HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 017 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, April 3, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 3, 2014

● (1100)

[*English*]

The Vice-Chair (Mrs. Patricia Davidson (Sarnia—Lambton, CPC)): Good morning, everyone. We'll call the meeting to order.

I welcome our witnesses for this morning's presentation.

We have with us from the Royal Canadian Mounted Police, Superintendent Jean Cormier, director, federal coordination centres, and Inspector Cameron Miller, federal coordination centres, domestic region.

From the Department of Industry, we have Thomas Steen, major case director and strategic policy adviser, Competition Bureau, fair business practices branch, and Mr. Morgan Currie, acting assistant deputy commissioner of the Competition Bureau, fair business practices branch, division C.

Without further ado, we will open it up to our witnesses for their opening statements, starting with the Royal Canadian Mounted Police.

Go ahead, Mr. Cormier.

Supt Jean Cormier (Director, Federal Coordination Centres, Royal Canadian Mounted Police): Good morning, Madam Chair, and honourable members of the committee. Thank you for inviting the RCMP to participate in today's proceedings.

l am accompanied by Inspector Cameron Miller, who is the officer in charge at RCMP National Headquarters. He is responsible for the oversight of the operations and administration of the Canadian Anti-Fraud Centre, referred to as the CAFC.

[*Translation*]

The CAFC is a joint partnership between the Ontario Provincial Police, the Competition Bureau and the RCMP, and plays a crucial role in educating the public about mass-marketing fraud.

[*English*]

l am pleased to be accompanied by one of those partners, the Competition Bureau, represented by Mr. Morgan Currie, assistant deputy commissioner, fair business practices branch, and Mr. Thomas Steen, major case director and strategic policy adviser, fair practices branch as well.

[*Translation*]

I am pleased to have this opportunity to be joined by my colleagues here today and say a few words about the RCMP, our involvement in the CAFC and our role in addressing identity theft, along with our partners.

Identity theft is a serious matter with serious consequences.

[*English*]

Criminal groups exploit technological advancement to compromise personal information for illicit purposes. While identity theft is not new, the scope of the problem has grown substantially. Sophisticated groups are able to compromise entire computer networks, infect multiple individual computers, or design fraudulent websites to mine personal data on a massive scale.

Millions of personal records can be obtained through one targeted cyberattack. Identity theft has evolved from impersonating one or another person to the creation of totally synthetic identities. Criminals utilize personal information stolen from various individuals to obtain legitimate identification in a fabricated name, a synthetic identity, that is. Synthetic identities can then be utilized for a number of illicit purposes such as fraud, industrial espionage, money laundering, and terrorist financing.

● (1105)

[*Translation*]

Over the past decade, the unprecedented rise in crime associated with personal identity information has made this type of crime a primary concern for Canadians.

[*English*]

The impact of identity crime on victims is unlike that of other crimes. An individual's identity is the basis of almost every aspect of modern life, and when it is compromised, victims often suffer long-term consequences. Apart from economic or financial losses, there is often damage to reputation, loss of access to credit and other services, and in some cases, victims even face criminal prosecution for acts committed by others utilizing their names.

Another key concern is the increased involvement of organized crime groups in identity crime. These groups operate across national and international borders to evade detection and prosecution by law enforcement.

Consequently, identity crime is often multi-jurisdictional, crossing municipal and provincial boundaries. Globalization and the absence of cyberborders means that many cases have international links and implications, making it that much more complex.

[*Translation*]

In 2010, the Government of Canada recognized the growing seriousness of identity crime by amending the Criminal Code with the addition of offences specific to identity crime. In 2012, the RCMP, in consultation with private and public sector stakeholders, developed its national identity crime strategy.

[*English*]

To put the scale of the problem into context, consider the following.

In 2013, the RCMP opened 3,411 occurrences related to identity theft and fraud. For the same year, Norton, operated by Symantec, a security, storage, and system management solution provider, estimated that $113 billion was lost globally to cybercrime and that Canada's share was approximately $3 billion. Over 24,000 victims of identity crime contacted the CAFC to report losses in that same year, to a total of $11 million.

In 2012, Symantec reported that an average of 604,826 identities were stolen per data breach, which means over 93 million identities were exposed. An example of that is the targeted attack on Target Corporation which resulted in the payment card information of 100 million customers being compromised.

These figures highlight the importance for law enforcement to work collaboratively with domestic and international partners to prevent, detect, and pursue those who engage in such activities.

[*Translation*]

We believe that information sharing between the different domestic partners, Government of Canada departments and the RCMP, as it relates to preventing identity theft, is crucial to addressing the problem.

[*English*]

The aim is to educate, prevent, detect, and deter such criminal activity as well as to facilitate the investigation and prosecution of those involved in such criminal activity.

[*Translation*]

Identity theft directly impacts individuals, businesses, communities, Government of Canada and international reputations.

● (1110)

[*English*]

Education on how to protect one's identity is everyone's responsibility.

[*Translation*]

Although many Canadians are now aware of the different methods utilized by criminals to steal their personal information, continued vigilance is paramount.

[*English*]

The RCMP is committed to protecting Canadians' financial well-being by continuing to contribute to efforts to detect and deter identity theft and the use of victims' identity to perpetrate fraud.

[*Translation*]

I thank you for your interest on this concern.

We look forward to answering your questions.

