HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

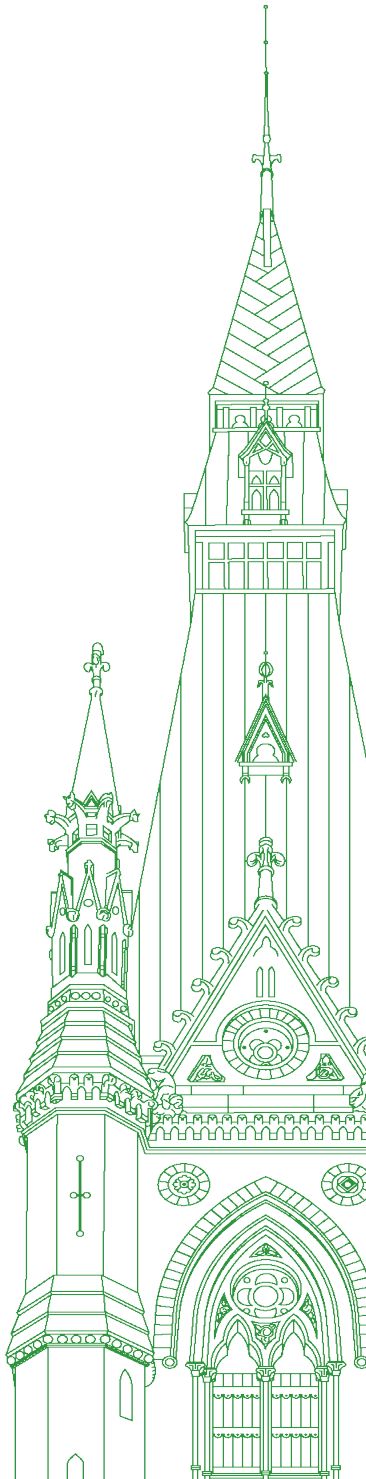
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 036

Monday, October 3, 2022



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Monday, October 3, 2022

● (1100)

[*Translation*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): I call this meeting to order.

[*English*]

Welcome to meeting number 36 of the House of Commons Standing Committee on Industry and Technology.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Monday, September 26, the committee is meeting to study fraudulent calls in Canada.

[*Translation*]

Today's meeting is taking place in a hybrid format, pursuant to the House Order of Thursday, June 23, 2022. I am sorry to join you virtually today. I always prefer to be here in person, but that is not possible today.

However, we are fortunate to have several witnesses joining us in person in the first hour today, including representatives from the Royal Canadian Mounted Police: Superintendent Denis Beaudoin, director, Financial Crime; Sergeant Guy Paul Larocque, acting officer in charge, Canadian Anti-Fraud Centre; and Mr. Chris Lynam, director general, National Cybercrime Coordination.

In the second hour, we have Mr. Randall Baran-Chong, co-founder of Canadian SIM-swap Victims United; Mr. Kevin Cosgrove, digital safety educator and civilian advisor; and finally, Mr. John Mecher, retired RCMP fraud investigator. They will be testifying in their individual capacities.

Without further ado, I will turn the floor over to representatives of the Royal Canadian Mounted Police for five minutes.

[*English*]

Mr. Chris Lynam (Director General, National Cybercrime Coordination, Royal Canadian Mounted Police): Good morning.

Mr. Chair and members of the committee, it is my honour to join you today to discuss the prevalence of fraudulent calls and other scams in Canada, and the efforts undertaken by the RCMP since we last spoke to you on this topic in May 2020.

I'm Director General Chris Lynam. I'm responsible for the national cybercrime coordination unit—the NC3—and the Canadian anti-fraud centre (CAFC) at the RCMP. Joining me today are Sergeant Guy-Paul Larocque, acting officer in charge of the CAFC, and Superintendent Denis Beaudoin, director of financial crimes within federal policing criminal operations.

Before discussing fraudulent calls and other scams impacting Canadians, I would like to briefly outline the mandate of the CAFC and the NC3. First, the CAFC includes a long-standing partnership among the RCMP, Ontario Provincial Police and Competition Bureau Canada. The CAFC works closely with Canadian and international law enforcement partners to combat mass-marketing fraud and other types of fraud, including fraudulent calls.

In 2021, the CAFC aligned its operations with the NC3, another national police service at the RCMP focused on combatting cybercrime. Whereas the CAFC focuses on fraud and online scams, the NC3 focuses more on combatting technology-as-target cybercrime, such as ransomware, data breaches and other cyber-intrusions. The CAFC and the NC3 work closely, given the strong links between fraud and cybercrime, to provide highly coordinated services to the Canadian and international law enforcement communities.

Since our last committee appearance in 2020, the CAFC and the NC3 have seen a significant increase in fraudulent activity in Canada. In 2021, the CAFC received reports of $379 million in fraud losses from victims—a historic year in reported fraud losses and a 130% increase compared to the previous year. At the same time, the CAFC estimates that only 5% to 10% of victims actually report fraud to law enforcement.

Of the reported fraud losses among victims in 2021, more than 70% were cyber-enabled, meaning that the fraudulent activity was committed via the Internet or related digital platforms, such as email or social media. These trends and the convergence of cyber-enabled fraud with other cybercrime activity underscore the importance of collaboration between the CAFC and the NC3, and the need for Canadian law enforcement to continually adapt and keep pace.

Despite the rise in online scams, Canadians continue to be targeted by fraudulent calls at the same time.

[*Translation*]

In 2021, the CAFC received over 32,000 reports where the victim was contacted by phone by the fraudster. Fraudulent phone calls can include attempts from criminals claiming to be law enforcement, the Canada Revenue Agency, banks and other financial institutions, among other types of fraud.

● (1105)

[*English*]

Make no mistake. It is incredibly challenging to investigate and apprehend fraudsters and cybercriminals. Oftentimes, we are dealing with thousands of victims, multiple policing jurisdictions, and cybercrime infrastructure and digital evidence in foreign countries.

[*Translation*]

However, these challenges also acted as a catalyst for Canadian law enforcement. We adapted, accelerated our efforts to collaborate with like-minded partners, and took on more of a holistic approach to combatting fraud and cybercrime.

Various RCMP programs continue to play key roles in several international operations against cybercrime and fraud. However, we also recognize that fraud, in all its forms, is a pervasive and enduring challenge, and we cannot simply arrest our way out of this problem. Our response to fraud requires broader efforts.

[*English*]

For example, in some cases, and where possible, we work closely with domestic and international partners to assist with the recovery of victim funds attributable to fraud. In 2021 the CAFC assisted in 36 instances of freezing or recovering funds, totalling approximately $3.4 million.

Another key aspect to combatting fraud and cybercrime is prevention, outreach and awareness-building. It is a happy coincidence that I am here and able to speak to you in October, cybersecurity awareness month. A key theme to our prevention activities this month includes awareness and prevention material about phishing techniques used by fraudsters. Our prevention efforts are ongoing throughout the year, with another notable month in March focused on fraud prevention. Last year for fraud prevention month we focused on outreach and awareness against impersonation scams.

In conclusion, our efforts over the past few years have been significant—insufficient but significant—and we remain committed to finding new ways to protect Canadians and reduce victimization associated with fraud and cybercrime.

I would like to thank the committee for the opportunity to speak with you today. We welcome any questions.

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

I'll now turn it over to MP Michael Kram for six minutes.

Mr. Michael Kram (Regina—Wascana, CPC): Thank you very much, Mr. Chair.

Thank you to the witnesses for being here today. I guess I should start by saying thank you for all the work the RCMP does. I think politicians and the public at large often take for granted the difficulty of the job that law enforcement has. I certainly want to express my thanks for all the work you do.

Telemarketing fraud is a difficult issue. I'm wondering if you could walk us through this. When you are investigating an incident of telemarketing fraud, how do you go about doing that when the perpetrators are located in Canada versus in foreign countries?

Superintendent Denis Beaudoin (Director, Financial Crime, Royal Canadian Mounted Police): It may not differ that greatly from other types of investigations. If the suspects are in Canada, we're going to utilize the vast tools at our disposal, including production orders, search warrants and other tools. When people are located outside Canada, then we need partnerships and we need to request assistance from foreign governments. Oftentimes, that creates delay. That's the main difference.

There are other differences, but I think that would be the main difference. If you are seeking evidence located outside of Canada, then you're going to need assistance from a foreign jurisdiction.

Mr. Michael Kram: Can you elaborate on how your co-operation with foreign jurisdictions has been going? Has it generally functioned well? Does it generally run into roadblocks?

Supt Denis Beaudoin: Well, I'm sure you would understand that it's very dependent on which country you need assistance from. We have a very strong relationship with countries that are close allies, whereas with other countries it's more difficult. Of course, any type of assistance for evidence goes through the Department of Justice and then through the justice department of the foreign jurisdiction.

There is a process in place, but sometimes we're not able to get the evidence we seek due to a lack of collaboration or willingness from the other country to collaborate. When we talk about complexity, that's definitely one that is at the forefront.

● (1110)

Mr. Michael Kram: When the committee studied this issue two years ago, one of the recommendations in the report was that co-operation in terms of telemarketing fraud be part of future free trade agreements. When we had the CRTC here last week, the witnesses indicated that maybe frameworks or agreements outside of free trade agreements with foreign countries would be more productive.

I'm wondering if the witnesses could share their thoughts on what future frameworks or agreements could be entered into between Canada and foreign countries to reduce this problem.

Mr. Chris Lynam: I'll answer that, although not necessarily about new frameworks. I can talk about some of the measures that exist now.

As Superintendent Beaudoin mentioned, there's both the domestic piece and then the international co-operation piece. That's a big piece of what the mandate of the CAFC and NC3 is about. It's about working with law enforcement partners domestically and then linking those efforts, where possible, to international efforts. That could be bilaterally with other countries and also multilaterally.

A good example in the cybercrime space is that we work quite a bit with the European Cybercrime Centre. They have a specific group, the joint cybercrime action task force, of 18 member states of Europol plus some third parties—Canada, the U.S. and Australia. Out of the Europol headquarters, they are in contact daily, trying to work these international investigations together.

That is a great example of how collaboration at the multilateral level can lead to further investigations and, if not to arresting or prosecuting cybercriminals and fraudsters, to going after their infrastructure. There have been quite a few successes on that front.

