HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 145 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, January 28, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Monday, January 28, 2019

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, we'll commence. I see quorum, so we'll call the meeting to order.

This is our first meeting on the study of cybersecurity in the financial sector as a national economic security issue, which in light of events in the past weeks and months is proving to be quite timely.

To lead us off are Mr. MacKillop and his colleague Mr. Lambert, both of whom are experienced witnesses before committees on the Hill.

We look forward to your 10-minute presentation. Thereafter, colleagues will ask questions.

Mr. MacKillop.

Mr. Barry MacKillop (Deputy Director, Operations, Financial Transactions and Reports Analysis Centre of Canada): Thank you, Mr. Chair, and good afternoon, honourable members.

I'm pleased to be here with Mr. Lambert. I have with me Monsieur Juneau, who's going to assist us in flipping through these slides. I would have found it very difficult to do both at the same time.

On behalf of FINTRAC, I'd like to thank you for the opportunity to go through exactly what FINTRAC is and who we are are. I know we're an agency that's not particularly well known, so hopefully I'll be able to expand a bit today on what it is that we do and how we do things.

FINTRAC is the Financial Transactions and Reports Analysis Centre of Canada.

[*Translation*]

Incidentally, the presentation will probably be mostly in English, but of course we can also answer questions in French.

[*English*]

We were established in 2000. Our enabling legislation is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act; I won't go through all its iterations and all the amendments. We're an independent agency that reports to Parliament through the Minister of Finance. We're the FIU, which is the financial intelligence unit, and also the compliance regulator of those businesses that are subject to the PCMLTFA. We're headquartered in Ottawa. We have three regional offices: one in Montreal, one in Toronto and one in Vancouver. The regional offices do our compliance, our exams and our assessments on all the reporting entities that report to us. All our intelligence is done through our office in Ottawa. Our budget is about $55 million a year, give or take.

We are not—and this is an important point and one that's not always understood—an investigative agency. We are an administrative financial intelligence unit, which means that we receive reports. We cannot actively go out and collect reports. We cannot ask reporting entities to give us specific reports on specific individuals or entities. We do not do any covert work on the web. We don't do any dark web investigative covert work or anything like that. We exist to analyze the reports that we receive under our legislation and from the reporting entities that are required by law to report to us.

We're also limited a little bit in our legislation in terms of specifics. If you were to ask me whether or not I disclosed on a particular case or a particular person, I would not be in a position legally to answer that. If I were to say whether or not I disclosed a particular case on a particular person, it would essentially be tantamount to making an illegal disclosure, for which I'd be subject to a potential five years in jail. As you can appreciate, it's not something that I would like to do. We can't talk specifics, unfortunately, with respect to the cases that we do, but we can talk about how we do it, what we do and what we do generally.

On this first slide, as you can see, we have the number of reporting entity sectors. These are the reporting sectors that must, under our legislation, report and provide reports to us. Our key regime partners in Canada include a number of different agencies and departments, all responsible for certain aspects of the anti-money laundering and anti-terrorist financing regime in Canada. The disclosure recipients, those to whom I can legally disclose depending on when we meet our legal threshold for reporting and for disclosing, are shown on the left of the slide.

Included in the types of reports that we receive at FINTRAC are electronic fund transfers in and out of Canada that are $10,000 or more, and there is a 24-hour rule applied to that as well. We also receive large cash transaction reports of $10,000 or more and casino disbursement reports on $10,000 or more going into or out of a casino. We receive terrorist property activity reports and suspicious transaction reports.

The suspicious transaction reports are in fact what we like to call our bread and butter. There are no monetary thresholds, and it's up to our reporting entities when they deem something to be suspicious relevant to money laundering or terrorist financing to report that to us. They usually provide us with a narrative as well. This provides us with significant quality information that we can then disclose to our law enforcement partners if we meet our own threshold of suspicion that it is relevant or would be relevant to a money laundering or terrorist financing investigation.

Also, while the CBSA is not a reporting entity, we do receive from them cross-border currency reports and cross-border seizure reports as well. We also receive voluntary information records from law enforcement and national security agencies, and we can get that from other government agencies, as well as the public, if they want to submit their own suspicions or their own information on what they perceive as or think is money laundering or terrorist financing.

● (1535)

We also receive queries and disclosures from our international partners. We have 105 MOUs signed with international foreign intelligence units. They can share information with us and we are at liberty to share information with them according to the MOUs that we have signed.

What do we actually do? We get our reports from our reporting entities. On the compliance side we ensure through exams, assessments and different techniques that they in fact are complying with the legislation's regulations under the PCMLTFA. Once we receive the reports, we will then do our own intelligence and analysis on those reports. We will obviously connect those with voluntary information records that we may receive from law enforcement and national security agencies. If we reach our threshold to disclose, we will then disclose tactical financial intelligence in support of ongoing investigations or, in some cases, we will proactively launch investigations.

We also do strategic intelligence in looking mostly at trends, topologies and research that we do on upcoming and emerging technologies and emerging threats to the financial institutions or to the anti-money laundering and anti-terrorist financing regime in Canada.

In terms of the number of reports we receive, we receive approximately 25 million reports a year—all reports, all told. From there, that's what we base our analysis on. As I said earlier, we are not investigative, so we cannot go out seeking additional information. We will of course use open source information to supplement our analysis prior to providing disclosures to our law enforcement or national security agencies.

As I said, we do tactical financial intelligence. That's typically related to specific targets, individuals, entities or investigations. We provide that to police. We can provide that to law enforcement and national security agencies, depending on the thresholds. We can also provide that to the CRA if there is a tax evasion, for example, or to the CBSA if there's an inadmissibility question. We can also provide it to our international partners if there is a connection between Canada and an international partner or another country. If we have an MOU and if we have authority and approval from our law enforcement partners in Canada, we could provide that to our international FIUs as well.

We also do a fair bit of strategic intelligence in order to look at analytical perspectives on the nature, scope and threats in this. It's obviously a fast-moving world when we're talking about anti-money laundering and anti-terrorist financing. We try to stay on top of that as much as we possibly can. We have a strategic intelligence unit that does that.

In terms of our contributions, we have provided disclosures on all types of fraud, including romance scams. We'll go straight to that on the public-private partnership that we launched with HSBC and the Canadian Anti-Fraud Centre, as well as law enforcement and major banks across Canada. Project Chameleon was launched in 2017, building on the success of Project Protect, which was on the money laundering related to human trafficking. This is on money laundering related to romance scams. It is, according to the Canadian Anti-Fraud Centre, one of the biggest and most lucrative types of scams in Canada. It tends to focus on seniors, as you can imagine. I don't think I have to explain what a romance scam is, as we probably all know, but if that comes up in the questions, we'll answer later. In light of time, we'll go to the next slide.

Again, rather than go into all of this, we'll look at our role on the strategic intelligence side in addressing the emerging technologies. We do keep track of innovative financial technology—fintech—trends and developments. We have people whose job it is to do that type of research. We work with our international partners as well, through Egmont or the Financial Action Task Force. We also will work with other international partners to develop trends, topologies and reports and to identify potential threats in the regime—they could be on the regime or potentially on the regime in the future—in looking at where the emerging technologies are and the intersection with anti-money laundering and anti-terrorist financing.

● (1540)

Mr. Chair, I think I've come in just under the time allotted. I will leave it at that. I'm available for any questions you may have.

The Chair: Thank you, Mr. MacKillop. You're obviously very professional. You're two seconds over.

Monsieur Picard, please, for seven minutes.

Mr. Michel Picard (Montarville, Lib.): I'll invite you to answer, Mr. MacKillop, in the language of your choice. However, to be as technical as possible, allow me to ask my questions in French.

[*Translation*]

You have clearly explained that FINTRAC is not an investigative agency but an agency that analyzes reports, as its name indicates.

Am I correct in saying that because you carry out analyses, you are able to detect abnormal behaviours or fraudulent schemes, whatever they may be? With respect to the new schemes that are being used, what is the technological aspect that has evolved over the past five or ten years? What technological evolution have you seen in the schemes you analyze?

Mr. Barry MacKillop: We are able to do that. As you said, we do strategic analysis, but we also look at the tactical aspect. We can see the changes that have occurred, if there are any.

These past years, we have mainly seen different payment methods, and attempts at anonymity through the use of cryptocurrencies, for instance. For transactions to be even more anonymous, people now use mixers. It is thus becoming harder and harder to detect abnormal behaviours, which exist both in Canada and internationally.

This is a challenge with respect to enforcing the law, as well as for those organizations that fight against money laundering. The development of new payment methods is certainly the biggest challenge.

● (1545)

Mr. Michel Picard: In a money-laundering scheme, you could say that the whole transaction chain is legal, except for the criminal origins of the money being laundered. I think that the technical means being used to launder money, despite technological progress, now accelerate transactions, which allows the perpetrators to cover their tracks better. These technological means hinder investigations, as the transactions go through different countries.

Do you think that the new technologies that are being used simply increase the efficiency and speed of the transactions, or are they used as tools for fraud or crime in the cyber world? I am excluding cryptocurrencies here, as that is a fairly particular universe. Is the technology being used to increase the speed of transactions, or are there other technologies that are in fact direct attack tools?

Mr. Barry MacKillop: That is a good question, and I am going to respond in English, because this is getting a bit more technical.

[*English*]

As you know, around the world, a lot of this is in English, so if I'm talking cryptocurrencies—in French I think it's *cryptomonnaie*—we're seeing a couple of things. Yes, it is faster. The speed of transactions is certainly faster.