[*English*]

The Vice-Chair (Mrs. Patricia Davidson): Thank you very much, Inspector Cormier, for your remarks.

Now we're going to be hearing from Mr. Currie.

Mr. Morgan Currie (Acting Assistant Deputy Commissioner of Competition, Competition Bureau, Fair Business Practices Branch Division C, Department of Industry): Thank you, Madam Chair, for the invitation to speak to you today about identity theft.

My name is Morgan Currie and I am an assistant deputy commissioner in the fair business practices branch, which is an enforcement branch of the Competition Bureau part of Industry Canada.

I am accompanied by my colleague, Mr. Thomas Steen, major case director and strategic policy adviser in the fair business practices branch. Mr. Steen established and is responsible for overseeing the bureau's enforcement regime to counter mass marketing fraud, or MMF, which we're here to discuss today. We're also very pleased to be here today with our partner, the Royal Canadian Mounted Police, which is represented by Superintendent Cormier and Inspector Miller.

I will begin my remarks by describing the mandate and role of the Competition Bureau. Then I will discuss our enforcement work to combat mass marketing fraud. Finally, I will touch upon partnerships that the bureau is involved in that help strengthen enforcement initiatives in the area of mass marketing fraud.

[*Translation*]

The Competition Bureau, as an independent law enforcement agency, ensures that Canadian businesses and consumers prosper in a competitive and innovative marketplace. Headed by the Commissioner of Competition, the bureau is responsible for the administration and enforcement of the Competition Act, the Consumer Packaging and Labelling Act (except as it relates to food), the Textile Labelling Act and the Precious Metals Marking Act.

The basic operating assumption of the Competition Bureau is that competition is good for both businesses and consumers.

[*English*]

The bureau will also be responsible for enforcing parts of Canada's anti-spam legislation when that law comes into force on July 1, 2014, together with the Canadian Radio-television and Telecommunications Commission and the Office of the Privacy Commissioner. Through this legislation the bureau will be able to more effectively address false or misleading representations and deceptive marketing practices in the electronic marketplace, including false or misleading sender or subject matter information, electronic messages, and locator information such as URLs and metadata.

The bureau promotes truth in advertising in the marketplace by discouraging deceptive business practices and by encouraging the provision of sufficient information to enable informed consumer choice. False or misleading representations and deceptive marketing practices can have serious economic consequences for Canadians, especially when directed towards large audiences or when they take place over a long period of time. They can affect both consumers and businesses that are engaging in honest promotional efforts.

The Competition Act contains criminal and civil provisions to address false or misleading representations and deceptive marketing practices in promoting the supply or use of a product or any business interest. Under the criminal provisions, the general provision prohibits all materially false or misleading representations made knowingly or recklessly. Other provisions specifically prohibit deceptive telemarketing, deceptive notices of winning a prize, double ticketing, and schemes of pyramid selling.

Identify theft, as the RCMP has described it, refers to the preparatory stage of acquiring and collecting someone else's personal information for criminal purposes. There are several Criminal Code provisions that address fraudulent conduct. The Competition Bureau's mandate in the mass marketing fraud realm relates to conduct that affects competition and to ensuring consumers have the information required to make informed purchasing decisions. Offences such as identity theft and frauds where no product or business interest are promoted do not fall under the bureau's mandate.

Mass marketing fraud is fraud committed via mass communication media using the Internet, the mail, or the telephone. Costing the Canadian economy $10 billion per year, it is an increasingly global criminal threat.

● (1115)

It has a substantial negative effect on economies and markets by undermining consumer trust and confidence in legitimate businesses. Large-scale criminal mass marketing fraud operations are present in Canada and other countries around the world.

Operators of mass marketing fraud schemes are highly adaptive, rapidly changing their methods and techniques to reduce the risks of law enforcement detection and investigation and to respond to consumer and business awareness of their current methods.

Identity theft and money laundering continue to be critical components of various mass marketing fraud schemes. Law enforcement agencies are witnessing an increasing exploitation of fraud victims to receive and launder victim funds or to receive and disburse counterfeit financial instruments. While most mass marketing fraud schemes are non-violent in nature, law enforcement intelligence indicates that some groups that engage in fraud employ threats and coercive tactics against uncooperative victims, rival groups, and their own group members.

The bureau often investigates large-scale mass marketing fraud crimes which have resulted in consumer losses of up to $500 million. The types of MMF cases that the bureau investigates include: scams targeting small and medium-sized businesses, such as directory and office supply scams; digital economy cases in which important information is buried in the terms and conditions; job opportunity scams; and health-related scams.

To effectively counter the threat of mass marketing fraud, investigative law enforcement and regulatory authorities in multiple countries have been: working together to gather and share intelligence on MMF schemes and how to disrupt them; increasing public awareness and education programs to help individuals and businesses recognize these schemes and avoid losses; developing measures to more promptly identify and support victims of mass marketing fraud schemes; and developing and expanding coordinated efforts among law enforcement agencies to fight MMF schemes.

To illustrate our collaboration, the bureau is a member of the International Mass-Marketing Fraud Working Group and the International Consumer Protection and Enforcement Network.

The bureau also plays a central role in the seven MMF Canada-U.S. law enforcement partnerships across the country of which the bureau is a founding member. Established in the 1990s to combat deceptive telemarketing, these partnerships now include Canadian and U.S. law enforcement agencies that work together to enforce laws dealing with mass marketing fraud. This collaboration has resulted in hundreds of investigations, prosecutions, and convictions.