Mr. Michael Kram: If Canada were to pursue future agreements with countries that we don't have agreements with yet, could you recommend some countries that should be at the top of our list?

Mr. Chris Lynam: I'm not sure I would recommend countries. I think we would continue to try to deepen the relationships we have with some of the key ones that are working together, as I mentioned, a lot of the European countries and our Five Eyes allies, the U.S., U.K., New Zealand and Australia. Those are the ones we are really working closely with on a lot of these international files.

Mr. Michael Kram: What percentage of the problem would you say is contained 100% within Canada, and what percentage of the incidents are based in foreign countries?

Sgt Guy Paul Larocque (Acting Officer in Charge, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police): This one is difficult to draw a specific number to because, for the vast majority of scam operations, they will try to work over many different jurisdictions. The way criminals operate in that sphere is that they will operate from point A, likely targeting a victim in point B, and then move the money to point C. We often see that when we look at data from the anti-fraud centre.

To say specifically what it is operating from the country.... We're aware there are scam operations originating from the country, but there are also many scam operations targeting Canadians that come from outside, from all over the world. It can be difficult to give a specific number, but what I can tell you is that Canadians are really being targeted by scam operations. The losses we see with reports at the anti-fraud centre speak to that.

Mr. Michael Kram: When it comes to—

The Chair: Thank you, Mr. Kram. That is all the time you have; I'm sorry. Thank you very much.

We will now turn it over to MP Dong for six minutes.

Mr. Han Dong (Don Valley North, Lib.): Thank you very much, Chair.

I also want to thank all the witnesses for coming today. Good morning.

The last report was two years ago, and technology has evolved quite a bit on the criminal or fraudster side. Could you describe to the committee what you have done to keep up with those technology advancements?

Mr. Chris Lynam: Part of the challenge, as you mentioned, is that you're dealing with very highly adaptive people, and they are criminals. They can very easily pivot to adopt the newest technique or figure out what technique works. For example, they will watch what's happening in terms of an incident or a government-type rebate, and they will very quickly be able to figure out how to go and put that scam pitch out to Canadians.

They are adapting technology to enable that as well. As we talked about, we now think that over 70% of the activity is cyber-enabled at the same time. We're working with law enforcement across the country to help them either build or acquire software or share best practices in techniques. There are some things out there now that, if we keep training on them in terms of techniques and what have you, are going to make us better prepared.

It's a bit like they move the yardsticks and then we have to keep moving the yardsticks down the field as well.

● (1115)

Mr. Han Dong: Yes. It feels like you're forever trying to catch up to their technology and their methods.

Do you have any stats on how many arrests you have made in the last two years in Canada?

Mr. Chris Lynam: We don't collect that in terms of the units represented here. I know that Statistics Canada releases regular crime stats on the prevalence of fraud and cybercrime. In some cases, that trend is increasing in the cyber-enabled. That has increased year to year.

One of the additional aspects is that we don't just focus on the arrests, charges or convictions. We try to take a holistic approach to reducing victimization. In some cases, that could be recovery efforts to help people freeze or recover their money, as I mentioned.

Other efforts are to work with different service providers, so if we come across infrastructure, web domains or websites that we think are being used by fraudsters, we reach out to those service providers to say that we think fraudsters are using this. They can then take action to take those offline and what have you.

We also focus a lot, as I mentioned, on the prevention side. We really focus on a holistic approach to tackling and reducing that level of victimization.

Mr. Han Dong: If you could provide the committee the actual numbers of arrests, and how many convictions have resulted from these arrests, that would be very telling. That would be very helpful. If you can figure that out later on and submit it to the committee, I would really appreciate that.

In terms of method, it sounds to me that you are more focused on the prevention and loss recovery, as opposed to investigating and catching the criminals. If the criminals are out there, they're going to find different ways to victimize more people. That, perhaps, is part of the reason the public always feels like we're trying to catch up to these technologies and criminal methods.

To change the channel, last week we heard from the CRTC that telecom industries, or companies, feed data—bulk data—to the CRTC. You report to the CRTC. Do you feel there is a challenge on information sharing between the CRTC and RCMP, or to a unit? At the same time, regarding the telecom and financial industries, are you able to get data from them or flags from them when suspicious activity is going on?

Mr. Chris Lynam: Sure. Actually, I might address one of your questions. I wouldn't want to leave the committee with the impression that police aren't heavily focused on investigating fraudsters and cybercriminals. The mandate of the CAFC and the NC3 is very much about enabling law enforcement agencies in Canada to do those investigations, and the federal policing part of the RCMP as well. There are many investigations under way. I wanted to point out that we don't just do that; we have other activities.

In terms of information sharing with the CRTC and other entities, we operate under what our authorities are in terms of sharing. There is some information we can share with the CRTC and vice versa. Almost any agency would say it can improve information sharing across the board and that would make things better, but there are many opportunities where we share now.

When it comes to private sector entities, like telecommunications companies and financial institutions, we have to be governed by how police operate. If we need information from the police, we often have to get a production order or other type of measure.

There are many opportunities or times when a bank will come to us as a victim and say, “We think we've been victimized,” or, “Some of our clients have been victimized.” There is regular communication, and we have talked about some of the outreach we do when we come across stuff that we think is impacting their clients.

Generally, yes, there is always scope for improved information sharing.

● (1120)

Mr. Han Dong: Is there anything you need from legislators like us?

The Chair: I'm sorry, Mr. Dong, but we have to move to our next round of questions. Your time is up.

We will now move to MP Masse, because Mr. Lemire had to step out for a few minutes.

Mr. Masse, the floor is yours.

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair, and thank you to the witnesses. I know Mr. Lemire will be back soon. I always enjoy his interventions as well.

I'm glad you finished with the last question. Why is this here at the industry committee? This is the frustrating part for me, having been here for a number of years. This is a regulated industry where we allow criminal activity to basically course its way through. That's the telco sector. None of this would take place, impacting our citizens, without the fact that we have spectrum auctions, we allow access to our infrastructure, and we regulate through the CRTC. All those different aspects provide a vehicle for this activity to take place. I really appreciate the efforts that have taken place, not only here at committee but also over the last number of years to make a difference.

What I'm worried about, and what I'm interested to hear further on in the conversation, is that this is very similar to white-collar crime. It seems to escape the grasp of Parliament Hill here in many respects. We go after the workers and we go after the street criminals, but I'm wondering whether or not there are sufficient laws in place.

I'll give a quick example. We saw Rogers recently drop the 911 access from citizens. We saw from the telco industry, from testimony here, that the telcos were not even working together properly to help each other out to protect 911. I'm wondering whether we should be taking the gloves off with our telcos in some respects to get more power or more improvements in order for the RCMP and other law enforcement to get better co-operation.

I'd like your comments on that, please.

Mr. Chris Lynam: Obviously more of a regulatory-type argument or position is needed whereby CRTC and the Government of Canada have more of the mandate in terms of how regulated the telcos are or whether additional regulations are needed. I could say that from the RCMP and law enforcement perspectives, we have good relationships with telcos. We try to work with them as much as possible within our current authorities. I really can't comment on whether the government should regulate this sector further. We focus on enforcing the Criminal Code provisions.

Mr. Brian Masse: That's fair enough. I take pride in having good relations with the telcos too, despite my criticism of what's going on. However, given the results we've received, not only in terms of consumer attacks—the Competition Bureau uncovered and documented the fact that some of the telcos were using improper marketing and aggressive tactics in their own telecommunications efforts—I'm just wondering whether or not this priority service is where it should be.

I know you're not keeping statistics on this, but are there arrests taking place and property seizure of some of the materials and the types of infrastructure? You mentioned in your presentation that some of that was happening. Can you give us a kind of snapshot of whether you are able to get the proper ability to do those things, or is it just basically going after the individuals on the end of the phone? I'm looking for the infrastructure that they're using. I know this is difficult, because you have domestic and international.

Mr. Chris Lynam: I would say it's a combination of both, or it's multi-faceted. In some cases, the RCMP has participated in large multinational operations in which we have participated globally in helping to take down infrastructure—computer hardware, computer servers and other things that cybercriminals or fraudsters need. There have also been pieces here in Canada.

Project by project it depends on the level that is taken. Then there's action also at the municipal and provincial levels as well. There are quite a few success stories in that area, where they've taken action at those levels.

Mr. Brian Masse: I have only a little time left. If there were two things you could get to help deal with this issue, what would they be? Is it proceeds from crime so that you could actually reinvest the money that you're saving Canadians and getting back for resources? Is it law changes or whatever? If there were a couple of things we could do to help you and to help your officers, what would they be?

● (1125)

Mr. Chris Lynam: The one low-hanging fruit I would ask for, particularly in October—cybersecurity awareness month—is that all Canadians really try to be more aware of what's happening out there, and that everybody who has an ability to get the message out, including the attentive folks in this room, be a proponent of prevention efforts. That's a core part of policing. If we can prevent a lot of this stuff up front, the level of victimization will be reduced. I'd say that's where everybody can play a role in really reducing the level of victimization out there.

[*Translation*]

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

Mr. Lemire, you have the floor for six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Mr. Chair. I appreciate your flexibility.

I am sorry if there are redundant elements. Sometimes life as a parliamentarian requires us to be in two places at once.

In the context of fraudulent calls, I am very concerned about the vulnerability of seniors.

Can you tell us if there are any new types of fraud affecting seniors that require greater awareness?

Are awareness campaigns incisive enough to reach our seniors well? Consequently, how vulnerable are they?

Mr. Chris Lynam: I'll let Sergeant Larocque tell you about the vulnerability of seniors in Canada.

At the Canadian Anti-Fraud Centre, there is also a program that aims to help Canadian citizens.

Sgt Guy Paul Larocque: Thank you, Mr. Lynam.

There is no doubt that seniors are a population that fraudsters always seem to target. They are often seen as easy prey.

If I look at our statistical data, the losses associated with seniors—in our case, it's those aged 60 and over—represent about 30% of the losses that are reported to us on an annual basis. That's quite significant.

At the Canadian Anti-Fraud Centre, we have a program in place that provides support for seniors. When detected by our analysts upon receipt of complaints, more vulnerable or at-risk individuals are redirected to the CAFC's Senior Support Unit.

This is a fairly unique and fairly special program in that we have volunteer seniors who come in to help us do this part of the work. These people are often retired and come from industry, either from telecommunications, banking or other sectors. Retired teachers also support us. These people follow up calls with the elderly. In addition, they also help us make presentations to target groups, often to seniors' groups.