If you look at things like romance scams, for example, yes, money laundering tends to be proceeds of crime. However, when it comes to romance scams, the proceeds are already in the financial system. This is the use of social media and the use of different ways of either anonymizing or representing yourself falsely and using social media to take advantage of people: They're sending money to you and you're using that to launder it. The crime is perhaps the false representation of yourself as opposed to committing a physical crime of robbing a bank and then trying to launder that money.

You are correct. It is quicker, and it can bypass.... If you're using cryptocurrency-type stuff, you can bypass the financial system itself to do that.

We're also seeing that the speeds at which transactions can happen are increasing. As for the types of crimes, with the use of social media and those types of things to steal identities and represent yourself falsely—such as putting false representations on Facebook and those kinds of things to "friend" people and take advantage of people—we're seeing more of that. Certainly, the ability to use the Internet and open source to identify potential victims is something that criminals are taking advantage of as well.

Then there are the other areas where you're looking at ransomware, for example, in which a fake email might be sent in or they're taking over somebody's computer and requesting payment from them to get back their access to their computer. We have seen cases of ransomware internationally. That seems to be a growing field right now in terms of criminals being able to take over and request payment. More and more, they'll request payment in cryptocurrency as opposed to cash or an email transfer.

Yes, the ability to use computers is increasing the capacity.

Mr. Michel Picard: I have a couple of quick questions.

[*Translation*]

Your agency comes into play when an incoming or outgoing transaction of $10,000 is reported to you. Are your algorithms limited to transactions of $10,000, or do they also analyze cases where a scheme is used to divide an amount of much more than $10,000 into several smaller transactions that will go undetected under the radar?

Mr. Barry MacKillop: Reporting entities are obliged to disclose transactions of $10,000 or more, but when they use the suspicious transaction report, there is no limit. They can report transactions of $200 that take place three or four times a week. Reporting entities are in a position to detect schemes, and we receive those reports. Our analysis is not limited by that threshold.

Mr. Michel Picard: Thank you.

The Chair: Thank you, Mr. Picard.

Mr. Paul-Hus, you have seven minutes, please.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Gentlemen, thank you for being here.

The purpose of our study is not to analyze fraud. We aren't as interested in the financial aspect so much as in the impact on the cybersecurity of transactions.

We understand quite well that FINTRAC is a hub that receives information from the list of agencies that were mentioned. Large accounting firms, for instance, must send you information on their clients, correct?

● (1550)

Mr. Barry MacKillop: Yes.

Mr. Pierre Paul-Hus: We know that there has been an increase in the number of criminal transactions on the Internet. Have you observed a change? Businesses do not report suspicious transactions to you out of the goodness of their hearts, but because they have a legal obligation to do so. However, people can use the Internet for their transactions and get around that. If no one sends you that information, you cannot have any knowledge of it. Cryptocurrency transactions or transactions on the dark Web happen without your knowledge, correct?

Mr. Barry MacKillop: Yes.

Mr. Pierre Paul-Hus: We can't say that FINTRAC is on the front lines. It is the agencies or businesses that are on the front lines instead. In this case, Canadian banks or financial organizations must inform you of suspicious transactions that take place on their networks.

Mr. Barry MacKillop: That is correct.

Mr. Pierre Paul-Hus: According to your analysis, what has been the biggest change in the past five or ten years? Is it the cryptocurrency transactions? Regarding cybersecurity, what has changed in the most spectacular way on the Internet?

Mr. Barry MacKillop: I would not say that it is cryptocurrencies at this time. What we see most is that people can transfer money quickly and internationally using a bank, or what we call peer-to-peer transactions. You can do transactions in that way. The Internet allows people to perform quick and complex transactions without going through a financial institution.

Mr. Pierre Paul-Hus: So money transfers are the primary element. If someone wants to send someone $100,000 through the Internet, he will be able to protect the transaction with codes and hide it. Is that correct? And yet at some point the money will land in a bank account somewhere and will be noticed.

Mr. Barry MacKillop: Exactly. Banks have to be vigilant and follow things closely. They know how to spot those transactions.

Mr. Pierre Paul-Hus: Do banks have automatic detection mechanisms? Are they always alerted if a transaction is over the $10,000 limit?

Mr. Barry MacKillop: Yes. They are also informed if transactions are under the $10,000 limit but occur within 24 hours or repetitively.

We work a great deal and very closely with the banks to identify money laundering indicators.

Mr. Pierre Paul-Hus: To me this falls under “Internet fraud”.

As for cybersecurity, our goal is to ensure that citizens are protected. We spoke earlier of phishing and other such schemes. With a view to protecting citizens, have you observed a marked increase in the number of reports in the past four or five years, or even over the past ten years? At what point did this increase occur? We were told that there has been a 41% increase since 2013. Is this a recent phenomenon? Can banks control it, or is it becoming a major issue?

Mr. Barry MacKillop: I would say that it is indeed a major issue, but that the banks do very good work. The percentage of fraud and money laundering disclosures we have received over the past five years has been constant at around 34% to 35%.

Mr. Pierre Paul-Hus: Fine.

With regard to monitoring and disclosure, let's take the example of a problem disclosed to you by RBC. Are authorities like the RCMP informed? Are they informed at the same time as you are? How do things work?

Mr. Barry MacKillop: Authorities are not necessarily informed. It depends on the situation. Banks can indeed transmit information to the RCMP.

Our role, however, is to receive suspicious transaction reports and analyze them. Once we are done, we can alert the RCMP or another police force.

● (1555)

Mr. Pierre Paul-Hus: So in cases of fraud, the bank will act internally, will send a report to FINTRAC, and try to solve the problem.

Mr. Barry MacKillop: Yes.

Mr. Pierre Paul-Hus: So there isn't necessarily a police investigation at that point. Is that what you are saying?

Mr. Barry MacKillop: More or less.

Mr. Pierre Paul-Hus: It depends on the size of the fraud, I suppose.

Mr. Barry MacKillop: That is right. Banks have been fighting fraud for a long time.

Mr. Pierre Paul-Hus: Okay.

Can you tell us about external threats? We are trying to determine how to protect ourselves in Canada, but threats can be internal or external. Can you tell us where they come from, for the most part?

Mr. Barry MacKillop: We mostly see cases of third-party fraud.

Where cybersecurity is concerned, I think the RCMP would be in a better position to tell you whether the threats are mostly internal or external.

Mr. Pierre Paul-Hus: I see. This is outside of your jurisdiction.

Mr. Barry MacKillop: Correct.

Mr. Pierre Paul-Hus: Are there things the government could improve—which you can tell the committee—that would make the work of your organization more effective?

[*English*]

The Chair: That question might be on the borderline of inappropriate given that you're a civil service individual. I am going to allow it in the event that you wish to speculate, but generally speaking—

Mr. Barry MacKillop: We don't speculate.

The Chair: Yes.

Mr. Barry MacKillop: You're correct.

[*Translation*]

The regulations on digital currency exchanges related to Bill C-31 from 2014 are being drafted at this time. They should soon come into effect and this will help us with cryptocurrencies.

[*English*]

Virtual currency regulations will be coming in. We consulted on them last June with the Department of Finance, which had the policy lead for the regime in Canada. There were broad consultations carried out last summer. The regulations are being drafted now to cover virtual currencies, for example, virtual currency exchanges.

[*Translation*]

It will help us a great deal.

Mr. Pierre Paul-Hus: Fine. Thank you.

The Chair: Thank you, Mr. Paul-Hus.

Mr. Dubé now has the floor for seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

I thank the witnesses for being here.

I have questions on your mandate and responsibilities and that of other agencies or police forces. More specifically, I am referring to slides 5, 6 and 7 in your presentation. I'll get back to Project Chameleon later.

How do you go about getting the information you share? You mentioned Facebook, for instance, and the fact that more and more people are sharing information like this.

Are you the ones who identify that information? Do you have employees who monitor social media? Do you then contact police so that they can act and target a particular individual?

The way in which things work is not clear. You mentioned several points, but things are not clear. What is the police's job, and what is yours?

Mr. Barry MacKillop: All investigations are handled by the police. We provide information specific to an entity or a person. We can receive up to 25 million reports a year, including suspicious transaction reports. We have two people who work on them. Their day-to-day work is to study these reports.

The technology enables us to identify certain keywords in order to detect a particularly interesting suspicious transaction. We can then check our database to see whether it contains other reports related to the person concerned. If we reach our threshold, we can proactively disclose the transaction to the police. The police must then decide whether to launch an investigation.

If we receive information from the police as part of an ongoing investigation, we'll check our database, as well as Facebook and other sources, to see whether we can find additional links to include in the report for the police. Our report contains only information from our database or public sources, which we collect for the police. However, the police must decide whether to conduct an investigation.

● (1600)

Mr. Matthew Dubé: I don't want to focus too much on one example, because I know the situation can vary.

When you say that you're looking for connections on Facebook, are you looking for links to content, such as a known phishing site seeking to extract financial information, or to people, such as business relationships that an individual guilty of suspicious transactions might have with a Facebook friend? How do you identify these people and their connections?

I don't see much difference between the police's investigative work and what your organization seems to be doing.

Mr. Barry MacKillop: We provide only information, not evidence. You're referring to tradecraft.

Suppose the police are investigating you, Matthew Dubé. If we check your Facebook page—because we're preparing a report about you—and you're sitting next to Jim Eglinski in one or two photos and there seems to be a link between you two, we could verify in our database whether you've ever transferred money to each other and establish whether you have financial ties.

We don't take everything available on Facebook. It must be linked to our database. If we want to establish links and identify members of your gang, we could certainly do so. However, it would need to be in our database as well so that we could share it with the police.

Mr. Matthew Dubé: I don't want to go too far beyond the scope of our study.

In the fight against terrorism, the way that police officers work generally protects innocent people and prevents them from being found guilty by association. In the example that you just provided involving a transaction with me, who has had issues in the past, the individual would be protected by the police's work. You would simply tell the police that money was transferred between us. It would then be the police's responsibility to check whether an investigation is warranted.