The Canadian Anti-Fraud Centre, which the bureau jointly manages along with the RCMP and the Ontario Provincial Police, is the hub of the national network of MMF partnerships. It provides intelligence and complainant information to law enforcement partners on a wide range of MMF crimes.

In addition, the CAFC, along with the bureau and the bureau's law enforcement and private sector partners, educates consumers on how to recognize, report, and stop various forms of MMF. In fact, the partners collectively promote fraud awareness during fraud prevention month, which takes place in March.

In conclusion, Madam Chair and members of the committee, I would like to thank you for the opportunity to be here today and to speak about the work the bureau is doing to combat mass marketing fraud. We recognize that this is a global problem and accordingly one that requires a coordinated approach. The bureau will continue to work together with law enforcement agencies across the globe to defend consumers against this threat.

Thank you. We look forward to your questions.

● (1120)

The Vice-Chair (Mrs. Patricia Davidson): Thank you very much to our presenters this morning.

We will go to our first round of questioning, of seven minutes including the questions and the answers. I hope I won't have to cut anybody off, but I'll give you a bit of notice if you're getting to the end of the seven minutes and still have more to reply to the question.

We'll start with Mr. Ravignat from the NDP, please.

[*Translation*]

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

My thanks to the witnesses for joining us today. Good morning; it is nice to have you with us.

I do not know if you are aware, but my party, the NDP, has introduced Bill C-475 and Bill C-580, which are designed to strengthen the legislation that deals with the privacy of Canadians. The bills offer a solution to the fact that, legally, Canada is significantly behind the times in this digital age.

My question is more general in nature.

As a national police force, the RCMP has as part of its mission to ensure that the law is obeyed. Do you believe that Canada is adequately equipped at present to combat identity theft? Is the legal framework tough enough to help you in your work?

[*English*]

Supt Jean Cormier: As I stated during my opening remarks, obviously the Government of Canada has recognized the growing problem with identity theft, and some new laws have been implemented to address it. Any new tools or new legislation that may be put in place to improve the tools that are available to law enforcement to combat identity theft would certainly be a welcome addition. I believe that Canada has an effective and efficient system, but as I stated, there's always room for improved tools for our tool box.

[*Translation*]

Mr. Mathieu Ravignat: Aside from the CAFC, what measures does the RCMP have at its disposal in the fight against identity theft and fraud?

[*English*]

Supt Jean Cormier: Madam Chair, this might be a long-winded answer, because there are a number of initiatives that we undertake. I can list some of them. If I go over the time limit, you can advise me accordingly.

The RCMP is committed to Canadian safety and security, obviously. We have a number of initiatives, and I'm going to list a few.

In 2012 the RCMP developed its national identity crime strategy. The strategy is supported by three pillars: education and prevention, intelligence enforcement, and prosecution. The strategy calls for the following: identifying priorities and emerging risk, and so analyzing developing trends; relying on the compilation and analysis generated by the criminal intelligence pillar; increasing the intelligence-based investigation project and coordinated disruption efforts; and developing a standard approach for ID fraud as well, and thus to investigations, including creating and adopting a protocol for multi-jurisdictional investigation, because as I said, many times this crime crosses borders.

[*Translation*]

Mr. Mathieu Ravignat: Allow me to interrupt you. What you are saying is interesting, but I would like to know what stage you are at in developing those standards.

[*English*]

Supt Jean Cormier: The strategy was just implemented last year, and we are working with private and public sector partners right now to implement these.

[*Translation*]

Mr. Mathieu Ravignat: You can continue if you have anything to add.

[*English*]

Supt Jean Cormier: We're also developing strong partnerships in which we work together to develop or implement the strategy along with public and private sector participants, reaching across the federal and provincial boundaries and involving provincial and municipal law enforcement as well as other entities. We're raising identity crime awareness with the judicial community and government officials from across the country and in other countries.

As stated by my friend in his opening remarks, a component of fraud prevention month, which was the month of March, focused on identity theft.

● (1125)

[*Translation*]

Mr. Mathieu Ravignat: Thank you.

Could you send us copies of your notes so that we can speed the process up?

I would like to ask one last question. Do I have time, Madam Chair?

[*English*]

The Vice-Chair (Mrs. Patricia Davidson): Yes.

[*Translation*]

Mr. Mathieu Ravignat: Okay.

We recently learned that, in 2013, the RCMP reported to the Office of the Privacy Commissioner a mere 26% of the cases in which personal information was compromised. In the previous 10 years, only 4% of cases were reported.

There must be a reason for that. I am wondering why your organization does not systematically report all cases in which personal information is compromised.

Supt Jean Cormier: I do not know if I can answer your question precisely. Essentially, we continue to identify cases of identity theft. The number of cases is actually going down, but the amount of information involved is increasing.

Mr. Mathieu Ravignat: That does not quite answer my question.

According to the Office of the Privacy Commissioner, the RCMP reports only some cases of breaches of privacy. That is a problem, and I do not know why it is so.

Supt Jean Cormier: In order to check that information, I would have to compare my notes with my partners at the Competition Bureau.

[*English*]

I don't know. I'm saying that maybe I should—

The Vice-Chair (Mrs. Patricia Davidson): I'm going to interrupt you here. Maybe we can come back to this during someone else's questioning. The time is at an end here.