Our program is primarily focused in Ontario. We are currently aiming to expand this program from east to west to ensure a greater presence in Canada. Ontario is the province with the largest victim pool as it is the most populous. In that regard, our efforts are well directed there.

We are making other efforts to try to minimize the impact of fraud, whether through our social media awareness campaigns or the many media responses we receive.

For example, in the last year, just at the anti-fraud centre, we have received almost 400 media requests. The media community is very helpful in getting our message out and trying to reach as many vulnerable people as possible.

The most important thing, and often the most difficult, is to encourage victims to recognize that they are victims of fraud and to report their case to the authorities. Reporting fraud remains a key element. Our goal is to understand the schemes that target Canadians so that we can adjust our messages accordingly.

Mr. Sébastien Lemire: What you are telling us sounds important to me.

You say that it is important for victims to report fraud to the authorities so that the authorities can better understand the schemes. You also mentioned the influence of the media in all this.

It's certain that my reflexes are those of a French speaker. If I receive a call in English, I suspect it may be a fraud. I can hang up immediately.

Have you seen any cases of fraudulent calls in French? Honestly, I have the impression that it happens much more in English than in French. What about the French side?

● (1130)

Sgt Guy Paul Larocque: In fact, most fraudulent calls are done in English.

Mr. Sébastien Lemire: This is because of the fact that it is international.

Sgt Guy Paul Larocque: In a mass approach, fraudsters target as many people as possible.

That said, fraud also takes place in French, by telephone. I don't have the information on the extent of fraud and the amount of fraud reports where the initial interaction is in French. However, there are many fraudulent schemes that use the French language. This certainly demonstrates the adaptive model of fraudsters. They will adjust to their "clientele", if I can put it that way, or their target audience, in order to maximize their profits.

Mr. Sébastien Lemire: It is often said that it is people close to the elderly who defraud them. Sometimes they can even operate over the phone posing as a company or whatever.

Is this scheme used by relatives to defraud their own seniors?

Sgt Guy Paul Larocque: I don't have any specific information on that. There is a scheme that we see that is still quite prevalent these days: it's called the "grandparent scam."

Fraudsters pose as a close family member who is in trouble. They have either been arrested, had an accident or need emergency funds. You'll find that these different schemes always involve the same kind of dynamics. There is often an emergency situation. They want people to act quickly.

In the grandparent scam, this is often the case. The fraudster poses as a relative who needs help—it might be a grandchild—and is caught elsewhere, in another province or community. This amplifies the urgency factor and attempts to get the victim to cave in to the pressure and send funds to the fraudster.

Mr. Sébastien Lemire: We had the opportunity to do a study on the subject two years ago, at the initiative of my colleague Mr. Masse, and we are discussing the subject again.

Do you feel that, in the last two years, the issue of fraudulent calls has been treated more seriously and that the recommendations from the first study have given you additional resources?

Sgt Guy Paul Larocque: In terms of resources, on our side, there has certainly been investment in the fight against cybercrime. Our director general can tell you more about the progress on the National Cybercrime Coordination Unit.

[*English*]

Chris, would you like to speak about that aspect?

Mr. Chris Lynam: Yes.

We've made some investments in the last few years to stand up the national cybercrime coordination unit to work alongside the CAFC. It's important because, as I mentioned, there is this cyber-enabled aspect, and it could actually be a combination of phone and online. A recent scam or attack that's often happening is you will click on something or you get attracted, and you give your phone number and other details. Then they call you back and are further able to entrap you in perhaps an investment scam, or they are able, even in real time, to convince you to give access to your system at a company. Then they have a foot in door.

As a result, there have been quite a few investments to stand up the NC3 in the RCMP and stand up additional cybercrime investigative teams to address this with a more holistic approach.

[*Translation*]

Mr. Sébastien Lemire: Thank you.

The Chair: Thank you, Mr. Lemire.

I will now yield the floor to Ms. Gray for five minutes.

[*English*]

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Thank you, Mr. Chair.

Thank you to all the witnesses for being here. Thank you for your service as well.

I want to start my questions today around something that we haven't talked about yet: SIM swapping and phone porting scams, which were brought forth as a concern during this committee's last study on this back in 2020.

It was reported in September 2021 that the CRTC logged nearly 25,000 cases of porting and SIM swapping fraud between August 2019 and May 2020. I was wondering if you had any statistics from the RCMP end on how many criminal reports were filed on this, and how many arrests, investigations, etc., occurred between 2019 and now.

Sgt Guy Paul Larocque: Thank you.

I don't have any specific numbers on SIM swapping. One thing that I've noticed at my centre is that the reporting is low on those instances, but it could also be directly related to identity fraud. If I link that to identity fraud, then obviously I have a significant increase over the past two or three years in terms of identity fraud reported.

On our end, we are under the impression that SIM swapping has decreased with some of the measures that have been put in place by the industry to prevent it. Right now, it's much harder to take the SIM card from your phone and swap it to a different phone without any additional layers of verification to be completed.

● (1135)

Mr. Chris Lynam: I'm just going to add one, and it applies to SIM swapping scams and others.

Folks have probably seen in a lot of their applications the broader application of multifactor authentication. When you go to log in to a bank or something, it's not just your password that gets you in there; you have to do something else, whether it's a text message with a code or what have you, and the application of that is very impactful. It is a great measure to reduce a fraudster's or a cybercriminal's ability to either get into your system or scam you.

As we're seeing that being rolled out further across all types of industry, it is a having a positive effect on reducing things.

Mrs. Tracy Gray: Great. Thank you.

Did I hear you say that some of those numbers might be just lumped all together into fraud reporting in general and that maybe it's not being separated out as much as it used to be? Is that what you are saying, potentially?

Sgt Guy Paul Larocque: It's because we don't track a specific category on SIM swapping. Typically when we get a report of that, it would be subcategorized under identity fraud or identity theft, because we track both.

Over the past two years, as I mentioned, we've seen a sharp increase in those areas, but the main reason that we saw that increase is that there have been many Canadians whose identities have been used to fraudulently obtain financial assistance. With that, we saw the rise in reportings of identity fraud.

As I mentioned with the SIM swapping itself, it's not something for which I have precise figures, so it's difficult for me to give you an exact number when I don't have that type of data.

Mrs. Tracy Gray: Okay. Thank you.

Do you have numbers—and you may not have them here today, but they may be something that you could table—with respect to reports that you get and investigations and arrests? Of course, the CRTC has its reports that it does, but then you have your own investigations. Is that something that you would be able to table for this committee to include with this report?

Mr. Chris Lynam: Do you mean specific to SIM swapping investigations or...?

Mrs. Tracy Gray: It could be, but it sounds as if they're maybe not being separated, so it's just the overall fraud. It would be helpful with this study to have it from your side. If you have any numbers, that would be helpful.

Mr. Chris Lynam: We'll go back and look.

I'll add that, as folks know, the RCMP is not the police of jurisdiction in all parts of Canada, so it might not give the full picture of what's happening at municipal or provincial levels where the RCMP isn't the police of jurisdiction. We'll see what we can find.

Mrs. Tracy Gray: That's great. Thank you very much.

You also mentioned that it's really important for Canadians to be aware, not even specifically around the SIM swapping and phone porting scams, of other types of fraud. Is the RCMP actively doing some type of education campaign, especially during this month? Do you have a campaign that's active right now?

Mr. Chris Lynam: Yes, for Cybersecurity Awareness Month, there's actually a government-wide effort. In many respects, the cyber piece is led by the Canadian Centre for Cyber Security, another initiative that was part of the new national cybersecurity strategy that was released in 2018.

Part of that, as I mentioned, is that this month it's about not getting phished. It's all about phishing. We both have activities that we support. We help out the cyber centre with that under their “Get Cyber Safe” campaign.

As I mentioned in my remarks, we have Fraud Prevention Month in March, which is a big event. Last year, I think we had over 300,000 visits to the CAC website during that month, and we think that through social media we reached about 700,000 people. It does give you a sense that if you craft the—

Mrs. Tracy Gray: Can I ask just one more quick question? I know we're out of time here. I'm sorry to interrupt you.

Mr. Chris Lynam: Sure.

Mrs. Tracy Gray: Are any of those communications in other languages? We know that cultural communities and new Canadians in particular can be subject to fraud. Is there outreach in other cultural communities in other languages?

Mr. Chris Lynam: It is a good point. The majority of those are in the two official languages of Canada, but we recognize that there is a need to figure out how to do more outreach to new Canadians or folks who don't speak English or French. At different levels or, in some cases, the non-profit or NGO sector, there's quite a bit of work in this space, but there's definitely more to be done.

● (1140)

The Chair: Thank you very much.

[*Translation*]

I now yield the floor to Ms. Lapointe for five minutes.

[*English*]

Ms. Viviane Lapointe (Sudbury, Lib.): I'd like to pick up on the questions that my colleagues MP Gray and MP Lemire were asking around raising awareness. I'm specifically interested in how we help vulnerable populations such as seniors.

You talked about what happens when complaints are put forward, but how can we get upstream from that in preventing this for those vulnerable populations? You described some campaigns with 300,000 hits to a website and social media, but a lot of our seniors don't have smart phones and they're not necessarily on computers. What are some of the things that we do to help those vulnerable populations?

Mr. Chris Lynam: I'll start, and then I'll turn to Sergeant Larocque to speak a little more about the senior support program.

I agree. Part of where I think we are now in terms of a program for prevention and awareness is really trying to tailor the approach to different audiences to figure out what resonates with them and what they need in order to stay safe online or not become the victim of a telephone scam.

You're right that seniors may feel more comfortable getting pamphlets or booklets. We've done some work in the past in producing booklets and using other formats, such as in-person meetings or in-person gatherings to promote that. COVID threw a wrench into a lot of that work for a couple of years, but we're now back into that space.

I'll let Sergeant Larocque talk a bit more about the senior support program and outreach activities there.

Sgt Guy Paul Larocque: In terms of outreach, we have proactive presentations that are done in person, to the extent that they can be done. Of course, as Mr. Lynam explained, COVID slowed down our efforts, but we still found ways to be able to reach out. We had virtual presentations when we could not be there in person. Our senior volunteers have now started to do in-person engagement.