Mr. Barry MacKillop: Absolutely.

As I told you, we receive about 25 million reports a year, and most of them are legitimate. We don't disclose this.

Mr. Matthew Dubé: On page 6, you talk about a public-private partnership and money laundering.

Mr. Barry MacKillop: Yes.

Mr. Matthew Dubé: In the field of cybersecurity, there's a major debate regarding whether the public or private sector is best and how to strike a balance between the two sectors. For example, banks brag a great deal about what they've done, but I imagine that they often work with you. Does your organization have any ideas on how to find this balance?

You're not necessarily here to develop policies, but you implement them. Is there a balance that would enable you to do your job well and that would enable the private sector to continue innovating to protect consumers?

Mr. Barry MacKillop: We're already carrying out three projects as part of public-private partnerships. In this area, we're working with the police and the private sector to develop indicators, whether the issue concerns money laundering related to human trafficking, fraud or the sale of fentanyl. So far, this has been very successful. Everyone seems to be working in their field and doing what they can. They're working very well together. We're receiving many more suspicious transaction reports. We've found that the development of indicators that are as specific as possible for a category of crime increases the quality and quantity of the suspicious transaction reports that we receive.

[*English*]

The Chair: Thank you, Mr. Dubé.

Somehow or another, the Dubé-Eglinski gang doesn't strike you as something that puts fear in your heart.

Voices: Oh, oh!

Mr. Barry MacKillop: I just thought I would bring the members together a little bit.

The Chair: Yes. That is a strange arrangement.

Mr. Spengemann, you have seven minutes, please.

● (1605)

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you, Mr. Chair.

Thank you both for being here today.

I want to spend a couple of minutes talking about terrorist financing, the origin of FINTRAC in 2000 and the impetus in 2001 of 9/11.

I had the chance to work in the civil service between 2003 and 2005 on smart regulations. FINTRAC was an interlocutor in that exercise with the North American security perimeter. It's now 2019. Can you talk about what the trend lines have been for terrorist financing and how you work continuously to keep Canadians safe? I also serve on the defence committee, so there's a direct connection there into that line of work. How important is the work you're doing in the field of terrorist financing today, and what trend lines do you see?

Mr. Dan Lambert (Assistant Director, Intelligence Operations, Financial Transactions and Reports Analysis Centre of Canada):

The issue of terrorist financing is one that has evolved in relation to FINTRAC. Going back to some of the things Mr. MacKillop was speaking to, after FINTRAC was formed and we were working with the banks and so forth, things like fraud were things that the banks were used to and were able to report on quite easily. The threat environment has evolved over time. The banks are looking for increasing assistance from an organization like FINTRAC in relation to being able to track terrorist financing, especially because the amounts used in terrorist financing are usually very low.

We've worked very closely with the banks over the last number of years to provide them with adequate indicators of what to look for in relation to their transactions. In that vein, we work very closely with the Canadian Security Intelligence Service and the national security side of the RCMP. We've had an evolving relationship with the banks in relation to how we disclose.

Mr. Sven Spengemann: It remains as true today, then, as it did then, that the disruption of finance networks is fundamental to our work in the fight against terrorism.

Mr. Dan Lambert: Yes.

Mr. Sven Spengemann: In your assessment, is the reporting threshold of $10,000 still relevant? Are there means to circumvent that in terms of the aggregation of amounts elsewhere through other channels? Is there a layer of analysis that escapes you because of the threshold?

Mr. Barry MacKillop: For the most part, the threshold remains useful. As Mr. Lambert just mentioned, when it comes to terrorist financing, those thresholds mean very little, because we don't see that many transactions linked to terrorist financing that would be of that amount.

What it really comes down to is the type of analysis and the type of work we can do with our reporting entities; the type of education we do; the awareness and the outreach; and the development of the indicators related to specific types of crime, whether it's terrorist financing or others, and how we can get those indicators out. We recently published what we call our STR trilogy, which is really guidance on how to fill out an STR, a suspicious transaction report, and on how we can look in very specific areas, whether it's with money services businesses or others, and at what types of indicators are more specific to them. That's the type of proactive and partnership work that we have to do with our reporting entities that will continue to lead us to quality reporting.

Mr. Sven Spengemann: Okay.

From a criminal justice perspective, is your mandate limited to money laundering and cyber-fraud as far as offences are concerned?

Mr. Barry MacKillop: Money laundering, terrorist financing and threats to the security of Canada.

Mr. Sven Spengemann: Would straight data hacking be part of that mandate, for example, the theft of data rather than the theft of money or the fraudulent diversion of funds?

Mr. Barry MacKillop: No, we wouldn't see that unless it was a hack on a bank and a whole lot of ideas were taken, or there was money taken or ransomware. For that type of hacking, we might see it in the reporting as a suspicious transaction report, for example.

Mr. Sven Spengemann: If it's a hybrid offence, if somebody's involved in hacking but also there's an adjunct fraudulent component to the crime, what's the delimitation of responsibilities between you and whatever other agencies come in to look at the hacking side?

Mr. Barry MacKillop: We would not be involved in that.

Again, we're limited to the reports we receive. We can only analyze the reports we receive and then disclose on those. Unless there were a connection made in an STR, for example, that was specific to that, we probably would not see that.

Mr. Sven Spengemann: Do you work closely with our international partners and allies, specifically the Five Eyes, in the field of cybersecurity?

Mr. Barry MacKillop: No, not in the field of cybersecurity, other than in understanding the use of cryptocurrencies, mixers, how money is being transferred and those kinds of things, and money coming in and out of the virtual currency world. We work with them on trends and topologies and so forth.

Mr. Sven Spengemann: How do you see Canada being positioned within the group of Five Eyes, and maybe more broadly globally, in terms of the effectiveness of the work that we're doing? Are there any gaps that this committee might be interested in exploring?

Mr. Barry MacKillop: I'm not sure that I can speak generally to how Canada is viewed on cybersecurity issues. Perhaps the RCMP may be able to speak to that. In terms of financial intelligence units, we're very well respected.

Mr. Sven Spengemann: The last sort of theme that I wanted to look at is the idea that good cybersecurity in Canada is good for business. In other words, if we have a basic platform of good cybersecurity through public-private partnerships, it will attract foreign direct investment because Canada is a safe place to operate.

To what extent are we doing well on that front with respect to the partnerships you have with banks and the way they are protected against attacks or other ways of financial online cyber-fraud? Is there anything more that we could do and that we should examine more closely?

Mr. Barry MacKillop: Unfortunately, that's a little outside of my mandate. When we work with the banks, we work on their requirements for reporting under the PCMLTFA, so when it comes to the cybersecurity area, unfortunately I'd have to suggest that you speak directly to the banks.

Mr. Sven Spengemann: Okay.

Mr. Barry MacKillop: They do things differently, and I'm sure they have proprietary issues. In terms of cybersecurity, I know they take it extremely seriously, but I can't speak to how well they're doing per se.

Mr. Sven Spengemann: From your perspective, it's their mandate to look after themselves as far as security platforms are concerned.

Mr. Barry MacKillop: I would think so.

Mr. Sven Spengemann: There isn't any support that's coming directly from the government?

Mr. Barry MacKillop: There's none coming from FINTRAC. I can't speak for the rest of government.

Mr. Sven Spengemann: Okay. That's helpful.

Mr. Chair, I'm just about out of time, I think.

● (1610)

The Chair: Thank you.

May I simply ask you, in the 15 seconds that Mr. Spengemann has left, by the time you receive your reports, do your analysis and send it back, is the horse already out of the barn?

Mr. Barry MacKillop: That would depend on the case. In some cases with the horse being out of the barn because the crime has been committed already, quite often very likely yes, and whether or not the ultimate crime has been committed, not always. There is a difference between broad-based money laundering schemes, for example, versus terrorist financing and the ultimate role of committing a terrorist act. I think that money laundering quite often is proceeds of crime, so the crime has been committed; whereas on the terrorist financing side it's proceeds for crime and hopefully we can play a role in preventing that.

The Chair: Thank you for that.

Mr. Motz, please, for five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair, and thank you, gentlemen, for being here.

You indicated—and you made it quite clear and reinforced it—that your role is non-investigative. You receive information as opposed to gathering it. You receive it and then you provide it to the agencies that have a law enforcement or investigative capacity.

With that in mind, can you walk us through the information sharing and how you operate to ensure that either national security, in the right circumstance, or policing agencies have all the information they require and you've received to go after the criminal element? Without giving away secrets, how does that actually look and work in real life?

Mr. Barry MacKillop: Without giving away trade craft.

The reports come in. We have an air-gapped database. Contrary to most financial intelligence units in the world, police, law enforcement...no one else has access to our database, not unless you work at FINTRAC, and that's only if you work on the tactical intelligence side and only if you're working on that particular case. There is "need to know" within the agency as well.

Essentially, the information comes in. Let's say it's a suspicious transaction report and one of the two people who look at this finds some key words. It looks like #ProjectProtect, for example, dealing with human trafficking. They would read through the STR. They would give it to a team leader in the geographic area. STR teams are set up by geography. They would give it, for example, to the central region team leader, who would then take it and do some quick searches in the database to see if in fact we have transactions. They would give it to one of our analysts, who would then take that STR and go through it.

Often the STR, especially with Project Protect, will identify that money went from this account to this account, or this IP address to this IP address. We would take that and search the rest of the database to see if we had other additional transactions that could be brought together to provide a very good picture for law enforcement.