Mr. Mathieu Ravignat: Sure.

That's fair. If you can send that information along to us, that would be great.

The Vice-Chair (Mrs. Patricia Davidson): If you do have information to send, send it in care of the clerk. Then it will be circulated to the entire committee.

For our second questioner, we'll go to Mr. Hawn, please, for seven minutes.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you all for being here.

I'd suggest that probably the RCMP applies some judgment. You get all these breaches. I assume you look at them and apply some judgment in deciding which ones are worthy of forwarding on and so on. Would that be a fair statement?

Supt Jean Cormier: That would be a fair statement. We would likely report to the Competition Bureau what is relevant to the Competition Bureau.

Hon. Laurie Hawn: Sure.

Mr. Currie, you talked about being part of various international organizations. I presume that you share best practices and so on. Is there somebody out there who has best practices that we haven't perhaps yet learned from or haven't yet implemented? Is there anybody out there we should be learning more from?

Mr. Morgan Currie: Madam Chair, I'm happy to report that our relationships are ongoing and frequent. Of course, one of the big issues of mass marketing fraud is how the criminals adapt to changes and take advantage of new technologies, but we frequently participate in these law enforcement groups and in these international fora, so we feel as though the information is being adequately shared among the agencies through those fora.

Hon. Laurie Hawn: You talked about the criminals adapting, and they're obviously very clever people. Do we hire any of those kinds of folks to try to stay one step ahead of the bad guys, you know, to give somebody a chance? “Okay, if you were going to do this, how would you do it?” Do we hire anybody to do that sort of stuff?

Mr. Morgan Currie: I can say that we have to keep our own technological methodologies of detection of such crimes at a high level. I don't think we have anybody or a practitioner like that in our employ; I might be surprised, but I hope not. But certainly we look at social media sites for information or technological tools, and our cooperation with law enforcement agencies and even consumer protection agencies help us to attract information and to obtain evidence. I think we're on top of it and staying on top of the trends.

● (1130)

Hon. Laurie Hawn: Superintendent Cormier, you mentioned education. Obviously, educating the public is pretty important. Who should be doing that education, other than generically everybody? What role does government have to play in that education?

Supt Jean Cormier: Actually, it plays quite an important role. As a matter of fact, one of the strategies against identity theft is currently being led by Treasury Board. They are in the process of developing the guideline on identity assurance. It's at the draft stage.

As I mentioned in my opening remarks, I believe that it's everybody's responsibility to be aware of it, but the prevention, obviously through publicity such as fraud prevention month, was part of it. The CAFC operates almost like a peer-to-peer type process. When people call to report that they have been the victim of identity theft, there is a person at the other end of the line who will sympathize with them and counsel them on how to prevent that from happening again.

There are also different practices in place that do focus on education and prevention, but I believe the Government of Canada has an important role to play in it. Completing the strategy would likely be a big part of it.

Hon. Laurie Hawn: Obviously, the private sector buy-in is important on that too, because they're protecting themselves. Are there any challenges with private sector buy-in or public sector buy-in that are causing difficulty?

Supt Jean Cormier: The buy-in is not the difficulty. Essentially, the difficulties and challenges that we face in regard to working with the private and public sectors and law enforcement are about the ability to share private information in certain instances, which are limited by privacy laws, obviously, and the need for the businesses that we deal with to respect client privilege.

Hon. Laurie Hawn: Following on that, obviously, the Privacy Act is there for a reason and that obviously gets in the way sometimes. How much of an impediment is it? I mean, how long does it take to get around the Privacy Act legally to get the kind of information you need? I know that would vary depending on the case.

Supt Jean Cormier: There's no way to get around the Privacy Act to get information—

Hon. Laurie Hawn: I mean working through the Privacy Act.

Supt Jean Cormier: To get it legally, obviously, if we're dealing with a particular investigation, we would have to go through the normal processes of obtaining court orders to obtain information that we may need for our investigation. Right now, there is certainly an appetite from the private and public sectors to share more information with law enforcement, and certainly for intelligence and prevention purposes, to build a database of people who are being victimized and suspects are being identified. There is more of an appetite there for that. Currently, there are relationships that are in the process of being developed at the CAFC that are improving that.

Hon. Laurie Hawn: Sticking with the Privacy Act aspect of it, if somebody comes forward and wants to share the information with you, the Privacy Act doesn't get in the way of that, does it?

Supt Jean Cormier: No. That is correct.

Hon. Laurie Hawn: Bill S-4 came into force in 2010, which added some new Criminal Code offences that target aspects of identity theft, some that were not, up until then, covered in the legislation. Has that had a positive impact at all on the ability to prosecute those kinds of things, that you're aware of? Now, the numbers obviously will continue to go up just because of volume.

Supt Jean Cormier: It has had a positive impact. I'm going to give you some of the numbers that I have here. In 2012, there were 2,813 cases reported, out of which 1,024 resulted in related charges. I don't have the comparative from the previous year, but I know from experience that it resulted in an increase.

● (1135)

The Vice-Chair (Mrs. Patricia Davidson): Thank you very much, Mr. Hawn. Your time is up.

We now move to Mr. Andrews, for seven minutes.

Mr. Scott Andrews (Avalon, Lib.): One of the things that we're studying with identity theft is we're trying to get a better understanding of how this identity theft is happening so that we can look at ways to probably prevent it or help educate people.