Just last week or the week before, one of my communications officers gave a presentation to newcomers. It was great to be able to familiarize them with all of the fraudulent threats that can be out there and to help them navigate through them.

I recognize that prevention will continue to be key. We'll never do enough prevention. There's always more that we can do, and it's always going to remain a challenge to be able to reach as many people as possible.

One thing that we've reproduced at the centre is using the hashtag #Tell2. Basically, if I tell two people about a fraud story or a fraud threat and then they tell it to two others, it will amplify the messaging.

You mentioned senior victims of fraud, who can be more vulnerable and difficult to reach. That's why we ask their families to be able to help us reach out and have those conversations with them.

Ms. Viviane Lapointe: Mr. Lynam, we heard from you this morning—and the CRTC told us the same thing last week—that only approximately 10% to 15% of victims of fraudulent calls file a report.

The question in my mind is how legislators can help increase those reporting numbers. The current process of having to contact the CRTC and complete a form is very onerous for victims.

What if there were a national automated system that all carriers were obligated to implement, through which simply using a code such as *555 would immediately end and block the fraudulent call? It would be reported immediately and it would help us track and trace these calls.

Has that type of system solution been considered?

Mr. Chris Lynam: I'm not aware of a solution like that. I think we need more ideas about how we make it easier for people to report it when they're a victim. It is part of the mandate of the NC3 to work with the CAFC to do that.

For example, we are building and rolling out a new online system called the national cybercrime and fraud reporting system. We started it and went right back to first principles. We went and talked to senior citizens to say, “Hey, if you were to report online, what language would resonate with you? How could we make it easier?” We've redesigned an approach that allows that. We are rolling it out. It's currently in our beta approach. We get about 25 victims a day and we iterate it constantly to make it more user-friendly.

That's just one example. We have to both make it easier and explore different ways to help Canadians report. That information feeds into the ecosystem that can then help investigations or further prevention efforts.

● (1145)

The Chair: Thank you very much.

We'll now turn it over to Monsieur Lemire.

[*Translation*]

Mr. Lemire, you have two minutes and thirty seconds.

Mr. Sébastien Lemire: The last report we adopted contained three recommendations that may concern you.

First, Recommendation 1 talked about data:

> That the Government of Canada work with the Canadian Anti-Fraud Centre, Statistics Canada, provincial governments and police enforcement agencies across the country to improve the availability and accessibility of data on fraud calls in Canada.

Recommendation 2 talked about data and information:

> That the Government of Canada work with the Canadian Radio-television and Telecommunications Commission, telecommunications service providers and police enforcement agencies to increase and improve information available to Canadians about fraud calls.

Finally, there was Recommendation 5:

> That the Government of Canada introduce legislation to facilitate the exchange of confidential information between the Royal Canadian Mounted Police, the Canadian Radio-television and Telecommunications Commission, and other Canadian governmental bodies in order to coordinate an effective response against fraud calls while protecting privacy rights.

So it was about data sharing, information and, particularly, the exchange of confidential information.

Has the government approached you in the last two years to improve practices? Has it taken a leadership role? Finally, have these recommendations been implemented?

[*English*]

Mr. Chris Lynam: Those are three good recommendations.

In terms of the first one, a lot of work has been done to get more data and information out there about fraud. Very shortly, we're going to be releasing a report on the annual activities of the CAFC, which will have a lot of additional data about fraud and what have you. That should be coming out in the next little while.

We're continually looking at information-sharing arrangements with other agencies and what have you. We talked earlier about working with the CRTC on that. I'd say there has been some progress in how we work with them, but there's more to be done.

I'll turn it over to Sergeant Larocque to talk about our open data approach at the CAFC.

Sgt Guy Paul Larocque: Right now there have been recent developments on that front. We want to release more data and make it more accessible to the public, so we're currently working with one of our units at the RCMP to publish that type of data using the open government data concept. For example, some of the reports that we publish are for prevention, like the bulletin reports and things like that. They will be the types of reports that we will look at to be uploaded to that portal, as well as fraud-related data that's coming.

Even for the academic sector, for example, if they want to do research, the data will be a lot more accessible, because some trend data will become available, hopefully, in the near future.

Of course, data will be anonymized to protect victim and suspect information, but the data will still be sufficient to enable some trends to be seen. As Mr. Lynam mentioned, the annual report will also provide some good contextual data as well.

[*Translation*]

Mr. Sébastien Lemire: Thank you.

The Chair: Thank you, Mr. Larocque.

Thank you, Mr. Lemire.

I will now recognize Mr. Masse for two and a half minutes.

[*English*]

Mr. Brian Masse: Thank you, Mr. Chair.

Prevention is everything in many respects. In fact, we have Mr. Mecher coming up. He's a former RCMP fraud investigator. He's been working on the Western Union file. He did an amazing job and will be testifying here.

We actually sent an email out to members of Parliament to try to get that out there. It was taken up by about 10 other members of Parliament. We sent that out twice. It's always hard to get it raised as a priority.

In 2018, the public safety minister then, Ralph Goodale, convened a summit here in Ottawa on guns, drugs, smuggling and so forth. I'd like your honest opinion on whether a summit is a good idea or a bad idea. Are we at the point where we need a summit on fraud or something like that to bring in the provincial, municipal, federal and other legislators to have something more robust for public relations?

I don't want to have meetings for the sake of meetings, by any means. I have enough of those. What I did like about the summit that Mr. Goodale put on is that it bound a lot of people who hadn't worked together in the past. Formal stuff and informal stuff took place later.

Given your time and the commitment, is a summit on fraud and cybersecurity something that would be worthwhile for the country at this point?

You're not insulting me if you just say no.

● (1150)

Mr. Chris Lynam: I think there would be great support for bringing the stakeholders together in different forms—whether it's a summit or some other type of activity—to talk about the impact and figure out solutions.

For example, there is a lot of activity already, with the government recently putting out a call for consultations for the renewal of the national cyber security strategy. That was an avenue both to solicit online input and meet with different stakeholders.

We talk about addressing cybercrime and fraud as being a team sport. It involves law enforcement, other government agencies and the private, non-public sector. I frequently go to conferences or events where that is the theme, and people are in those rooms committed to figuring out solutions to reduce victimization.

I think events or activities whereby we can bring those stakeholders together to say, “This is what I'm seeing and here are some solutions I think I can put on the table” would be beneficial.

The Chair: Thank you.

Mr. Masse, go ahead briefly, if you want.

Mr. Brian Masse: Thanks, Mr. Chair. I'll just follow up with Mr. Larocque.

You mentioned getting multilingual material out to people. For example, to get it in Arabic and other languages, is it just a matter of resources? It is expensive to get proper translation. I know this from my riding and so forth. Is that the case?

Sgt Guy Paul Larocque: It is.

To clarify that, to some extent it's being done in regions. It's not only us producing the fraud awareness piece. For example, we've worked with my colleagues in B.C. They have put posters and pamphlets into multiple languages to alert people of the danger of using a cryptocurrency bank machine, so information is being translated into multiple languages in some regions. It's on a very regional basis, but of course there are always areas where we could improve on that front.

Mr. Chris Lynam: If I could just quickly add—

The Chair: Very briefly.

Mr. Chris Lynam: Yes, part of it is the translation, but we also have to take a holistic view that culturally it might not be the translation. In the approach you take in trying to get the information out there and engaging new Canadians or indigenous communities and people like that, you've got to find the right approach in how you get that prevention message out, considering what resonates with them and how they want to hear and receive that information.

[*Translation*]

The Chair: Thank you.

I now give the floor to Mr. Généreux for five minutes.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

I also thank the witnesses.

Mr. Lynam, earlier you used the words “pervasive and enduring challenge”. As I understand it, this is a persistent challenge. Let us be clear: today's technologies mean that this challenge will remain, inevitably.

Knowing this, what are your goals?

Earlier you mentioned that fraud losses were $379 million and recovery was $3.4 million. Can we link these two figures? The recovery is not even 1% of the losses.

Is this possible? Is my calculation correct?

Sgt Guy Paul Larocque: Recovering money from fraud will certainly always remain a challenge, as the fraudsters' model is very adaptive. Once a barrier or safeguard is established, the fraudster will certainly work hard to circumvent those measures. We see it every day: new frauds surface and old frauds are brought back to life. Prevention remains the key to curbing fraud. As you can see, the amounts recovered or returned to victims are far less than the losses reported.

Indeed, when money is transferred to a fraudster, the fraudster will move it around quite quickly. In the majority of situations, when a bank transfer is made, the funds disappear to other accounts within the same day. So the trail fades fairly quickly.

This is why people need to understand that when faced with a fraudulent request, they need to take a step back, to avoid transferring money to fraudsters. Time is on their side. Unfortunately, when the transfer is made, the hill to climb to recover the funds can be very steep.

● (1155)

Mr. Bernard Généreux: Mr. Larocque, you said earlier that you use volunteers, people who work in telecommunications, to help you set up ways to improve your kinds of research.

Do you use the services of hackers? Do you hire people who were once active on the dark web and have advanced technological knowledge? These people have the skills of the fraudsters, but they would be there to help you and prevent it from happening again.

It's a funny question, but I think...

Sgt Guy Paul Larocque: Actually, that is a very good question. I'm going to let our director answer it, so he can also tell you about one of our sub-units related to cybercrime.

[*English*]

Mr. Chris Lynam: I would say we don't use hackers or cybercriminals, but interestingly, there are good lessons to be learned in terms of their activities and how they conduct their criminal activities or what have you.

By learning that, you can then make your systems harder or figure out how someone got into a system and then adopt the appropriate prevention approaches. There's actually an industry out there involving penetration testing, a service that companies offer. They'll try to get into a network, and in those cases, those penetration testers usually have to fall under a pretty tight regime.

We have to be a little careful, but we can learn lessons from how hackers operate. We learn them and try to incorporate them into how we protect and follow up.

[*Translation*]

Mr. Bernard Généreux: May I...

The Chair: Mr. Généreux, your time is up. Thank you.

Mr. Erskine-Smith, you have the floor for a few minutes.

[*English*]

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

My first question is in relation to some of the numbers on the CAC's website. The dollar amounts seem to track in 2022 to where we were in 2021, with well over $300 million lost so far, and are on track to maybe even exceed last year's numbers, but the number of victims of fraud seems to be tracking much lower. I wonder how you could explain that.