Once we have that, we will put our own case together. We have summary sheets. We have transaction tables. We have i2 charts. We have fact sheets that identify who is included in the disclosure and why. We will do some open source information. We'll also look in our database to see if this is related to any other previous cases on which we disclosed. If so, we will include that. Then we will send that out to the appropriate law enforcement agency.

● (1615)

Mr. Glen Motz: Given that information—it's very helpful, thank you—how do you work with the Financial Consumer Agency of Canada? What information would you share with them?

Mr. Barry MacKillop: None.

Mr. Glen Motz: Do you work at all with such credit rating agencies as Equifax or TransUnion, or anything along those lines, in a manner that would protect the consumers with information like that? If you're getting information....

I take it by the headshake that, no, you don't share information with them either.

Mr. Barry MacKillop: Correct.

Mr. Glen Motz: If that's the case, if you are receiving information about a general theme of frauds that are going on that are impacting Canadians, am I clear on your mandate—that you don't share that information with agencies that could protect Canadians?

Mr. Barry MacKillop: It's not enforceable at this moment in time.

Mr. Glen Motz: Let's say you're talking about the romance scam or other ones like that. Do you put out bulletins that alert consumers through either consumer protection agencies or credit rating agencies that would provide some guidance and protection to the average Canadian consumer?

Mr. Barry MacKillop: Yes, but not on the tactical side. If we're talking strategic general trends, we do trends and topologies. We've done reports on that. We do operational briefs. We've done operational alerts. Depending on the nature of the product, they may be made available publicly and available on the website. They may be sent specifically to reporting entities or they may be sent specifically to an international body, let's say, which will then use that information to create a broader product that would be available publicly.

Mr. Glen Motz: In the seconds I have left, could I ask that you commit to providing the committee in writing with some of those things about how FINTRAC actually works to protect Canadians from those sorts of scams? Would that be possible?

Mr. Barry MacKillop: FINTRAC's mandate is not necessarily to.... That's outside our mandate. We exist to detect, prevent and deter money laundering or terrorist financing. Most of it is on the tactical side. On the strategic side, whatever we have is on the website if it's publicly available. Do we send this directly to FCAC, for example? No. Would they get any tactical disclosures from us? Absolutely not. It would be illegal for us to do so.

All the reporting entities that report to us, we do provide them, if we do operational briefs or alerts or.... Our operational alert on fentanyl, for example, is available publicly. On Project Protect, on the public-private partnership and the indicators related to money laundering related to human trafficking, that is available. That is there. Above and beyond that, there is nothing we would have.

The Chair: Thank you, Mr. Motz.

Ms. Dabrusin, go ahead for five minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

I'm going to work it backwards a little bit, because right from the beginning you said you don't do the investigations yourself—

Mr. Barry MacKillop: Correct.

Ms. Julie Dabrusin: —so you're relying on others to be gathering that information based on certain metrics, I guess, that you have helped them put out to try to figure out what their levels are, and what information they would have to seek out. Then they would provide it to you. Is that essentially—

Mr. Barry MacKillop: If I may, all the reporting that is required is set out in legislation or regulations.

Ms. Julie Dabrusin: Yes.

Mr. Barry MacKillop: They must legally report those types of transactions to us.

Ms. Julie Dabrusin: Do you provide them with any guidance? I thought I understood from some of your earlier testimony that you provide some guidance to them as to what might be a suspicious transaction, or how to fill out your reports, and that type of thing.

Mr. Barry MacKillop: Correct.

Ms. Julie Dabrusin: Then it's on them to develop their own algorithms or their own way of searching out what information they would be providing to you.

Mr. Barry MacKillop: Correct.

Ms. Julie Dabrusin: Do you notice a difference in the quality of the information? Are different institutions better set up to provide you with that information?

For example, there are banks, and then there are street corners—moneylending, quick paycheque types of systems. Do you have the same quality of information coming from both of those types of institutions?

● (1620)

Mr. Barry MacKillop: No. Generally speaking the quality of the reporting we receive as well as the quantity—close to 90% of our reports come from our big major banks—tend to be reflective of their abilities, capabilities and their maturity, I think.

Ms. Julie Dabrusin: Different institutions might have different levels of reporting or quality.

Mr. Barry MacKillop: Correct.

Ms. Julie Dabrusin: Would some of these institutions be outsourcing how this information is gathered by other parties? Some smaller institutions might not have strong in-house capacity. Are some of them outsourcing that capacity?

Mr. Barry MacKillop: They can, yes.

Ms. Julie Dabrusin: I think in a few questions we've been talking about the individuals. There is also tracking of individuals' transactions as part of these algorithms to gather up that information and to see if there's something suspicious and if there is, to move it over to you.

Do you provide any advice on how to make sure that information is kept protected and intact?

Mr. Barry MacKillop: Do you mean on their end or on our end?

Ms. Julie Dabrusin: I mean on their end. We can talk about your end too.

Mr. Barry MacKillop: On their end, no, we don't specifically. We do have record-keeping requirements, but how they protect that is really up to them in terms of how they institute their own protections of private data.

Ms. Julie Dabrusin: On your end, because you get a large number of financial reports—I think you said 25 million—how is that information protected as well?

Mr. Barry MacKillop: It's done extremely well. We have very stringent security, both technical and personal security. We're talking about insider threats as well. Everybody at FINTRAC from the clerk in the mailroom to the director has to have a very high level of security, and it's reviewed. Our intelligence database is air gapped so no one has access to that. We're also reviewed every two years by the Privacy Commissioner to ensure that what we disclose is only what we are legally allowed to disclose.

We also have very strong retention and disposition policies in place whereby we segregate and dispose of reports that we're not allowed to keep after a 10-year period and so forth. We have extremely strong policies and procedures on the protection of privacy because having those is key to the existence and ability of FINTRAC to do its job.

Ms. Julie Dabrusin: Because we're talking about cybersecurity, have you noticed an increase in perhaps outsider probes or attacks trying to get the FINTRAC information that you have gathered? Has there been any uptick on that?

Mr. Barry MacKillop: No.

Ms. Julie Dabrusin: No, so it remains static.

Mr. Barry MacKillop: Yes, and we have never had a breach.

Ms. Julie Dabrusin: That's also good.

Thank you.

Mr. Barry MacKillop: Yes, I'm very proud of that.

The Chair: Mr. Eglinski, go ahead for five minutes, please.

Mr. Jim Eglinski (Yellowhead, CPC): You should never say you have never had one; you better hope you never have one.

Mr. Barry MacKillop: I said we never did. I'm not projecting; it's factual.

Mr. Jim Eglinski: I would like to follow through with what my colleague was dealing with here a little earlier. You were talking about your partnership with the different organizations—financial entities, accountants, the RCMP, and stuff like that. The banks are supposed to report unusual transactions to you. You're saying you're dealing with roughly 25 million a year.

Mr. Barry MacKillop: That's all reports, all told, and 19 million of those would be electronic funds transfers in or out of Canada.

Mr. Jim Eglinski: It concerns me. Are the banks compelled to tell you—and I believe that's what you've told us—if there are unusual transactions going on involving larger amounts over $10,000? Are they regulated to tell the local police authorities or is it only limited to your organization?

Mr. Barry MacKillop: No. They're obliged by law to report those transactions to us. They can certainly adopt their own—

Mr. Jim Eglinski: I just want to give you a scenario, and I'll use Julie, because she used me.

● (1625)

Ms. Julie Dabrusin: I saw you do it.

Mr. Jim Eglinski: Julie gets stung by some foreign entity over the computer and she sends $300,000 to them. The bank lets you know and you look at it. If you think it's fraudulent, which it is, you let the RCMP know. Is there any chance of any repercussions for the criminal from outside of Canada, and is there absolutely any chance for Ms. Dabrusin to get her money back?

Can you tell me of any cases in which the money has been returned?

Mr. Dan Lambert: We work very closely with intelligence agencies around the world to continue to track the money in cases such as this, as does law enforcement.

We don't enforce the law, so as you say, in situations in which money goes offshore, does the investigation continue from an intelligence standpoint? Yes.

In terms of the questions about recovery of the money and prosecution, those would be best answered by law enforcement.

Mr. Jim Eglinski: You're saying it would be an outside agency that would do that.

Mr. Dan Lambert: Well, if it's a foreign jurisdiction you would get—

Mr. Jim Eglinski: Once the money has gone out of Canada, realistically the probability of getting it back into our country is probably zilch, right?

Mr. Dan Lambert: Efforts are made by law enforcement in those situations.

Mr. Jim Eglinski: I had an alarming situation happen between Christmas and the new year in a scenario exactly like the one I was talking about. A senior in my riding was defrauded. His wife found out about it and she contacted the local RCMP who said, “We have no way of returning that money to you. We cannot handle the investigation. There is no probability of your ever getting it back. Contact your member of Parliament and scream and holler. Hopefully he can do something.” So here I am, throwing it back publicly.

We need to address these situations, and I am just trying to get an honest answer. Are we going to be able to accomplish anything with all our different programs—your program and the support agencies that you rely on to give you the information? The banks didn't help. They sent the cheque or the draft over, and it's almost impossible to clean it up after the fact. That's what my concern is. We need to stop them before it's after the fact, and we need to have some way of alerting ourselves. Is there any way of alerting ourselves to these fraudulent people from overseas coming out with these programs and catching gullible persons?

Mr. Barry MacKillop: It's very difficult, in part, when we talk about these types of scams. If the person, Julie, willingly sends the money, it's hard to indicate whether it is a fraud if you're the banker and Julie walks in and says, “Listen, I really want to do this and this is what I want to do.”

We do work with banks and we do a lot of work with other reporting entities to make sure we have indicators that we can develop with them so they can ask the right questions. But if Julie is answering those questions in a certain way, I don't know that Julie would enjoy the bank stopping her from transferring the money if she really wanted to do it.