Mr. Cormier, in your opening statement you talked about opening some 3,411 occurrences relating to identity theft. Do you have any breakdown on what types of identity thefts that these may be?

Supt Jean Cormier: I'm going to check. Sorry, no, I do not have it here with me. I have the total statistics from the Canadian Anti-Fraud Centre right now and the total statistics for the RCMP. I don't have the breakdown.

Mr. Scott Andrews: Could you give us some idea of how people are doing this type of identity theft?

For example, yesterday we had Passport Canada in here, and I'll ask a question on that in a minute. They said a lot of things that were given to them were stolen documents and people were trying to acquire an identity through stolen documents. Is that a common way that people are trying to create a different identity?

Supt Jean Cormier: Yes, in my opening remarks, as well as in my partner's opening remarks, we talked a lot about cybercrime that takes place now because of the advance in technology.

The phishing scam is still very much a concern, obviously, where people receive e-mails soliciting personal information, bank information, and credit card information, pretending to be a financial institution, for example. That is still very common.

Theft from mail is still a concern. Personal papers that are stolen from the mail system can result in identity theft. As a matter of fact, Canada Post was one of the partners in developing the strategy here for the RCMP along with a number of other partners. You mentioned Passport Canada. Passport Canada has one of the best systems in the world in preventing fraud with their system that they have in place. Passport Canada should likely be looked at as an example of how to implement systems to prevent fraud.

Mr. Scott Andrews: Yesterday they said, I think it was in 2013, they had 70 cases of people trying to obtain a passport through an identity that was not their own. They then passed that information on to the RCMP. What do you do when you get that information from, for example, Passport Canada when someone tries to obtain a different identity?

Supt Jean Cormier: It's considered a fraud, and we would investigate it as a fraud-type investigation. Obviously, we'd investigate what the intent was behind it, the reason. It could be an illegal immigrant in Canada. It could be somebody wanting to engage in other criminal offences. We have to look at every possible angle that is involved. It starts from receiving the complaint, to taking the statement from the witnesses, to following the leads for the suspect.

Sometimes when they report matters to us, because they only have the false identity, and they cannot provide us with the true identity of the person, so sometimes it becomes a challenge to identify who the culprit was. But where we can trace the suspect, certainly we fully investigate those cases as fraud.

Mr. Scott Andrews: How do you tell someone that someone tried to use their identity? Is there a process in place, if you come across someone trying to pass themselves as someone else, for telling the actual Canadian or person that their identity has been compromised? Is there a format or is that a priority to try to let the person know that their identity was trying to be compromised?

Supt Jean Cormier: It forms part of the course of the investigation if there is actually another person's identity that's being used fraudulently. Yes, we will advise the victim that they have been the victim of fraud, and that somebody else has tried to use their identity.

We provide them with advice as well as to the impact it may have on them, because if the person gets detected trying to use a person's identity, that identity may have been used for other purposes unbeknownst to law enforcement or unbeknownst to the victim. There is a need to have contact with the victim. It's part of the normal process of the investigation, and also, to obtain a witness. That person becomes a witness essentially, as well as a victim, to say that the person was not the person who tried to get a passport, or tried to get a bank loan, or whatever the situation was.

● (1140)

Mr. Scott Andrews: Once a person is a victim, what steps do they need to take to try to make sure they can reclaim their identity if it's gone to a certain point? Do you see a lot of victims saying that it's been a year and it's still impacting them?

Supt Jean Cormier: Yes. As I stated in my opening remarks as well, there can be a long-term impact on the victim. Rebuilding and clarifying your credit history when you were a victim of fraud or identity theft is not an easy process. It is complex and can be difficult to complete. In some cases, yes, I've heard of victims waiting months before the situation was completely resolved.

Mr. Scott Andrews: Is it mainly with their credit history? Is that the common one of trying to regain their correct credit history?

Supt Jean Cormier: I believe that is the one that is more complex and problematic for victims, yes. Depending on the type of fraud that the individual may have used the identity to commit, it may have an impact on them as well.

Mr. Scott Andrews: I think at some point in the future we're going to have the credit agencies come in. Is there anything we should be asking them about trying to help victims get their files straightened out more quickly? Is there an angle there for us to ask them about?

Supt Jean Cormier: I don't know exactly what is involved in their process. I'm sure they have due diligence processes that they have to verify as well, because I'm sure that anybody with bad credit could go to them and say, "I was a victim of fraud. That's not my bad mark on my credit history."

I'm sure they have a pretty stringent due diligence process that they have to go through. Sometimes the delay can be frustrating for victims, but it is necessary at the same time. For me to tell another agency what would be required would be difficult.

The Vice-Chair (Mrs. Patricia Davidson): Thanks very much, Mr. Andrews.

We'll now go to Mr. Zimmer for seven minutes.

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

I have a couple of questions, and I'll start with the Competition Bureau. What officially is your mandate, in the simplest of terms?

Mr. Morgan Currie: Our mandate is to ensure that Canadian businesses and consumers prosper in a competitive and innovative marketplace. Our focus is very much on competition for Canadians and the health of the economy. Generally speaking, we have provisions that deal with criminal matters such as price fixing. We evaluate proposed mergers to see if they might limit competition for Canadians for products and services. We have a branch that looks specifically at abuse of dominant position, when large companies that dominate a marketplace might be engaging in acts to limit competition.