Sgt Guy Paul Larocque: The answer is that on average, losses for victims have increased. There are trends with fraudulent investments, mostly related to crypto sectors like bitcoins or any use of cryptocurrencies, whereby scammers—

Mr. Nathaniel Erskine-Smith: Is there an explanation, not for the disparities, but for why we see a lower number of victims?

Sgt Guy Paul Larocque: Yes. It's because the losses are higher, on average, for victims. We have fewer victims reporting much greater losses. That can explain why—

Mr. Nathaniel Erskine-Smith: No, I'm not asking about the disparity; I'm asking if we're seeing greater success. Is there something you can point to that says we've been more successful, and therefore we see a lower number of victims?

Sgt Guy Paul Larocque: No, sorry. I don't have a specific correlation to that.

Mr. Nathaniel Erskine-Smith: Okay.

[*Technical difficulty—Editor*] measures, have they been successful?

Sgt Guy Paul Larocque: I'm sorry?

Mr. Nathaniel Erskine-Smith: [*Technical difficulty—Editor*]

[*Translation*]

Mr. Sébastien Lemire: Mr. Chair, on a point of order.

There is a sound problem that makes it difficult for the interpreters to work, so I would like that to be taken into account, please.

[*English*]

Mr. Nathaniel Erskine-Smith: [*Technical difficulty—Editor*] The STIR/SHAKEN measures, the very measures that were part of our 2020 report [*Technical difficulty—Editor*] that came forth thereafter, I'm wondering how successful they've been—

[*Translation*]

Mr. Sébastien Lemire: I'm sorry to interrupt you, Mr. Erskine-Smith, but the interpreters can't do their job because the internet connection isn't good enough.

● (1200)

[*English*]

Mr. Brian Masse: I think you were asking about STIR/SHAKEN and whether that's been successful. Is that correct, Nate?

Mr. Nathaniel Erskine-Smith: That's right.

Sgt Guy Paul Larocque: As far as I'm concerned, STIR/SHAKEN is not fully implemented, so it's hard for me to tell if it's effectively working.

One thing we noticed with fraud that is initiated by telephone, though, is that scammers are using a lot of spoofing technologies to make you believe that the number that's calling you is actually local when it's not.

What it tells us at the Anti-Fraud Centre is that it's another example of scammers being very adaptive at finding ways to be able to still connect with their victims.

The Vice-Chair (Mr. Michael Kram): Thank you very much to all the witnesses for appearing today.

We have just completed the first hour of this meeting. We will need a few minutes to suspend the meeting while we switch out the witnesses.

Thank you so much, everybody.

● (1200)

_____(Pause)_____

● (1205)

The Chair: My apologies, dear colleagues. I lost my Internet connection toward the end of the meeting, so thank you to our vice-chair, Mr. Kram, for stepping up.

We are back for this second hour of committee, and with us for this hour are Randall Baran-Chong, Kevin Cosgrove and John Mecher. Thank you for joining us this afternoon.

Without further ado, I'll cede the floor to Mr. Baran-Chong for five minutes for his testimony.

Mr. Randall Baran-Chong (Co-Founder, Canadian SIM-swap Victims United, As an Individual): Good afternoon. My name is Randall Baran-Chong, co-founder of Canadian SIM-swap Victims United.

I'd like to thank the committee for inviting me to reappear because, the last time I was here, the lockdown was announced that afternoon, so I hope not to be the harbinger of another pandemic.

To refresh your memories, number portability, which was introduced in 2007, was designed to enable customers to switch carriers easily while retaining their phone number, but it's something that has been exploited by fraudsters to transfer ownership of a phone number to themselves, often by manipulating the customer service representative of a telco.

Once in possession of your phone number, they take advantage of SMS and text-based authentication methods and click “forgot my password” to take access and control of the victim's accounts. If you think about it, that can be everything from your email to banking to cloud storage to crypto-wallets. Within our organization of over 20 victim advocates, we have people who have lost possession of all their data, had hundreds of thousands of dollars stolen, and, in my case, had a livelihood threatened with extortion.

What has happened since that last fortuitous meeting? As part of its November 2020 report, this committee—with a few different faces now—had two key recommendations, which I am paraphrasing. One was that a hearing be held and, in the absence of that, legislation.

The minister responded by saying that we entrust the CRTC and the wireless network portability council, which is composed of the telcos themselves, to handle it and do its job of self-enforcement, and that legislation is unnecessary, as unauthorized porting is covered as a crime.

I can speak for almost all victims in our group that our issue is not with criminal enforcement of this issue or with the perpetrators themselves; it's a real matter of distrust of the telcos and their regulator. To do something probably never done in this chamber before, I'm going to quote rapper Ice-T. Our attitude is more, “Don't hate the player, hate the game”.

What I mean by that is we know that criminals will always look for vulnerabilities to exploit, but it's the system, the telcos, that we entrust to protect our personal information that do the math of what it costs to prevent these frauds versus the near-zero cost of punishment they bear in the event of failure, and the regulator that exists to protect the public has failed us. In fact, both of them have been thus far dismissive, unsympathetic and ignorant of victims.

Since our last meeting, the following has been revealed: It's more prevalent than most people thought.

Ms. Gray alluded to this. An access to information request filed by a Globe Telecom reporter—who ended up being a victim of SIM-swap fraud, ironically—revealed 24,627 cases, to be exact, of unauthorized ports over the 10-month period of August 2019 to May 2020. That represented 1% of all ports.

Compare that to credit card fraud, where only 0.17% of transactions are fraudulent. At a peak, 2.5% of all ports were fraudulent. Its magnitude can be massive. Two Canadians, one in Montreal and one in Hamilton, have been charged with stealing between $40 million and $50 million in cryptocurrency and other credit card fraud in Canada and the United States.

Meanwhile, other victims in our groups are attempting to recoup millions in stolen funds due to telco customer service representatives surrendering personal information to fraudsters, enabling execution of the unauthorized port.

Finally, telcos have self-enforced in the meantime, and unsuccessfully in the beginning. After a number of failed attempts to address the problem, they introduced text notifications around the summer of 2020. This continues to fail. We know this because of victims who emerged afterward. There is a group of 14 that we are aware of who were attempting to recoup several million dollars back in 2021. Telcos have failed to prevent the exploitation of their representatives and they apply the practice inconsistently.

The fact remains this: Our digital identities and our phone numbers are only growing in criticality. Your SIM is the new SIN number—that is, until SMS-based two-factor authentication is replaced wholesale.

The second point is that the safety of our digital identity is as strong as the weakest link and, in this case, telco customer service representatives, CSRs, are the weakest link in the line of defence of our phone numbers.

Investigations have revealed phone conversations and chat logs of CSRs being socially engineered into providing information to fraudsters. This speaks to a lack of training, misaligned incentives to prioritize customer throughput over customer protection and a lack of punitive measures for the telcos themselves in the event of failure.

● (1210)

Finally, it remains that progress and practices around unauthorized porting remain opaque. The fact that we were unable to produce numbers and that they can only be produced through access to information requests speaks to that. There is no proactive disclosure of data on incidences or effectiveness of practices.

We need to have a hearing to get a more thorough understanding of the situation and response situation and allow for victims to be heard. Second, we need to codify rules that create consistency and durability in practices, including transparency in metrics. Third, we need to introduce enforcement for non-compliance, as I suggested back in 2020 when Australia introduced fines of up to 250,000 Australian dollars for non-compliance.

These three recommendations are all supported by over 12,500 Canadians who signed an OpenMedia petition to that effect.

Let's not wait another pandemic for things to happen on this. I welcome your questions, and a way to a cure.

Thank you.

The Chair: Thank you very much, Mr. Baran-Chong.

I'll now turn it over to Mr. Cosgrove for five minutes.

Mr. Kevin Cosgrove (Digital Safety Educator and Civilian Advisor, As an Individual): Good afternoon, everyone.

I'd like to thank the committee members for offering me this opportunity to speak today.

My name is Kevin Cosgrove. I'm a network technician, educator and digital safety advocate in Windsor-Essex County in Ontario. I've been working in the IT field for almost three decades, but I've shifted to working more with actual people, through contacts, throughout our community. I've been working with law enforcement on digital fraud and educating the public in that area.

I teach classes each semester with seniors specifically. As we know, seniors are a major target for online, digital and phone fraud. In the stats I receive way down at my end of things, almost 25% of the victims of fraud are seniors. Each year we spend time with local police and educate seniors on how to avoid fraud.

I know this committee has certainly focused on things at the higher levels—dealing with the telcos and other things at international levels—but I'm the guy down in the trenches having the little old lady coming to me, telling me she got scammed, needing that type of help, and asking who she should call.

My biggest frustration in working at a local level and being an educator specifically focused on these matters is that the information is already available and out there. The RCMP, especially, has a phenomenal amount of information. When I speak to people in my classes, however, no one's heard of it. It's not that the RCMP is not doing a good job or is not doing any outreach, but when I speak to people, they're unaware.

As the committee is aware, the RCMP has a fabulous publication known as *The Little Black Book of Scams*. It's a wonderful publication, and they've had it for quite a few years. After doing this for almost 20 years, I only know one person who saw a physical copy of it. That's definitely an issue with some of the programs we have; some of the education and outreach we're getting from the RCMP isn't necessarily getting down to every level.

Of course, there's also sometimes a disconnect when the RCMP is not the leading authority in a jurisdiction and relies more on local police to deal with that. They're doing their own jobs. Basically, each little area we're running into is trying to reinvent the wheel instead of having a unified response to some of this stuff.

A big focus I have, when I'm teaching seniors and putting stuff out in the community, is making it accessible. When I got into doing this almost 20 years ago, I noticed that the focus on details, definitions and such things is unwieldy for the average person picking up a pamphlet and trying to understand it. I'm not disparaging some of the information out there, but an 84-year-old woman does not care what the differences are among phishing, smishing, spear phishing or whale phishing. They don't care about those types of details. They need information to keep themselves safe without reading a PSA, a public service announcement pamphlet that goes in the wrong direction for educating the public.

I'm definitely ready for any questions you may have. I think I had a few questions for the RCMP when I was sitting back there. However, that's not my place.

Thank you very much for the opportunity.