The Chair: Ms. Damoff, you have a couple of minutes.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Maybe this is a question more for the RCMP than for you, but if a Canadian company has contracted out to a call centre or a business in another country to conduct business for them and then fraud occurs, under whose laws does that fall? Is that Canadian law? For example, if RBC is using a company in India to do calls and there is something fraudulent or a security breach, whose law does that fall under? Do you know?

Mr. Barry MacKillop: No. I think you're correct in that it would be better asked of our RCMP friends or maybe our Justice lawyers. I'm not sure.

Ms. Pam Damoff: Okay.

Similar to my colleague's question, over the holidays I heard about a woman in Milton who was in a similar situation, but it was a much larger amount of money, though. They were all below $10,000—it was a romance scam—so it didn't trigger anything anywhere along the way.

Following up on what Sven was saying, is that number too high? If people are being asked to send $5,000 and then $7,000, it's not triggering anything at the bank because they are answering in a correct manner. Would it be triggered if that amount were lower?

● (1630)

Mr. Barry MacKillop: If it were lower, if the threshold were $1,000, we would see every transaction in or out of Canada that was worth $1,000.

Ms. Pam Damoff: That's right.

Mr. Barry MacKillop: That would be a lot of transactions for us to analyze.

In our experience, what we've seen is that we're probably better off doing the training, the outreach and the awareness and working with our big banks in terms of what the trends and some of the indicators are so that they can identify them. It's as important to identify through the indicators if you're a potential victim and to pass that along to us. We could then pass it on to the police. We have done that. We've passed it on to the police and they've been able to talk to the victim and stop the victim from sending the money on a continual basis.

I'm not sure that it's necessarily a threshold thing, unless you go to a zero threshold. Again, that's a lot of transactions in a database and sometimes when you're doing an analysis and the ocean gets too big, it's kind of hard to find the fish.

The Chair: Thank you, Mr. MacKillop and Mr. Lambert. That's an interesting launch of our study.

With that, we'll suspend for a couple of minutes while we ask the RCMP to join us at the table.

Again, thank you.

● (1630)

(Pause)

● (1630)

The Chair: Colleagues, we're back. We have as our second set of witnesses Chris Lynam and Mark Flynn, who will no doubt introduce themselves. They're both from the RCMP.

Are you leading, Mr. Flynn? We don't have your rank on our list. It says you're director general, but....

Chief Superintendent Mark Flynn (Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police):

Chief superintendent is the official rank.

● (1635)

The Chair: Chief superintendent. The police on our committee know what that means. I don't pretend to know.

Please go ahead.

C/Supt Mark Flynn: Good afternoon, Mr. Chairman and honourable members of the committee, and thank you for the opportunity to speak with you on this issue of cybersecurity in Canada's financial sector.

As introduced, I am Chief Superintendent Mark Flynn, the director general of financial crime and cybercrime within the federal policing criminal operations area.

I'm here today with my colleague Chris Lynam, the acting director general of the national cybercrime coordination unit, who will also provide a brief opening statement following my remarks.

[*Translation*]

I'll start by describing what cybercrime is and the types of activities cybercriminals are engaged in.

[*English*]

Cybercrime includes crimes where technology is the primary target as well as where technology is the enabler or instrument for other types of criminality, whether it is financial crime, including fraud and money laundering, the trafficking of illicit drugs or other national security offences.

Cybercrime is a global problem that is multi-faceted and complex with multi-jurisdictional elements and new and continually evolving technologies that impact the safety and economic well-being of Canadians and Canadian businesses. Canadian businesses and individuals, especially vulnerable members of our society such as the elderly and young people, are targets for cybercriminals because of our relative wealth and open, Internet-dependent economy. ln particular, the financial sector is targeted by cybercriminals both directly and indirectly. ln other words, Canadian financial institutions' systems are attacked from two sides, namely, via a company's infrastructure itself or via the portals through which the company's clients access its systems.

To explain this further, I'll go into more detail. Cybercriminals may attempt to directly compromise the financial institution's computer infrastructure through attacks that grant unauthorized access to the core systems themselves. These attacks are attempts to make a profit through the theft of money from those systems or through the movement of money through those systems, to steal private information or, in some cases, to damage the reputation of the company. These crimes are perpetrated by individuals working alone, organized crime groups or professional cybercriminals employed by larger entities, including foreign state actors.

Criminals also indirectly attack financial institutions by obtaining user credentials or other personal information to gain unauthorized access to individual user accounts. Obtaining these user credentials can be done in a number of ways: by using accessible tools from the Internet to obtain passwords, through social engineering or by simply purchasing large databases of personal information on the dark web. The relatively low cost of these attacks has enabled both malicious individuals and new organized crime cyber groups to undertake these attacks on an unprecedented scale.

The wide availability of a whole new range of illicit cyber tools has given rise to an entirely new cyber environment which consists of a wide range of entrepreneurial actors, including malware developers, infrastructure providers and administrators, and platform data resellers who collaborate with others in global networks or independently offer their services and expertise to others via the Internet for profit. We refer to this as the criminal cyber-ecosystem or, on some occasions, we call it cybercrime as a service.

When it comes to Canada's financial and commercial sectors, the volume and severity of cybercrime affecting Canadians and businesses is significant. Global financial services and institutions continue to be targeted by a range of malicious cyber-attacks that generate significant illicit profits for the perpetrators.

Also, the advancements in technology that can be used to assist traditional crimes such as theft, fraud or money laundering has led to a shift in the way that law enforcement must respond to large-scale cyber and financial crimes. Essentially, what we are witnessing are new cybercrimes and old crimes perpetrated in new ways.

In addition to cybercrime organized crime groups, professional money launderers and international money controllers are no longer bound by traditional methods of laundering money and moving their proceeds of crime.

● (1640)

Dark-web marketplaces, the growth of virtual currencies and complex trade-based money laundering schemes are examples of technology-enabled advancements and criminal techniques that have effectively eroded borders and allowed criminal organizations to set up a truly global footprint and a global reach that's associated with that.

Cybercriminals seek to profit through the deployment of malware, such as banking trojans; a multiplicity of online fraud scams; email compromise; or through extortion events, including ransomware or distributed denial of service, also referred to as DDoS attacks, etc. Any of these crimes can be perpetrated from inside or outside Canada.

These innovative cybercrime techniques reveal that the majority of current cybercriminality is financially motivated, as is the case with a lot of crime. It's about gaining access to money in the end and profiting from it.

While the RCMP has been gaining a better understanding of the scope and magnitude of the threat, challenges do remain. For instance, the global reach of cybercriminals means that law enforcement has to be concerned about criminal actors from around the world, no longer just the criminals who are within our borders. This is an international priority for many law enforcement agencies, which will continue to grow in significance and scale.

Furthermore, policing efforts in the cyber realm continue to face challenges largely due to the cross-cutting nature of cybercrime. It applies to all types of crime and it is borderless, as I stated. The borderless nature makes it possible for cybercriminals to commit their crimes across multiple jurisdictions. One cybercriminal can victimize numerous individuals on a massive scale in a way that is not possible in the physical world.

In response to the threats and challenges being faced, the RCMP's cybercrime strategy guides investigation and enforcement efforts to reduce the threat and help mitigate victimization and the impact of cybercrime in Canada. This approach is built on three pillars. The first is to identify and prioritize cybercrime threats through intelligence, collection and analysis. The second is to pursue the cybercrime and the criminals through targeted enforcement and investigative action. The third is to support cybercrime investigation with specialized tools and training.

The cybercrime strategy includes an operational framework developed to guide the RCMP's federal policing action against cybercrime. As cybercrime transcends all types of criminality, the use of specialized investigative teams is essential. The RCMP's federal policing cyber investigations are undertaken primarily today by our national division cybercrime investigative team. However, it leverages the expertise and other specialized investigative supports, such as undercover operations and tactical Internet operation support, which are necessary to augment the investigative outcomes.

The RCMP also plays a central role in the Government of Canada's overarching priority to provide for the safety and security of Canadians.

At this moment I'll turn it over to my colleague so he has a moment for opening remarks as well in relation to the new cybercrime centre that's being set up for law enforcement.

The Chair: Thank you, Superintendent Flynn.

Mr. Lynam, you have about a minute and a bit.

Mr. Chris Lynam (Acting Director General, National Cybercrime Coordination, Royal Canadian Mounted Police): Good afternoon, and thank you, Mr. Chairman, for the opportunity to speak with you today.

As my colleague touched on, law enforcement is facing several challenges in addressing cybercrime. The traditional Canadian policing model is predicated on the assumption that the offender, the victim and the justice system are largely collocated jurisdictionally. However, as we know, most cybercrimes are multi-jurisdictional, if not multinational, impacting victims across traditional jurisdictions, and this brings into sharp focus the need for a coordinating mechanism.

Law enforcement requires a means to gather information and intelligence regardless of the jurisdiction, and a mechanism to coordinate investigative efforts. It is not efficient for multiple police services to be allocating scarce investigative resources on the same criminal activity in an isolated fashion.

Another key concern is that cybercrime is under-reported and there are varied reporting mechanisms in Canada, which is confusing for the public.

The 2017 Canadian survey of cybersecurity and cybercrime undertaken by Statistics Canada found that about 10% of businesses impacted by a cybersecurity incident reported the incident to a police service in 2017. Despite under-reporting, the number of cybercrimes reported to police in Canada has increased in recent years. In 2017, nearly 28,000 cybercrimes were reported to Canadian police, which is an 83% increase compared to 2014.

The under-reporting of cybercrime prevents law enforcement from connecting the dots and responding to cybercrime on a larger, coordinated and more targeted scale. It also hampers governments in understanding the magnitude and extent of the problem we are facing.