In our branch, the fair business practices branch, the core of our work is to investigate cases of false and misleading representation and deceptive marketing practices that cause consumers to have unclear information when they go to make purchasing decisions.

Mr. Bob Zimmer: I heard what you said earlier, and it goes along with what you had just suggested.

Can you give us an example of mass marketing fraud, and maybe some examples of other types of fraud? Can you give us an example that occurred in Canada? What was the fraud? How did the Competition Bureau nip it in the bud? How were the victims recognized in the whole process?

Mr. Thomas Steen (Major Case Director and Strategic Policy Advisor, Competition Bureau, Fair Business Practices Branch , Department of Industry): I can handle that one.

My colleague, Mr. Currie, stated four examples of the types of mass marketing fraud the bureau handles.

The first category covers scams targeted at generally small or medium-sized business, whether they're in or outside of Canada. If the perpetrators are in Canada but target people outside of Canada, the act applies to that, as well as to situations when the victims are in Canada.

Of those scams targeting businesses, a typical one is the directory scam. This is committed either by telemarketing or by fax. There's always an Internet aspect to these scams as well. Generally what they try to do is they use what we refer to as the assumed sales technique, where they call someone at a business—actually it could be an organization, a charity, a church, a government agency, anybody that runs an office, really—and they try to leave the impression with them that they've already bought this directory every year and they're just calling to renew their listing and update their information. They sometimes try to use names similar to the Yellow Pages group, or companies such as that. People don't realize that they're committing to a payment, whether it's over the phone, or sometimes they send facsimiles to companies saying to update their information, sign the form, and send it back. Buried in fine print, they're committing themselves to $1,500 a year to be listed in the directory.

There is a product, per se, usually a directory listing on the Internet, but it's not accessible. For instance, for any commercial purpose to be listed in a directory, if I have a towing company, I would want my consumers to maybe google towing companies in Ottawa, and my company name would come up. It probably does come up in the Yellow Pages directory or Canada411, but not on these scam ones, so they're of no commercial value to businesses.

How do we investigate those? We receive complaints. We have our own complaint centre, through the Canadian Anti-Fraud Centre, and through our partnerships. Then we evaluate those complaints. We have enforcement priorities, and at a certain point we decide to investigate. When we get to that stage, we have several investigative tools in our toolbox, including search warrants, sections under our act where we can apply for people to provide information, written returns, or records, or provide information under oath. We have to apply to courts for these powers and show that there are reasonable grounds that these offences have occurred. That's what really gets us started on our investigation, when we use those powers and we analyze that information. Eventually, we complete our investigation and refer it to the federal prosecution services with recommendations to charge, and it's their decision whether the individuals or companies should be prosecuted.

● (1145)

Mr. Bob Zimmer: Following up on that last point, how often do you see those groups actually prosecuted, and what is the restitution for the victims? Have you seen victims compensated? What is the typical end of the road for that particular victim of this crime?

Mr. Thomas Steen: To the first part of your question, a very high percentage of the cases we refer to the federal prosecution services are prosecuted. We have a very close and good relationship with them. We work with them along the way, so there are very rarely any surprises in our investigative technique or what we've uncovered. For that reason, I would say well over 90% of the time, maybe 95% of the time, the cases we refer are prosecuted.

As far as what happens down the road, first of all, the provisions in the Competition Act dealing with this type of conduct are criminal in nature, so the accused can either be fined on summary conviction up to $200,000, or most likely, our cases go by way of indictment, not summary, and the fines can be very high at the discretion of the court, and jail terms to a maximum of 14 years can be imposed.

There is also means for restitution.

Mr. Bob Zimmer: What can happen and what actually happens are two different things completely.

What do you see typically happen to the victims of the crime at the end of the day? Are they being rewarded or are they not? We're talking about obviously the highest watermark, but what often happens? That's what I'm asking.

Mr. Thomas Steen: A few things happen.

Often what happens is that the targets are convicted. They are often fined significant amounts of money, hundreds of thousands, if not millions of dollars, and a time sentenced to jail terms. The highest jail term received so far is three and a half years, but it wasn't until 2009 that the penalty was increased to 14 years in jail, so we expect more severe jail terms.

In terms of victim restitution, there are provisions in the Criminal Code for that avenue for judges. There are also proceeds of crime that attaches to our offences, as well as Criminal Code offences. At times we do that.

It's really a question most of the time of what kind of evidence we're able to uncover at the time of our investigations. The criminals are smart, as has been said, and often they move and hide their money. When we find it, we do what we can. We're getting better and better at identifying those assets.

● (1150)

The Vice-Chair (Mrs. Patricia Davidson): We're going to have to stop there. The time is up.

Thanks, Mr. Zimmer.

That finishes our first round of questioning. We'll now go to the second round, which is five minutes, and we'll start with Mr. Angus, please.

Mr. Charlie Angus (Timmins—James Bay, NDP): I stopped at a bank machine at a bank in Ottawa one night and took money out. The very next morning, the caisse populaire in northern Ontario called my wife and said, “We think a fraud has occurred.” They had identified that my card had been compromised, and the very next day the passwords were changed.

That was extraordinary. That doesn't happen all the time. It made me realize that I could have gone a month without realizing that I had been compromised. My bank account could have been cleaned out because I'm on the road, and I'm not paying attention.