There was some mention earlier about STIR/SHAKEN and what kind of progress has been made there. Even though I'm a civilian, I speak with criminal intelligence analysts at the CAFC and the financial crimes unit in Windsor. According to them, the types of calls that are specifically targeted by STIR/SHAKEN have diminished. People are no longer reporting receiving calls that say "Canada Revenue" on their phone. They may see that exact same phone call show up as a long-distance number, but in terms of a spoof call being displayed as law enforcement or Canada Revenue, that has definitely decreased, according to the information I've been given.

● (1215)

[*Translation*]

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

I'll turn the floor over to Mr. Mecher for five minutes.

[*English*]

Mr. John Mecher (Retired RCMP Fraud Investigator, As an Individual): Greetings. Thank you very much, Mr. Chair and honourable members of the committee.

My name is John Mecher—that rhymes with teacher—and I was with the RCMP for over 32 years. During that time, I spent approximately 10 years investigating fraud, mostly in the greater Toronto area. I've investigated various frauds, including the infamous CRA scam. After I retired in 2019, I continued my work in a volunteer capacity to create fraud awareness.

Although I'm open to discussing many aspects of fraud, including organizational and governmental missed opportunities, I've chosen to focus on a foundational component of fraud prevention. Specifically, I will speak to the difference between "fraud awareness" and what I call "meaningful fraud awareness".

First, it's always good to reiterate the losses, which continue to escalate year after year and are currently at an all-time high. As per the Canadian Anti-Fraud Centre, last year those losses rang in at over $383 million. Worse yet, that amount, as per the Canadian Anti-Fraud Centre, only represents 5% of the actual losses.

What we're looking at in Canada is that fraud has become a multi-billion-dollar enterprise for fraudsters all around the world. Those same fraudsters tend to prey on people I describe as traditional fraud victims, such as seniors, newcomers, refugees and the intellectually challenged. Although I can offer several egregious examples of fraudsters targeting members of those communities, I must remind everyone that just about anyone, given the right set of circumstances, can fall for a scam.

It's also necessary to remember that the victim impact often goes beyond simply a financial hit. In some cases, the victim's life savings are wiped out, and that's often never recovered. Sadly, victims also face layers of emotional impacts, ranging from embarrassment to depression, and in extreme cases, unfortunately, many victims end up taking their own lives.

Specific to phone fraud, even though these scams have been around for decades, we have yet to implement measures that have been able to reduce their ease of access to our phone systems. Statistics from the Canadian Anti-Fraud Centre reinforce that point, as the phone has been and continues to be the preferred method of solicitation for fraud.

Furthermore, with a view to the CRA scam that arrived in Canada in 2014, along with subsequent variants, I remain unconvinced that there is any sense of urgency in creating a barrier to the exploitation of our phone systems. To that end, we also need to be aware that we can't rely on enforcement—albeit necessary—or the courts as a meaningful deterrent for fraudsters. Unfortunately, we're not left with many options to protect our fraud-vulnerable communities.

All that said, fraud awareness is the solution, and that needs to be employed. However, it needs to be employed in a meaningful, relentless and focused manner, but that is something that does not always happen. If the status quo approach to fraud awareness worked, we would not be seeing losses growing on a yearly basis. At the same time, although many people in Canada do great work on this front, we need to do much more, and we need to do it now.

Although fraud awareness can involve websites and social media, if potential victims are unaware of those platforms, it's pointless to believe that a series of tweets or online posts can create meaningful fraud awareness. From my perspective, the golden rule of meaningful fraud awareness must be driven by our ability to get the message to those who need to hear it the most. In failing to do that, we will continue to see further victimization.

Lastly, I'm willing to work with any parliamentarian in a non-partisan manner, just as I did with Mr. Masse on the Western Union file, which was a once-in-a-lifetime opportunity for victims of fraud to recoup losses.

Thank you.

● (1220)

The Chair: Thank you very much.

[*Translation*]

Mr. Deltell, you have six minutes.

Mr. Gérard Deltell (Louis-Saint-Laurent, CPC): Thank you very much, Mr. Chair.

Gentlemen, welcome to your House of Commons.

[*English*]

I have a question for all three of you, but first of all I would like to address some points with Mr. Cosgrove about the RCMP.

Your testimony is quite interesting. If you meet any RCMP officers in the corner, you can talk to them. They are very open-minded. Don't be afraid.

Mr. Cosgrove, you raised an issue about the fact that the RCMP have many tools, but unfortunately, people don't know that. Does that mean that people are not informed or does it mean that the RCMP hides some information?

Mr. Kevin Cosgrove: On my level, and just from the education side of things, I do look into the CAFC and the RCMP and the resources that they have, and the resources are excellent. I sometimes rewrite things for my own classes or I just use their own materials. There's no need to reinvent the wheel with some of this stuff. In just talking to people, many of them don't know it's there.

I can't speak at all to why there's not enough information given out, or a split in jurisdictions where local law enforcement or the RCMP are not taking a local interest. I'm not sure of the exact reason. The material is there. On your side, and the committee's side, of course, you have an interest in the actual statistics and the numbers. The average person is not interested in accessing that information.

In terms of fraud prevention, awareness, and everything else, I teach a special program with our local university. It's for people 55 and older. I've been doing it every semester for eight years now, and there's always a class that signs up. I also do talks with our regular police. The interest is definitely there. There's no question about that. I have people coming to me, and not just me, trying to chase people down and put pamphlets into their hands, but the information is already available. People can look this stuff up online. They can get pamphlets. They can visit their local police. There's an unlimited number of ways people can be educated to prevent this stuff, but somehow there's a disconnect. That's why I've been focusing my own work, even working with MP Brian Masse, on trying to educate the public specifically.

It's been going well. I'm hoping that after a few years there will be a big hole in a map where reporting and fraud happens. That might be a little optimistic, but getting the information, as far as I'm concerned, does not require SHAKEN/STIRRED. It does not require enforcement. It doesn't require U.S. law enforcement co-operation. If every person whom I've reached so far knows what a scam is, whether it's through SMS, text, online, or a phone call, they can identify the fraud in the first place. None of the other approaches is effective.

● (1225)

Mr. Gérard Deltell: Mr. Cosgrove, we don't have any RCMP people at this committee, but we have a former RCMP officer in Mr. Mecher.

Mr. Mecher, I would like to know what your thoughts are when you hear Mr. Cosgrove talking about the fact that there is plenty of information, but people are not aware of that information.

Mr. John Mecher: That actually speaks largely to what I was talking about, and I couldn't agree with him more. Having the information isn't the issue; getting that information to those who need it the most is the issue. That speaks to having a proper communications environment.

I want to reiterate that there are many people doing good work. A case in point is what Mr. Cosgrove is doing. From a national perspective, it's my humble position the RCMP, and by extension the federal government, doesn't see fraud and fraud awareness as a priority.

To be fair, during my time within fraud, I've never seen any federal government actually pursuing fraud or fraud awareness as a priority, so this is not something unique to just now. The only thing that's more pressing now is we're seeing losses completely off the charts compared to what we were seeing 10 years ago.

Mr. Gérard Deltell: We should keep in mind that you're only talking about 5% of the losses that were identified. We are losing billions of dollars.

If I have enough time, Chair, I would like ask Mr. Baran-Chong a question.

Mr. Baran-Chong, I deeply appreciate your comments. I want to get back to the third recommendation you made. Maybe I was not aware very much, but you talk about those who are not complying and that there is an obligation to comply.

Can you explain your third recommendation?

Mr. Randall Baran-Chong: I believe my third recommendation was around what the Australian communications commission did. What it did was introduce a process, which was very similar to what we proposed back in 2020, that essentially there had to be an authorization by the customer to execute the port. If the company did not comply with that, for every incidence of the company not doing that, there would be a fine of up to $250,000. One of the Australian carriers has paid over $200,000 for 15 instances of non-compliance. They didn't go for the full max for each instance, but certainly it happens, and we've seen the reductions because of that policy, so there is that deterrent element.

● (1230)

Mr. Gérard Deltell: Do I have enough time, Mr. Lightbound?

[*Translation*]

The Chair: You have 20 seconds, Mr. Deltell.

[*English*]

Mr. Gérard Deltell: Thank you so much, everybody.

[*Translation*]

The Chair: Thank you.

I give the floor to Mr. Gaheer, for six minutes.

[*English*]

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Mr. Chair.

Thank you to the witnesses for making time for the committee.

Mr. Baran-Chong, you were slightly critical of telcos, and I say that with sarcasm, obviously. You say in your own words that they have been “unsympathetic”, unhelpful, and that they have quite literally failed.

What are the missed opportunities? What could they be doing better to prevent fraud?

Mr. Randall Baran-Chong: I guess it's because it's equally personal, since I'm a victim myself. Since then, I have been able to hear the recording from the police of the customer service representative who impersonated a Rogers employee, called the Rogers store, and essentially got my information. It was surrendered very easily. The scammer essentially impersonated this employee and was able to provide a customer number and all the other stuff. I think it speaks to a broader problem within the telcos and the ability to socially engineer and exploit these folks.

I think part of the problem is that if you think of an incentive, I can tell you an outcome. The problem is that these customer service reps—and I have sympathy for them—are not very highly paid and they are not very highly trained. A lot of their metrics are based upon how many customers they can get through during their shifts. What's the satisfaction of that? Their incentives are more to.... If someone wants to try to port their number, let them do it. They don't want to put up resistance. They don't want to challenge whether this is the right person or things like that. If the incentives continue to essentially enable them to focus more on throughput, business outcomes and things like that, versus protecting customers' privacy and information, then I think this problem will persist.

The second thing in terms of awareness is that there is, of course, the broader awareness of good hygiene. Let's move away from SMS-based 2FA. This is something that the Federal Communications Commission in the United States has been promoting, as they consider SMS-based 2FA and SIM swapping a national security threat, but there's also the corporate awareness. For example, when Rogers introduced its text notification form in its first failed attempt at 2FA, customers thought the text notifications were frauds. They thought they were spam as well, but it's because of Rogers' practices being so obscure and their not sharing these practices that customers weren't aware that this was trying to protect them.

There are many different opportunities, and a lot of them emanate from the telcos themselves.

Mr. Iqwinder Gaheer: Thank you.

You also are critical of two-factor authentication. Are there alternatives, or what would you recommend moving to?

Mr. Randall Baran-Chong: Yes. I'm more critical of SMS-based two-factor authentication because the vulnerability is that once the number is stolen from you, the SMS goes to the fraudster. However, there are other things out there like app-based two-factor authentication. You may have heard of Google Authenticator, which is very commonly used.

