself, that's fine. You want to apply for a credit card and you go to a bank, you fill in a form, and so forth. But when someone contacts you out of the blue, even when it is the bank, and says that something's gone wrong and they need your personal information, don't respond to that. Go directly back to the institution yourself and inquire with your own bank branch, for example, if there is a problem, because you need to be very careful when people ask for personal information out of the blue. That's the bottom line here.

● (1250)

Mrs. Tilly O'Neill Gordon: More and more we need to get that message out on how we can make people listen to that and not jump at the first thing because sometimes people just become nervous or curious as to what went wrong with their banking and automatically give the information that they shouldn't. So that's a very important message we need to get out more and more.

The Chair: Actually, you are out of time, so sorry, Tilly.

Thank you very much.

Thank you to all of our witnesses. We are going to conclude our questioning with that.

Mr. Fernandes, Mr. Bulatovic, and Mr. Jenkin, it was very helpful and we may in fact need some more input from you as we proceed with our study, but we'll certainly call on you if we do.

I'm going to suspend the meeting briefly, then, and we'll reconvene in camera just for five minutes or so.

The meeting is adjourned.

[*Proceedings continue in camera*]