● (1645)

[*Translation*]

In response to challenges and to bolster Canada's ability to fight cybercrime, budget 2018 announced $116 million over five years and $23.2 million per year for the creation of the national cybercrime coordination unit.

[*English*]

The unit will be a national police service, stewarded by the RCMP, supporting and working with law enforcement across Canada. lt will act as a coordination hub for cybercrime investigations in Canada and will work with international partners on cybercrime.

The Chair: I think we'll have to leave it there. You will have to work in the rest of your remarks in responses to Ms. Damoff and others.

Ms. Damoff, you have seven minutes, please.

Ms. Pam Damoff: Thank you very much, Chair.

This was an issue that was actually brought to my attention by a constituent. You talked about various jurisdictions and countries being involved. Many of our banks contract out services to other countries. If a Canadian bank is contracting out, for example, to a call centre in India and there is a hack or a data breach, whose laws apply to that? Who investigates? How can Canadians know that their data with Canadian companies is safe if it's being transferred to other countries?

C/Supt Mark Flynn: It's challenging depending on the technical elements of that contracting. There are different jurisdictional elements to it as to who owns the data, where the actors, the individuals, the cybercriminals are when they perpetrate their offences. It's not a straightforward answer for all situations.

Where a contracted service was for handling calls, all the data was in another country and the person that committed the crime was in another country, there would not be an offence against the Canadian Criminal Code in that scenario. However, in many situations it's difficult to even state with some of the modern technologies that are used for data storage in which country that data resides solely. There are a lot of cloud services where the data is residing in Canada and in another country all at the same time. In some of those situations, there would be contraventions of the Criminal Code. In others, there simply would not. However, we would work with our international partners when there is a Canadian interest to ensure that what can be done to investigate it and hold the individuals to account for their action is done in the Canadian interest.

Ms. Pam Damoff: The laws in Canada or regulations about what financial institutions do share to other countries, if that data...it's possible that you can't actually charge anyone on a data breach.

C/Supt Mark Flynn: Statute policy recommendation would go beyond what would be appropriate for me to make—

Ms. Pam Damoff: That's fair. Thank you. I'm going to turn to your colleague.

I was going to ask you about the cybercrime coordination unit. I'm wondering if you could finish what you were saying, particularly as it applies to the financial sector and its impact on the Canadian economy.

Mr. Chris Lynam: One of the main objectives of the new national cybercrime coordination unit will be to work with the financial sector on a couple of fronts. One is to make sure that information about threats is being exchanged or shared. As well, if the financial institution is a victim or has victims as clients, they will have an easy way to bring that to the attention of law enforcement so that action can be taken.

What's happened to date is, in many respects, there are really good relations among the financial institutions and law enforcement and the RCMP. With this new unit and some other resources that the RCMP is getting in an investigative capacity, it will increase the ability for us to work with the financial institutions to deal with new threats or when they are victims.

● (1650)

Ms. Pam Damoff: What are the ongoing challenges that you're facing when you're addressing and responding to these threats?

Mr. Chris Lynam: For example, if you're meaning if a financial institution is reporting....

Mark, do you want to answer?

C/Supt Mark Flynn: Yes.

The biggest challenge we have today in those reports is the sheer volume of the victimization that's occurring, and the fact that the anonymization that's available on the Internet is being taken advantage of by the cybercriminals makes it much more difficult to track them down. However, we are combatting that through the international collaboration that we have, the much closer relationships that we do have with the financial sector. We are leveraging the resources that many of those large banks and other financial institutions have to secure their own networks and integrating them into our investigative efforts to help de-anonymize or help take advantage of errors that occur while cybercriminals are using the Internet to commit their crimes, to tackle them more effectively.

We've gone well beyond the days of the police saying, “Thank you for the report.” Now we will go and investigate and we will tell you what you need to know. We are working much more collaboratively. In fact, in one significant incident we had recently, we actually integrated security staff and financial institution security staff and private sector cybersecurity expertise into our investigative efforts, and the benefits are proving to be very high.

Ms. Pam Damoff: The banking industry is one aspect, but we're also talking about the impact on the economy when businesses are hacked. You can get everything from small businesses to quite large ones. One of the hotel chains recently had all their data breached. Is there consistency in terms of how businesses are dealing with this? Are there gaps in terms of ensuring that they've got proper security on their systems?

C/Supt Mark Flynn: I would not say there's consistency. We see quite a broad range of responses when a corporation is victimized.

We are working closely in our public messaging to ensure that there is trust and confidence in the police to be able to do something about it. As in the example that the honourable member spoke about earlier, it is not helpful when someone does report to the police and they get a response of, “Sorry. We can't do anything for you.”

We're trying hard to build trust and confidence. That is bringing more people to the table to report. Under-reporting of cybercrime is a significant challenge for us and we need to remove the stigma of victimization that is associated with cybercrime to enable us to learn more about it and tackle it appropriately.

Ms. Pam Damoff: Thank you.

The Chair: Thank you, Ms. Damoff.

Mr. Motz, you have seven minutes, please.

Mr. Glen Motz: Thank you, Chair, and thank you, gentlemen, for being here.

A year or so ago, this committee was tasked with doing a study on Bill C-59, which was a national security bill. In the testimonies we heard from Retired General Michael Day who reported to the committee that he has zero confidence in Canada's readiness to deal with emerging threats like artificial intelligence used in cyber-attacks and quantum computing that could hack through regular security regimens now in a matter of seconds.

With that in mind, how is the RCMP getting ready for that or how are you helping other agencies in the industry prepare for that emerging threat that's occurring right now?

C/Supt Mark Flynn: In the RCMP, our mandate is the investigation of criminal offences. We do have the Canadian Centre for Cyber Security as well as other entities that give advice on the securing of systems and other technological assistance that they provide there.

However, from an investigative perspective or a public safety perspective, we are putting a fair bit of effort into education and ensuring that people are aware of what can occur, that people are taking steps to assume there's going to be a compromise and make efforts to identify when someone unauthorized is in their networks and report to us. Even if we can't do anything about that individual incident, the gathering of the information from that incident along with the other victims who forward information to us can lead to a successful conclusion down the road in holding to account the people who are responsible for multiple compromises.

● (1655)

Mr. Glen Motz: Thank you.

I'm going to take an angle from my colleague Ms. Damoff. I know the position you're in in law enforcement, but I really have to tell you that from experience—and I'm sure Jim can attest to this—if we were in your position, we would say things like, “We wish government would have thought of this” or “We wish this legislation would have considered this”, because you're playing it out in the field. I don't want to put you in a bad spot, but I'm going to ask it differently.

This study is about protecting Canadians. This study is about ensuring that we have legislation in place that allows law enforcement to do law enforcement functions in a manner that will protect Canadians better, that will allow FINTRAC and every other agency that does this to do it better. You don't have to tell us specifically, but in the roles that you gentlemen play now, just give us a general theme as to what gaps you see that we as a committee can start looking at specifically to address those gaps to ensure that everything.... This is all about public safety. This is the public safety committee. Your role is public safety.

No offence, but sometimes it's easy to hide behind “Well, I can't say that”, but I actually think you can say that. From my experience, yes, you can say, “Here are the gaps that I see that law enforcement, that government, that whoever, can look at specifically.” I would offer you the courage to go ahead and do that.

Voices: Oh, oh!

The Chair: I don't think it's an issue of courage; it's an issue of the appropriate role of civil servants, etc., but given the passion with which Mr. Motz struggled with his question, I'm more than willing to have you respond in whatever way you see fit.

C/Supt Mark Flynn: Okay. We both have something to say here, but I'll let Mr. Lynam go first.

Mr. Chris Lynam: What I'll say is that the sheer fact that this committee is looking at cybersecurity and cybercriminality is adding to the conversation about what a challenge it is for not only Canada but also others to determine how to deal with this. The more attention that is brought to either the challenges law enforcement has or how we're going to address them or how other departments, including the new Canadian Centre for Cyber Security, are going to make sure that Canadians and also businesses know how to protect themselves better and what to do when they are victims of cybercrime.... From that perspective, I think bringing more attention to the issue is of importance.

C/Supt Mark Flynn: I'll add to that. The attention that comes to this has to be in a way that removes, as I stated earlier, the stigma attached to it, because I've seen over the last couple of years that I've been involved in cybercrime as an area of focus that a lot of organizations do not report it because of the stigma. When a large corporation is compromised, if it does not report the information to law enforcement or to other organizations through which we can gain access to the information, there's nothing we can do about it. The more we paint them, as opposed to the cybercriminal who actually perpetrated the offence, as the evildoers, the more that drives that reporting down and the more that takes away from our being able to successfully investigate it.

Mr. Glen Motz: I really appreciate that. With that in mind, because fewer than 10% of businesses report cybercrime, is it a feasible ask or suggestion that we mandate reporting cybercrime? Is it feasible to say that if you're the victim of cybercrime, whether you are a small, medium or large business, you have a responsibility to report that to the authorities, however that may look? Is that a reasonable expectation from the Canadian public?

C/Supt Mark Flynn: There would be an interesting challenge that could occur in that.

● (1700)

Mr. Glen Motz: Yes.

C/Supt Mark Flynn: There has to be a balance, as my FINTRAC colleague spoke about earlier, in the threshold for reporting. The system could be inundated with reports alone.

We're very much focused on the trust and confidence and on finding the right balance in the volume of reporting. Through the national cybercrime coordination unit that's being set up, we'll have that public reporting portal. If we have people reporting to police and police aren't prepared to receive the reports and offer sound advice or guidance, such as you experienced or your constituent experienced, reporting alone will not solve this problem. There has to be a balance between reporting and being able to respond, and we have to have the systems in place to be able to receive and make appropriate use of a report when it comes in.