The problem is that there was a Princeton study of 140 of the most popular websites. With regard to many of these websites, the first factor of authentication they promote is an SMS-based two-factor authentication. We need to move away from that, especially for these critical industries.

I can tell you that some of these banks within Canada still use SMS-based 2FA, and that's their only form of two-factor authentication. We need to really look at moving away from this if that vulnerability and that distrust of telcos persists.

Mr. Iqwinder Gaheer: In your testimony, you also said that there was no data released on the incidences. That strikes me, because shouldn't the CRTC be collecting that?

Mr. Randall Baran-Chong: Oh, I'm sure they collect it, but they just don't want to share it. The only way this person—a Globe and Mail telco reporter, ironically—was able to access it was to file an access to information request to get that information.

PIAC, the Public Interest Advocacy Centre, has requested it multiple times, and the CRTC has written letters saying that no, this is not in the public interest or that this would compromise, potentially, the security of individuals and security in the telcos.

It's an absurd argument, in my opinion, for defending the telcos.

Mr. Iqwinder Gaheer: That's great. Thank you so much.

Mr. Randall Baran-Chong: Thank you.

[*Translation*]

The Chair: Thank you, Mr. Gaheer.

I now give the floor to Mr. Lemire for six minutes.

● (1235)

Mr. Sébastien Lemire: Thank you, Mr. Chair.

Mr. Cosgrove, you were present in the room when RCMP officials testified. We asked questions about seniors. I did, my colleague Viviane Lapointe did, and perhaps other members as well.

Were you satisfied with the answers you heard?

[*English*]

Mr. Kevin Cosgrove: Yes, I was. I have communicated with them over the years, even just in doing my local programs and education. They have reached out to me.

As far as further support or being able to take basic information that we've had available and working more hand in hand goes, no, it's not really something that I've had experience of, whether that's because we're down in Windsor and just off in the corner, or because we have our local police to deal with it. That part I can't speak to.

There are times in doing the things that I do—working with our local police or doing education and working with our university—when I definitely do feel like I'm operating a grassroots program that shouldn't be grassroots after 10 years. More support, regardless of the direction, would definitely be a benefit.

I have looked at their own materials. I certainly have nothing to disparage about that. It is good and sufficient material. It's very elaborate, but whether or not it's getting to everybody is the question we're probably looking to answer here today.

[*Translation*]

Mr. Sébastien Lemire: Many of our recommendations are along the lines of better collaboration, greater transparency, data sharing, particularly with industry and government agencies.

Do you feel that this collaboration is sufficiently practised at the moment? I imagine you heard the CRTC's responses last week as well.

I'd especially like to know what more we could be doing, at this point.

[*English*]

Mr. Kevin Cosgrove: It's to make the information more accessible. As I said, having higher-level programs or information is not the information that people need. It's very detailed. It's sending potential fraud victims a dictionary and just hoping that they read the whole thing instead of boiling it down to just what the fraud actually is all about and how to avoid it.

For most fraud, it doesn't really matter if it's through a text, a phone call or an email: These are the same types of scams that they're using. You can get an email about cryptocurrency or have a phone call about investing in cryptocurrency. The method doesn't matter.

From what I've seen, there is a lot of focus on information that spends too much time on the methods, making some of the information seem like it's over people's heads. I focus on dialing things down and keeping things straightforward. There's a publication that our local businesses, the Windsor police and a few other private donors actually funded for publication. That was put out through the community, and the reception from it was phenomenal. It's not taking the high-level information and seeing how much we can give to the people or how smart I can make myself seem; it's about how we can take that information and present it to people so that they're going to find it useful.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

Mr. Baran-Chong, I think you would have a lot to say about this. So I'll ask you the same question.

What is your view on the current state of the industry, and more importantly, what are the recommendations to ensure that we actually improve the situation?

[*English*]

Mr. Randall Baran-Chong: Thank you.

When our group saw the recommendations from this report, we were actually quite appreciative, because I think they essentially reflected what we had asked for in terms of supporting a hearing. The response, I believe, from the ministry about the hearing was that they didn't feel it was appropriate to have a hearing because they didn't want to solicit views from the public on how to protect themselves—which I thought was somewhat silly, because where the telcos have gotten to now is based on a recommendation we made back in 2020. However, because they have dragged their heels or have not listened to us, more victims have accumulated in that time.

The second thing is that they don't understand that a hearing is not just to, let's say, solicit recommendations or things like that. Many of these victims do not feel heard. You may recall that you asked me back in 2020 how Rogers had responded to my fraud case. They offered me $100. Their customer service representative gave away my information, which took away all of my data. The scammer threatened to destroy my life, to destroy my career, unless I paid $25,000. That's what they asked from me, and Rogers wanted to give me $100 for that. That was the apology.

Other folks who have lost hundreds of thousands of dollars are taking them to court instead. They're not co-operating. It takes these criminal investigations to reveal the kind of decay that's within the practices of the telco. That's why we continue to believe there needs to be a hearing to give that transparency in terms of the numbers. What are the practices? What are the ways and different patterns in how victimization occurs?

The third thing is that we want to codify it. The FCC also believes there is no consistency and durability in these practices. They can choose to not do this or just to say that it was a slip-up. The fourth thing is that we need that enforcement there, which we believe the Australian example shows is critical to ensuring there is compliance and things like that.

Those are the three or four things we stick to, and I believe the committee was a part of this the last time.

● (1240)

[*Translation*]

Mr. Sébastien Lemire: Thank you for your clarity and, above all, for your testimony. You greatly advance our thinking.

[*English*]

The Chair: Thank you very much, Mr. Baran-Chong.

Thank you, Mr. Lemire.

We'll move to Mr. Masse for six minutes.

Mr. Brian Masse: Thank you, Mr. Chair.

I'll continue with you, Mr. Baran-Chong, and start by thanking you. Your efforts have been nothing short of heroic. I'm looking at what you've gone through. Sharing that and being here again as a witness is much appreciated.

We had the CRTC here on Friday, and I swear I almost broke down into a Lewis Black-style rant with regard to the testimony we heard. My concern is exactly what you're expressing. I'm wondering about a summit. I'm reclassifying it as that. You're talking about a hearing as the original thing—I think it's the same type of thing—where we could get, I think, some more public-led accountability and then also some expectations for our cross-jurisdictional agencies, whereas when they sit here individually, it's hard for them to criticize and to make recommendations for others. Perhaps if we had more of a civilian-based approach.... I'm just wondering what you think about that, and then I'll go to Mr. Cosgrove and to our witness on telecommunications data.

Please go ahead.

Mr. Randall Baran-Chong: Yes, we're highly supportive of the idea. It doesn't matter really what form it takes. Again, it's all about being able to be heard. We've learned a lot from the different victim stories, because our group essentially is very grassroots. I identify them by scanning through articles and reaching out to them, or they come to us and they tell us the circumstances of these issues.

A public-based approach can help people understand how the fraud itself happens, or those points of confusion that enable the fraud—for example, when they get a text message and they don't know whether it is a fraud or not.

The second thing is that if you think about portability, it takes two to tango. There are two telcos involved in it, because it's typically going from one carrier to the winning carrier, so there needs to be a kind of consistent practice and standard across the industry itself.

Third, I think there needs to be a much deeper layer at the business process level when we're talking about these vulnerabilities within the organizations. This isn't just in Canada. This is in the United States and in other countries where we've seen SIM swaps occur, because insiders or the ability to socially engineer people within the organization essentially enables an open season on people's information. I agree with you on that suggestion.

Mr. Brian Masse: I'm going to move to Mr. Mecher and Mr. Cosgrove. Maybe I'll start with Mr. Cosgrove, since he's right next to me here.

I thank you and Mr. Mecher for your efforts. It's been fun working with you in many respects, because this is one of these issues that feel almost like the war on drugs, you know? It's so hard to go after some of the top players in this, but at the same time, prevention is a major tool. I do like Mr. Baran-Chong's approach, though, in the sense of making sure there's an accountability level for some of the telcos. I don't think we get to let them off the hook.

Mr. Cosgrove and Mr. Mecher, what are the things we can do to unshackle your advocacy to help with prevention? I think it's a two-way street for these things.

Mr. Kevin Cosgrove: In my advocacy, where I've hit a dead end is that basically I'm stuck at the local level. We're dealing with a border city in a town with a university and a college. We have a very high multicultural population, and I can't even get funding for standard translations. Living in Windsor and with French being our second official language, I don't even have a French copy at the moment, and this is something that I've been involved with for years. It's not something I've just started. This is a problem that I've been trying to crack, and thankfully, with MP Brian Masse inviting me for this committee, my appearance here might even provide some opportunities to get this out.

Anything that I've done over the years is all completely non-profit. It's all volunteer time. I'm not paid for any appearances, I'm not paid for any of the booklets or publications that are put out. This is solely just non-profit, and even at that level, it's definitely difficult getting any level of support.

● (1245)

Mr. Brian Masse: Before I go to Mr. Mecher, maybe you can submit your booklet to the clerk, and I'd ask that our committee have that translated so that you have your publication. We can do that here on the Hill.

Mr. Mecher, can you follow up on this, please?

Mr. John Mecher: Okay.

Some of the frustrations I had when I was in the RCMP have actually carried over, and I'm not surprised. One of the things is a passion project I have to try to create awareness. I've never had any high sense that I myself would be able to have a big impact. It's a term that Kevin used several times, “grassroots”, but I kept pushing, pushing, pushing, and most recently came our experience with the Western Union matter. The Federal Trade Commission of the United States was the genesis behind that. They basically forced Western Union to hand over in excess of half a billion dollars through a deferred prosecution process, and those funds went to victims of fraud related to Western Union around the world, which is an amazing gift for victims of fraud.

However, the big problem was with getting that information to victims in Canada. The U.S. Federal Trade Commission kept repeating that message, but it did not resonate in Canada.

In March, I start repeating their message the best I could on my limited social media platform, and then, having no luck, I finally got frustrated and actually wrote the commissioner of the RCMP, both on June 1 and June 7, with a view that at that point the end date for the Western Union offer was at the end of June. It was going to die at the end of June. Unfortunately, my plea went nowhere.