Mr. Cormier, how important is it when someone's information has been breached.... What is the timeline to inform them so that they can take preventive steps? How important is it to have a quick response time?

Supt Jean Cormier: It is very important, obviously, but it depends on how the information is compromised.

In the example when you were a victim of a compromise, you were advised the following day. That's a pretty quick response, which probably minimized.... The quicker it's identified and the quicker the response, the more chance we have, or that the organization will have, to minimize the impact on the victim as well. It's very important.

Mr. Charlie Angus: We've talked many times to the Privacy Commissioner. She's expressed her frustration about the need to update Canada's privacy laws, because we see examples in the private sector where it's voluntary reporting of breaches. Certainly, if something has been breached in your company, you don't want to disturb your customers. We've seen 40 million and 50 million addresses, information taken out from companies. We've seen half a million students' information lost and over a month went by.

How important is it, do you think, that the Privacy Commissioner be informed of breaches in the private sector or in government to ensure that people can take steps in case it has been breached for criminal purposes?

Supt Jean Cormier: That the Privacy Commissioner be informed of the breach, or that the information be shared with law enforcement or other partners that could have an impact in minimizing the impact on the victim?

Mr. Charlie Angus: The commissioner's role is to decide whether or not the breach is significant enough that individuals have to report it. You don't need to scare someone if the data has been put in the wrong closet, but then the commissioner gets to decide whether or not a breach has occurred and someone has been affected here.

Supt Jean Cormier: Then it would be very important, obviously, that they be engaged promptly and that the information be assessed as soon as possible. The privacy law, obviously, is necessary. I enjoy my privacy as much as anybody else in this room, but it needs to be balanced as well with the need to protect victims of crime.

Mr. Charlie Angus: We're seeing now international gangs, international espionage. In 2011 the Treasury Board's and the Department of Finance's computers were hacked by someone who was trying to get passwords and sensitive information. It was traced to China. Was it for espionage reasons? Was it for criminal reasons?

Given the incredible power that's in the espionage and hacking world, the ability to use algorithms to gather all manner of data way beyond the ability of any individual to keep track, how realistic is it for present-day police enforcement to be able to stay on top of this? How much training is needed? Is it sufficient? It seems to me we're dealing with a level of scale of criminal activity that has dwarfed anything that ever happened back in the old 419 scam days when they had to actually run them through fax machines.

Supt Jean Cormier: Obviously, having a properly trained police officer to investigate those types of crimes is very important. Having the right partnerships in the public and private sectors to help us investigate those crimes can be very important as well. There are other parts of the Government of Canada that are also responsible for the electronic world or the cyberworld out there. It is very important to have the right training. In Canada, the RCMP have some very well-trained officers in that field. We have a good reputation in comparison with our partners around the globe in relation to our abilities in that area. Certainly because of the advance in technology and how quick technology develops or changes, there is that constant need for continued improvement in training.

● (1155)

Mr. Charlie Angus: How important is it to have a transnational response? These gangs are setting up in some very sophisticated businesses now in domains where it's possible to carry on this activity and pretend that it's perfectly legal. Are they beyond the reach of Canadian law? Do we need to have a transnational response?

The Vice-Chair (Mrs. Patricia Davidson): Your time is up, Mr. Angus, but perhaps we could have a quick reply, please.

Supt Jean Cormier: Certainly.

That is important and at the same time, it is a huge challenge for law enforcement because when we go from jurisdiction to jurisdiction, sometime other jurisdictions have different laws than we may have here domestically, so it's not allowing us to take the same action or certain action we'd like to take to prevent it.

It's important but it's one of our biggest challenges at the same time.

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

Thanks, Mr. Angus.

We'll now go to Ms. O'Neill Gordon, for five minutes, please.

Mrs. Tilly O'Neill Gordon (Miramichi, CPC): I want to thank the witnesses for being here today.

Your presentation today is certainly very valuable and makes us think of all the many mistakes that we make along the way, that we don't cover our tracks, especially when it comes to banking machines. We all go to banking machines. What would bring this about? Is there one main reason someone could get into it and take your money? What's a common mistake?

Supt Jean Cormier: I will turn it over to Inspector Miller to answer.

Inspector Cameron Miller (Federal Coordination Centers, Domestic, Royal Canadian Mounted Police): Madam Chair, one of the main methodologies of obtaining information from bank machines is something called skimming. There could be a false insert placed into the bank machine where people actually key their numbers into what they think is a legitimate machine and it processes it but the data is being captured.

You'll notice on bank machines today, there's a little bit of a shield over the PIN pad to protect your PIN, your personal identification number. People in the past have installed cameras in the vestibules where the bank machines are so they could watch and record you punching in your PIN and the magnetic strip at the same time would be compromised by the skimming machine.

At the end of the day or in the morning before the bank would open, the criminals would go back, remove the insert and then download all the information in the video, getting multiple PINs and multiple magnetic strips, and then they will upload them onto other ones. They compromise multiple cards, create them in a factory-type setting, and then attempt to bleed as many accounts as they can.

Mrs. Tilly O'Neill Gordon: That's very scary, but anyway it's great information to have on hand.

You mentioned, Mr. Cormier, about education on how to protect one's identity is everyone's responsibility. What are some means or ways that individuals can reach out to educate themselves about identity theft? I guess I have a lot to learn.