Mr. Glen Motz: Thank you.

The Chair: Thank you, Mr. Motz.

Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé: Thank you, Chair.

I have a few questions about reporting.

The first thing is on the reporting mechanism now that's part of the national centre. I'm wondering how that works in parallel with the new obligations under PIPEDA to report to the Privacy Commissioner, for example. Some of those instances would always be crimes, I suppose, but there's a difference between some of the crimes that might be reported to you versus some lackadaisical attitude towards software patching and things like that. How do those two reporting mechanisms tie together?

Mr. Chris Lynam: In reality, they're not connected. The obligations under PIPEDA are related to data breaches and the regulations around that where the new public reporting system that we'll put in place is voluntary. It involves either individuals or primarily small and medium-sized businesses that want to make sure they have an ability to let law enforcement know they're a victim. The ability of their doing that can help police in their investigative and intelligence efforts.

To the example that was provided here, unfortunately, there will likely always be cases where that money is not going to be returned, but by having a very robust and modern public reporting system that has strong analytics behind it, we could very quickly understand that perhaps 10 other people in Canada have been victimized by that same person or that same cyber entity, moniker or email address. Because of that level of impact—we can see that at a national level—we can then work with other police services across Canada to go after that cybercriminal. Right now that doesn't exist.

Mr. Matthew Dubé: If that's optional, it's hard for me to imagine why a company, if they have an obligation to report already, wouldn't take advantage of the ability to also report it to law enforcement, but there could be a whole slew of reasons why they might not do that.

Does your unit then look at anything that might have been reported to the Privacy Commissioner but wasn't necessarily reported to police? Now it's out there and is probably public, and the commissioner is going to report on it. What's your ability to tackle that afterwards?

Mr. Chris Lynam: We're going to do some outreach with the Privacy Commissioner to understand more how they are handling or managing these data breach reports. Again, under that regime, there's no obligation for that information to be accessible to police. There may be some things on the prevention side or things like that which might be useful, but we're moving forward with a voluntary scheme that has the public or businesses report directly.

You're right. We could have businesses that report to both and we would encourage them to do that.

Mr. Matthew Dubé: Presumably the reason PIPEDA is now forcing these disclosures to the Privacy Commissioner is to make it public because many of these corporations in particular were keeping it under wraps and then it was only coming out two years after the fact. I guess it's like regular police work. If there's no complaint or reporting, then you see it out there but you can't necessarily act on it.

Am I understanding that correctly?

C/Supt Mark Flynn: I'll step in.

If we learn about a compromise that has a significant impact on Canada, there has to be a balance. We will follow up with those companies and encourage them to report to us in detail.

The mere fact that there's been a compromise does not allow us to effectively pursue a criminal investigation. We need much more information than the simple fact of a compromise. It has been challenging at times but we will work with some of those large corporations because it's often difficult to get to the right person to gather the information we need. We do that outreach. We do not have to wait until the organization reports to us. However, it is only an effective investigation when that corporation is willing to work with us in the investigative stages of our response to what's occurred.

● (1705)

Mr. Matthew Dubé: Does the unit have an increased capacity associated with it? In other words, from a technical perspective, has the unit provided law enforcement with additional capabilities that didn't exist when the RCMP was doing it? I'm assuming the same type of collaboration under a different name.

Mr. Chris Lynam: Yes. The unit will not only have new people focused on enabling that collaboration with police services as well as the private sector, but it will be underpinned by a new information management and information technology system to allow information sharing between law enforcement to do some of the analytics, as I mentioned, in the public reporting, to really allow the law enforcement cybercrime capabilities that may be with the local or provincial level to get more capacity.

Mr. Matthew Dubé: I want to jump in with the 30 seconds I have left to talk about people. Are there any challenges—

The Chair: You have more than 30 seconds.

Mr. Matthew Dubé: Okay. That's good, then, but it is running out.

I want to ask, in terms of people, if there's any challenge finding that specialized skill set with individuals who can be afforded the proper security clearance. It's something we've heard in different fields related to cybersecurity. Is that a challenge you're facing both with the unit and with the RCMP also more specifically?

Mr. Chris Lynam: I would say, for anybody, whether in the public sector or private sector, who is looking to hire cybersecurity talent, there's only a limited pool out there right now. There are initiatives to increase that to find the right people who have the right technical background or the right critical and analytical thinking who you can bring in and train to the right level. There are some challenges there.

A lot of the approaches we've developed to date are really playing on that. There are a lot of Canadians out there who want to help law enforcement pursue cybercriminals. They are less interested in working in a cybersecurity field or another field. They want to help serve their country. They may not make as much money as they would in the private sector doing it, but we've had some success in that approach.

The Chair: Thank you, Mr. Dubé.

Before I turn it over to Ms. Sahota, there were 28,000 reported cybercrimes. How many resulted in charges?

Mr. Chris Lynam: Mr. Chair, I wouldn't have that figure in front of me. We can get back to you.

The Chair: In percentages, would it be 1%, 2%?

C/Supt Mark Flynn: It's a small fractional per cent probably on the number of actual victimizations versus the number of charges that are laid.

The challenge in answering that question goes back to the definition of what exactly is a cybercrime, because it includes all of the cyber-enabled crimes whether they be fraud threats over email, compromises on large systems, etc.

The Chair: I'm just working off your figure as to what you say is a cybercrime. Less than 5% and less than 1%? Am I in that range?

Mr. Chris Lynam: To Chief Superintendent Flynn's point, it's probably small. If you would like, Mr. Chairman, we could get back to the committee with the—

The Chair: Basically what you're saying is that this is a pretty low-risk crime from a criminal standpoint.

Mr. Chris Lynam: Yes. Unfortunately, there are a lot of cybercriminals getting away with what they are doing.

The Chair: Okay.

Ms. Sahota, you have seven minutes, please.

Ms. Ruby Sahota (Brampton North, Lib.): Thank you.

It has been referenced many times here today what you feel the gaps may be. I would like to focus on your introductory speech where you talked about the investment in budget 2018 for the creation of this new RCMP national cybercrime coordination unit.

This sounds great, and I know it probably takes time to really get it fully up and functioning. Would you say it is right now, and if not, how long would it take, and what was in place before the creation of this unit?

● (1710)

Mr. Chris Lynam: I will start, and then maybe I will hand it over to Chief Superintendent Flynn, who can talk about the current RCMP resources that are devoted towards cybercrime.

The new unit will achieve its initial operating capability in April 2020 and then ramp up over three to four years from now to achieve full operating capability in 2023, and 2023 is when the full public reporting system would also be in place.

This is a new unit, as you can imagine, for the RCMP. We are hiring and training new people to do that and establishing partnerships with police services across Canada as well as within the private sector and non-governmental sectors. As well, as I mentioned, we're implementing a new IM/IT system to underpin its operations.

Ms. Ruby Sahota: You said in your introduction that there were consultations done, and there was a laxing in two areas and that's why we are where we are.

What was in place before creating this unit?

C/Supt Mark Flynn: Right now, within our federal policing criminal operations area that I'm in charge of, we have quite a few efforts under way to help build trust and confidence, build the relationships with the financial institutions, the banks, the private cybersecurity companies, as well as leveraging our Canadian Anti-Fraud Centre, our federal policing public engagement group, our contract indigenous policing education efforts that are out there, to ensure they were taking on the multipronged approach of partnership. We're leveraging what's already there within the cybersecurity industry, whether it be banks or in private-type security companies, building those relationships, ensuring we understand the problem itself.

As I stated earlier, we would be overwhelmed with the reporting. I'll go back and reflect on my first day in the cybercrime area in federal policing. I asked for a report of every incident, every possible technological attack that was going just against Government of Canada systems. It overwhelmed my email system with two reports, so the volume is too much.

We have to collaborate in our response to that. We put significant effort into it. I'm very much looking forward to the new centre being stood up so that we can appropriately hand over some of those responsibilities to the centre to perform those actions on behalf of all law enforcement in Canada because—

Ms. Ruby Sahota: That's interesting. You say there's under-reporting from individuals and other companies, but you are overwhelmed with the amount of reporting there already is, or incidents that are happening.That's very interesting.

I believe Mr. Dubé touched on it a little bit, the difficulty to recruit cybersecurity specialists. You were talking about initiatives that are under way to increase experts. What are those initiatives? Can you shed some light? Who are the partners in that?

Mr. Chris Lynam: I know within government circles there's an initiative to collectively recruit and hire computer scientists. They are interviewed. There's a screening process. Then departments can follow up with those individuals to see if they're a good fit for specific individuals. Collectively, the federal government has an initiative to bring in computer scientists.

Ms. Ruby Sahota: Is there a partnership with academia when it comes to that? Are we training enough people in Canada? Is there a gap there?

Mr. Chris Lynam: I think there is, as we've seen in many fields, a push to have more cybersecurity folks in Canada in the public or private spheres. I know in the RCMP we've had quite a few discussions and have explored options with different educational institutions about co-op intern opportunities of bringing in students early in their studies. Then it maybe translates into a full-time job once they graduate. We've also discussed with the private sector about interchange opportunities. There is some appetite in the private sector of having their IT security folks come and work with law enforcement and vice versa to exchange skills and what have you.

We're really putting forth a multipronged human resources strategy that looks at universities, current people in the public sector, as well as current folks in the private sector.

Ms. Ruby Sahota: Are you hiring from outside of our borders as well to help when it comes to this?

Mr. Chris Lynam: Primarily, for the public servant approach here to be hired in the government it's Canadian citizens. I know there are some initiatives in some provinces and elsewhere to try to bring in cybersecurity expertise from abroad, but it's not my area of expertise.