I explained who I was, the experience I had with victims, my engagement with fraud and so on, but there was no response until close, I believe, to the end of June, at which point it was almost moot. At that point they basically posted it on the Canadian Anti-Fraud Centre website. The perverse thing at that time was that it was posted, I think, on June 26, and at that point it was believed that the offer was going to expire for intake at the end of June. It was pointless doing that, because any victim would need at least a week or more to get all their documentation together.

However, two days later the Federal Trade Commission announced that there was going to be an extension to the end of August. The only meaningful access I've had to advance this cause came when I engaged Mr. Masse, and then he pushed it forward. He has a much larger platform than I'll ever have, so I'm very appreciative of that.

What it speaks to, and I try to be as respectful as I can when I say this, is that at the highest level, the RCMP does not appreciate fraud or appreciate the impact fraud has on its victims. That is a current frustration I have now, and it was also a frustration I had when I was actually a member of the RCMP investigating fraud.

The Chair: Thank you very much, Mr. Mecher and Mr. Masse.

I will now turn it over to MP Kram for five minutes.

Mr. Michael Kram: Thank you very much, Mr. Chair.

I have a couple of questions for Mr. Baran-Chong and then I'll be sharing my time with Ms. Gray.

Mr. Baran-Chong, you said you were offered $100 compensation from Rogers. Have you ever pursued suing Rogers for damages in civil court?

Mr. Randall Baran-Chong: No, I have not.

Mr. Michael Kram: Why not?

Mr. Randall Baran-Chong: Well, I've consulted several lawyers. It's interesting, because unlike others who've had significant financial losses.... In the case of credit card fraud, let's say, the credit card company or the banks end up kind of compensating folks for that. Other folks who have crypto-thefts are still trying to recover their losses, and many of the people within our groups are trying to recoup between hundreds of thousands to millions of dollars. However, my theft was very insignificant financially. They had essentially taken possession of all of my information and tried to extort me with it. Extortion and the kind of psychological distress of thinking your life is going to be over is something that's very hard to quantify. Therefore, it was just not worth pursuing.

This action was my form of getting my compensation.

● (1250)

Mr. Michael Kram: Okay.

The last time you were here, you had what I thought was a very practical recommendation when it comes SIM swapping. I'd just like to read from the minutes what you said two years ago:

> Let's say your phone is actually legitimately stolen. Then you have to go into a store to actually provide government ID to validate that it's you and that you are executing the port.

That sounds like a pretty practical and effective solution. Is that still your recommendation?

Mr. Randall Baran-Chong: That's in the case of a stolen phone. There's a bit of balance here, right? The CRTC wants to allow you to easily port your number. There is actually a rule that they have to execute it within two and a half hours. My bigger recommendation, which doesn't have to apply to just a stolen phone, is that when you have text notification that your number has been requested to be ported, you have to proactively consent by texting back “yes”—that yes, you are trying to execute that port.

Take what happened to me, for example. If I'd gotten that text message at 11 o'clock on a Tuesday, would I have executed a port? Absolutely not. That would never have gone through, and I wouldn't be in front of you today, but that process did not exist at the time.

Afterwards, the telcos introduced a text and didn't require the proactive notification. This was the problem, because people thought it was fraudulent text, ignored it, and executed the port anyway. It wasn't until much later that they did.... According to the Rogers website right now, they say that they have introduced this practice that I introduced back in 2020 before this committee. They're saying that it applies now, but again, there are inconsistent practices and things like that.

This proactive notification should help prevent a significant number of these scams.

Mr. Michael Kram: Okay.

I will turn things over to my colleague Ms. Gray.

Mrs. Tracy Gray: Great. Thank you very much.

My questions are also for Mr. Baran-Chong.

During your testimony, you referenced your experience with Rogers. Of course, we had Rogers here for an emergency committee meeting this summer, and the CRTC really seemed to be defending the telecoms instead of being a regulator. Your comment actually was very similar when you said it seemed like they were standing up for the telecoms.

I'm wondering if you can go into that in a little more detail. Really, the CRTC should be holding the telecoms to account and standing up for Canadians. It seems like it's the other way around. Could you explain what your comments were in a little bit more detail?

Mr. Randall Baran-Chong: Absolutely. You kind of wonder whose corner they're in.

We've been consulting with PIAC quite a bit. We've been trying to get this data, for example. You'd think macro-level data is not too big of an ask or too much of a threat to security. We weren't even asking at the telco level what the data was in terms of the incidence of SIM swaps. The CRTC rejected that. The CRTC said that the hearing does not need to occur because the public has no real contribution to helping solve this problem.

Therefore, the question is this: Is the regulator trying to defend the telcos from being embarrassed or from further legal action? I know that a lot of the times in the early days, when people were trying to do lawsuits around this, they thought they were one-off incidences. When we heard it was 25,000 cases within that 10-month period, we were shocked. We thought it was in the few thousands or so. If you think about it, the prevalence and magnitude of this crime is massive. We think they're protecting them because this could be a big, big fraud and completely embarrassing.

The Chair: Thank you very much, MP Gray and Mr. Baran-Chong.

We now have to turn it over to MP Fillmore for five minutes.

Mr. Andy Fillmore (Halifax, Lib.): Thanks very much to the witnesses. Thank you, Chair.

I'd like to bring us back to the topic of data in the era of great interest in protecting public privacy.

I'll get us there in this way. About six months ago I visited the cyber centre of excellence in Vancouver. It's embedded in Mastercard. It's a centre that this government invested about $50 million in. They're devising techniques and algorithms that will help to identify fraud during transactions.

I learned things. For example, in cases of ported or cloned phones, Mastercard can tell, if I normally type holding my phone this way, that someone's pretending to be me because they're holding it another way. They know if I hold it this way, flat instead of up, and how hard I'm pushing on the keys, or whether I'm using two thumbs or one finger. Some of the techniques that are emerging to figure out if the right person is on the other end of that phone are incredible. That's the bank and credit card perspective.

Then there are the vendors. The vendors are also party to fraud. They're creating profiles on all of us—what time we shop, what we buy and all of those kinds of things.

There are really three parties. There are consumers, banks and vendors involved in many of these things, and everybody has data. There's all this data being generated.

Perhaps I'll begin with Mr. Mecher.

In your experience, are there adequate feedback mechanisms or data sharing between the RCMP, CRTC, banks and vendors? Are we doing a good job there? Is there required reporting? Is it required to have fraudulent transactions reported to the RCMP? Is it voluntary by the banks?

Can you say anything on the discussion of data sharing in the era of the protection of personal privacy?

● (1255)

Mr. John Mecher: I really can't speak to privacy matters. That's really not my niche.

I can say that previously, banks in particular have been periodically fully engaged on the fraud-fighting front. At the same time, some banks have gone in the opposite direction and, through willful blindness or what have you, have actually assisted fraudsters. That usually catches up with them.

Mr. Andy Fillmore: Let's use the Mastercard example. When they detect a fraudulent transaction, is there a requirement that they inform the RCMP, or is that really a matter between their customer and them?

Mr. John Mecher: Honestly, I don't know. I might give you a guess, but I don't want to hedge an answer on a guess.

Mr. Andy Fillmore: Would Mr. Cosgrove or Mr. Baran-Chong have anything to add on that point?

Mr. Randall Baran-Chong: I would add that there's a company called EnStream, which is a joint venture of the major telcos. One of the services they offer is identity verification to prevent things like SIM swap fraud. This is a product that they sell to the banks.

I've spoken to some folks on the cybersecurity teams in the banks, and they know SIM swap fraud well, because banks are the ones who ultimately pay for it. They're the ones who are compensating for the credit card losses, other thefts and things like that. Banks are being sold a product by the telcos whereby the telcos can help identify frauds. There's this kind of perverse organization that exists.

Some other countries have done some of the stuff that you're alluding to. For example, they will block bank transactions after a port. There will be a bit of a freezing window. They know that there's a high risk of things like that.

There are connections between bank, telcos, privacy and security in the enabling of these frauds.

Mr. Andy Fillmore: Thank you.

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

I have to cut you off because we're almost out of time. We still have two questioners.

I'll turn to Mr. Lemire for a short two minutes and 30 seconds.

[*Translation*]

Mr. Sébastien Lemire: Thank you, Mr. Chair.

I have listened to the witnesses and I see the importance of legislating for victims of fraud. The government has introduced Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.

What is your opinion of this bill? Does it go far enough?

Do you have any recommendations for us in this regard?

[*English*]

Mr. Randall Baran-Chong: I'm admittedly not familiar with Bill C-27.

[*Translation*]

Mr. Sébastien Lemire: Very well.

Mr. Mecher, what are your thoughts?

[*English*]

Mr. John Mecher: I'm sorry. I didn't hear your question.

[*Translation*]

Mr. Sébastien Lemire: Have you heard about the new Bill C-27?

Does it go far enough in protecting victims?

[*English*]

Mr. John Mecher: No, I haven't.

[*Translation*]

Mr. Sébastien Lemire: Fine.

Thank you.

● (1300)

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

I yield the floor to Mr. Masse for two and a half minutes.

[*English*]

Mr. Brian Masse: Really quickly, Mr. Mecher, do you feel that a civilian-led attempt to bring the different jurisdictions together would be appropriate at this time, whether it be to help coordinate...? It doesn't have to be aggressive to the RCMP, the CRTC and the others, but I'm wondering whether a third party is required to help coordinate the sharing of resources and the sharing of information.

Mr. Mecher, did you hear that?

Mr. John Mecher: I had a technical issue.

Anything is worth a try. I don't think that particular approach is entirely unique. It might be beneficial. The nice thing about having it beyond law enforcement, I suspect, is that it would be a whole lot easier to be transparent.

Mr. Brian Masse: Mr. Cosgrove, I'll go quickly to you on a civilian-led approach, and then I'm sure I'm out of time.

Mr. Kevin Cosgrove: Yes, absolutely. There is a tendency from the stuff that I see myself, because I'm speaking from my own experience, to over-complicate things, overpresent them and overformalize some of this information. If we're looking at seniors as being a major target of just about any type of fraud, making big formal documents and online bills and everything doesn't make them aware of this stuff.

We need to get down into the trenches and resolve this stuff more in person or with easier information.

Mr. Brian Masse: Thank you, Mr. Chair.

[*Translation*]

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

I thank our witnesses for their presence today, which has been invaluable to the work of the committee.

I wish you a great week and a beautiful afternoon.

The meeting is adjourned.