Supt Jean Cormier: There are different methods for a consumer or individual to protect themselves from identity theft. Obviously some publications are available out there. You could go to any police office and look at their bulletin board and they would have pamphlets on identity theft. Nowadays, the use the of the Internet is a good way as well.

We talk about the Internet being a scary place to get your personal information stolen but it is still a very good place to obtain information. For example, the Canadian Anti-Fraud Centre has a good website that promotes certain ways to protect an individual from identity theft or other frauds.

Mrs. Tilly O'Neill Gordon: We know that the means is certainly rampant and becoming more and more rampant. Do you see any one reason that is causing this to rise?

Supt Jean Cormier: I believe it's because of the advance in technology that is making the world more accessible to anybody around the globe. Obviously it's a transnational type crime. The crimes that are being committed are not necessarily being committed by somebody in Canada. They can reach into Canada from anywhere in the world, and as a result, more people end up being victimized.

I don't have the comparison chart but I'm sure if we were to compare the number of Internet users to the increase in the number of victims, there would be some relation.

● (1200)

Mrs. Tilly O'Neill Gordon: That was going to be my next question. How much identity theft is paper-based in comparison to how much occurs online?

Supt Jean Cormier: I was asked that question in a different format earlier, and I do not, as I said, have the breakdown of the different types of identity theft.

Mrs. Tilly O'Neill Gordon: Of course we all know this is quite a worry for many individuals. Do victims of identity theft ever become aware that they have been targeted, and how?

Supt Jean Cormier: Yes, when we are involved in an investigation we do make an effort to advise the victim, but certainly if it's not reported to us, sometimes the victim will not be aware of it.

At the same time, I would like to state that the cases reported to the CAFC, the Canadian Anti-Fraud Centre, represent only 5% of the victims. That means that 95% of the victims either do not report to the police, or at least they do not report it to the Canadian Anti-Fraud Centre.

Certainly, that's why the publicity about making everybody aware of the Canadian Anti-Fraud Centre being the central repository for this type of information is paramount as well, because the more we know about what's going on out there, the better we can develop strategies and tools to prevent those types of crimes.

The Vice-Chair (Mrs. Patricia Davidson): Thank you very much, Ms. O'Neill Gordon.

I don't have any other names on the list.

Do you wish to speak, Mr. Andrews?

Mr. Scott Andrews: Yes, I have a couple of questions.

Both of you can help to answer this. What pieces of information do criminals need or do people need to create an identity theft? How many pieces of your life do they need to know about? Do they need to know your address, your date of birth? How much information do they need to know to try to create an identity?

Supt Jean Cormier: I'm just going to touch on it, but I'll turn it over to Inspector Miller to answer as well to add to it.

Essentially there are a number of vital statistics or information that would be required.

Insp Cameron Miller: When you're going to create an identity, obviously the more information you have, the better. If you can start off with something along the lines of a breeder document, which is a source document such as a passport or a birth certificate, you can go from there.

If you want to create a synthetic identity, you can start with something as little as a name. From there you can start to build your identity and decide how old you want this person to be, and then you can create a birth certificate and you can start creating false documents and forge them. Using false and fraudulent documents, the synthetic identity can go on to create further documents from there.

To answer the question, you can start off with as little or as much as you want. The more you have, the better and the easier it is.

However, with methods of production today you can start off with pretty much nothing other than a name, an identity, and an age group range in your head.

Mr. Scott Andrews: It could be a fictional name. It doesn't have to be an actual person.

Insp Cameron Miller: Yes, one of the things with a synthetic identity is that it's not a real person, so the name could be John Doe or Jane Doe, as you choose, and from there you build up Mr. Doe's or Mrs. Doe's characteristics, where they choose to live, at 123 Any Street, in any town, anywhere.

Mr. Scott Andrews: Mr. Currie, how do you see this online through mass marketing and such? Is it more synthetic or are individual consumers having their identity stolen?

Mr. Morgan Currie: Well of course the criminals become more sophisticated and under-reporting is a big problem for us. So we try to capture, through use of a credit card. We create fake identities as well to try to attract this type of behaviour. We try to subscribe to something to see if there is any fraudulent activity out there.

Tom can help me with this and will probably be a bit more precise. Whenever there is a situation where you're buying something or there is a free trial offer and you're submitting credit card information, you're immediately at risk of being upsold products that you had never even heard of, and then having difficulty cancelling that service before you're being charged hundreds of dollars. That fits into our law as a serious deceptive practice.

● (1205)

Mr. Thomas Steen: We've recently had several cases in which that occurs. A product is offered on a free trial basis—just pay a few dollars, maybe $3 or $4, for shipping and handling—and it is paid for by a credit card. Buried in the terms and conditions where it is very difficult to locate and read, or understand the terms, the consumer in fact is agreeing to a purchase plan of $80 a month or something like that for that product. Worse, two other products might kick in that are completely unrelated and that appear on the consumer's credit card statement under completely different descriptor names.

As Mr. Currie has stated, it's really difficult to get out of those traps, because the phone numbers provided go to call centres that often don't answer the calls. You get a major runaround telling you to call another number. Often, the only recourse for consumers is to call their credit card company and cancel the card, and it's very difficult to get their money back.

Mr. Scott Andrews: Thank you.

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

I'd like to take this opportunity to thank our presenters today.

We've certainly heard some extremely interesting information, scary information in some aspects, but we appreciate the time you've taken.

Since we have no more witnesses, I will declare the meeting adjourned.