● (1715)

Ms. Ruby Sahota: My last question is on the coordination with the local police forces that you were talking about. You were talking about, or previously it was talked about, the romance cybersecurity crimes. In my experience those kinds of crimes were happening even before the cybersecurity part was added in. What I'm finding from people I speak to is whether it involves cybersecurity or not, there's been little the police forces can do about fraud. You willingly hand over your money to someone, and they're gone with it. What is going to be done in that regard to try to lay more charges, as the chair was talking about earlier?

C/Supt Mark Flynn: I'll start with one element, and then I'll hand it over to Chris, because Chris will be responsible for some of this as we move forward.

Currently, we have the Canadian Anti-Fraud Centre. I'm not sure if you're familiar with that organization up in North Bay, which is a partnership between the OPP, the Competition Bureau and the RCMP. They do a lot of amazing work around fraud and understanding the problem. There is also severe under-reporting. We believe there's 10% or less, more likely less than 5%, reporting of fraud. However, that information, when it's collected en masse, is being utilized to shape some of our international operations in dealing with, say, call centres that are in other jurisdictions. There are actual results that are coming from that. A big part of that is understanding the problem, gathering the information, offering support to the victims.

I sat in on some calls when someone has called the Canadian Anti-Fraud Centre. The help that those call takers on the front line can give to those individuals when they call in to say they just lost a large sum of money, or even if it's a small amount of money.... They feel bad because of the fact that they've been victimized. Those call takers do an amazing job in helping those people understand they're not alone. They destigmatize it, help them get advice and guidance on where to go and what to do. It's making a significant difference.

They also have a very important—

The Chair: I'm sorry. We're going to have to leave it there. We have a clock, unfortunately.

Mr. Paul-Hus.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

Mr. Flynn and Mr. Lynam, we've been talking about the establishment of a national unit, which isn't ready yet but will be ready soon. In terms of government business, I'm still bothered by the administrative burden on all departments. We're now talking about cybercrime, a very fast business world. The players involved in cybercrime are either organizations or individuals that operate from home. This type of financial terrorism comes from all over the place.

Do you think that the establishment of the unit, which will cost Canadians over $125 million, will lead to operational efficiencies, or that we'll once again be dealing with extensive administrative structures that will ensure that, in the meantime, the criminals will continue to operate?

I know that it's difficult for you to answer yes or no. However, you may be able to tell me that certain things could be done to improve the situation.

[*English*]

C/Supt Mark Flynn: I can start with that, Chris.

When you say “the centre”, I'm assuming you're—

[*Translation*]

Mr. Pierre Paul-Hus: I'm talking about the unit.

[*English*]

Mr. Chris Lynam: I would agree that

[*Translation*]

the threats, in terms of cybercrime, are constantly evolving. It's therefore important that government and RCMP systems and structures be flexible and responsive to new threats.

[*English*]

What I will say as the person who right now is charged with putting together the new unit is that we did a lot of consultation, both with police services and with the private sector, to really understand how, particularly in the private sector, they are addressing this threat from a cybersecurity perspective. One of the key take-aways we had was that you have to constantly evolve.

We have the ability in building this new unit from the ground up to really push an innovation agenda and build a culture of being adaptive. We've even had success in terms of the funding, the number of positions we've been approved to have and ensuring we have enough IT developers within the unit to be able to change the IT system. If a new threat comes on the market and we need to very quickly change the public reporting systems so that Canadians and businesses can report it, we've accounted for that.

It will constantly be a challenge to try to even just keep pace with the cybercrime environment. From a culture perspective, we're going to do all we can to really make sure that it's not a bureaucratic structure that can't respond.

● (1720)

[*Translation*]

Mr. Pierre Paul-Hus: In September, I had the opportunity to visit the United States. I was able to see the government side and the private side. The Americans are facing the same issues. The government structure is the same everywhere, but their approach includes the private sector, in particular companies such as HackerOne. The American government awards contracts to these companies to increase effectiveness.

You've been talking a great deal about the private sector. Have Canadian companies already been identified as key cybersecurity partners of the Canadian government?

Mr. Chris Lynam: Yes. As I've already mentioned, the partnerships with the private sector are very important for the new unit. The public sector, private sector, police officers and other stakeholders will work together to address these threats.

Mr. Pierre Paul-Hus: From the beginning, we've been in reactive or defensive mode. Attacks occur, and we must then determine whether our systems are effective. You're currently responding to complaints. You find that there aren't enough complaints and you want there to be more complaints so that you can take broader action.

According to the RCMP, are the cybersecurity structures of Canadian financial companies, such as banks and everything related to money, up to standard? There's certainly still room for improvement, but do you think that the banks are doing enough for Canadians?

[*English*]

The Chair: You're going to have to work that into another answer. Unfortunately, Mr. Paul-Hus is out of time.

[*Translation*]

Sorry.

[*English*]

The Chair: Mr. Picard.

Mr. Michel Picard: Thank you, gentlemen.

Maybe to help us focus on more limited angles, because this is a very wide study, what triggered the creation of the unit—the enabler aspect of technology, the target aspect of technology, a new sector of activity? What was the basis for deciding that we need a unit for cybercrime?

Mr. Chris Lynam: There were a few things and you touched on a couple of them. Really, from both the statistics we had and the knowledge about the under-reporting, it was an area where there was victimization going on in Canada that we did not have sufficient resources to address. Canadians and businesses actually also told the government that. When the cyber consultations happened in 2016, addressing cybercrime and making sure law enforcement had a solid coordinating mechanism was part of what they heard in those consultations.

As well, police across Canada, through the Canadian Association of Chiefs of Police, also called for creation of such a unit, both in a resolution and in a pretty dedicated study on cybercrime, which they did in 2015. That led to the creation of the unit as well as to new resources for the RCMP to increase its enforcement capability.

Mr. Michel Picard: Thank you.

We look at past fraud—Norbourg, $135 million, and Norshield, $400 million. In the credit card business, we report close to $1 billion in credit card fraud yearly. Numbers are great, but they target companies specifically.

Do we face attacks—hacking or fraud—that put at risk limited companies still, or do we start to look at fraud or the impact that may affect a whole sector of activity? Let's say that someone hacked the stock market with a service denial attack and they closed down the stock market for one week. Imagine the impact on our economy, which may then create a national security issue.

Where do we stand today in terms of threat?

● (1725)

C/Supt Mark Flynn: My biggest fear today is around the collective threat of all of the smaller compromises that are going on, or the number of small compromises that are used to then gather information that is leveraged in attacks against the banks and other online service providers that are out there.

When you add that small piece from each offence together, it creates some pretty significant numbers. When you talk fraud in general, and just look at seniors in 2017, and realize that there is 22 million dollars' worth of actual reported losses in the small number of reports that we get, that's a staggering number. You have to understand that has a significant impact on all of those individuals.

Gathering that information together, better understanding it and collecting the technical information that allows for investigation of those things is where we're going to have a bigger impact on Canadians. Also, it's important to move beyond just the security, and when we think of large corporations and the amount they invest in cybersecurity, it's appropriate. The attack platform that's out there, the number of criminals around the world who can now reach across the Internet to cause that harm is something they all should be concerned about.

Obviously, we're not on the defensive side; we're on the investigative side. We need to have the appropriate balance between the two in order for us to be able to both protect Canadians from a security perspective and pursue the people who are responsible for it. When we just do security, that allows the criminals to still be out there, to still commit their crimes without repercussions. We have to have an effective investigation going after them.

It's the same as a physical bank robbery. We would not just make banks more secure and throw every armed robber out on the street. We need someone to pursue them, and we have to do that in collaboration.

Mr. Michel Picard: I have 30 seconds.

Your mandate is not to recoup the money but to try to investigate from a criminal standpoint. Is your challenge trying to avoid a fraud occurring? If you find money, money is usually recouped and sent to the treasury and not to the victims.

C/Supt Mark Flynn: Right. We always try to reduce the amount of victimization that goes on. In fact, that's a change that I would say the RCMP can be credited with in some of our international law enforcement conversations, in which we've brought to the table the traditional practice of having an isolated investigation where victimization is allowed to occur to ensure we can investigate without compromising the fact that we're investigating. We're turning that a little bit on its head. We're directly engaging with the financial institutions, as an example, while we're investigating, to ensure that they have the information that we can provide.

Even though it may compromise our ability to pursue the investigation, we feel it's more important to reduce the victimization and reduce the losses as soon as we can. We're doing that in a collaborative manner with them to ensure that we do have viable prosecutions at the end of it as well.

Mr. Michel Picard: Thank you.

The Chair: Thank you for that.

If cybercrime is virtually risk free from the standpoint of the criminal, and that's on a 3G or 4G network, what preparations, if any, are you making with respect to the inevitability of the 5G networks?

Can you answer that in less than 30 seconds?

C/Supt Mark Flynn: For us, the difference between 3G, 4G and 5G from the types of cybercrime that I identified as the one I'm most concerned about is really the speed at which those offences can be carried out and where. There are obviously technological elements. We're concerned about the ability and further anonymization that's permitted by that.

The Chair: So it's speed and anonymization, and we're not catching people right now.

C/Supt Mark Flynn: I would not like to leave you with the impression that there are not consequences. We are becoming much more effective. You've seen some of the news releases out of our national division cyber investigative team and some highly successful operations they've pursued. I believe you'll be seeing some additional news articles in the near future about some other large successes in which there are significant collaborations.

The Chair: We'll look forward to those successes and that good news.

On behalf of the committee, I want to thank you. I appreciate both of you coming and making a contribution to this study.

Colleagues, we have two routine motions.

You have before you a budget for this study. I'm assuming it's acceptable to you. Does someone wish to move it?

Mr. Dubé will move it.

Second, I'm suggesting February 20 as a deadline for written briefs for this study.

With that, the meeting is adjourned.