HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

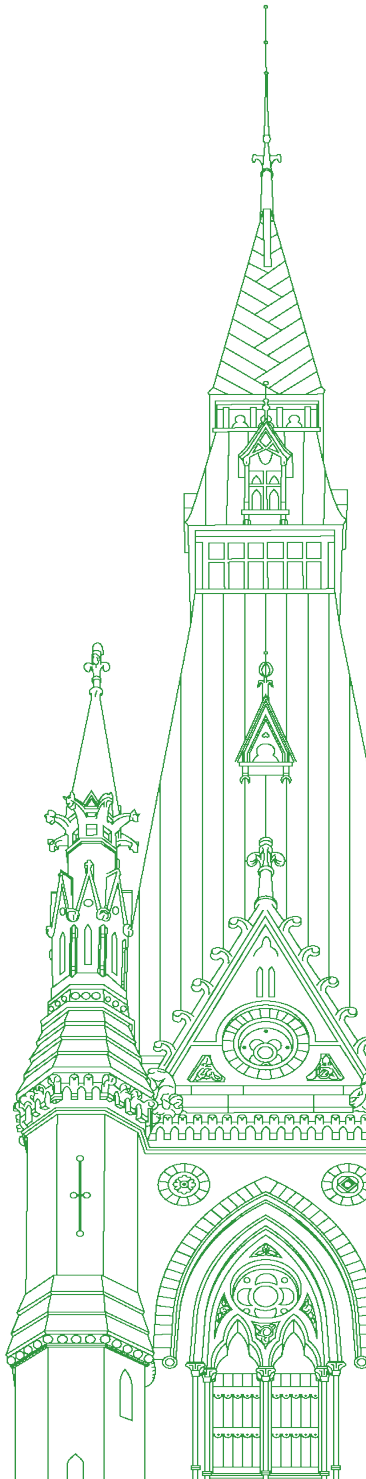
43rd PARLIAMENT, 1st SESSION

Standing Committee on Industry, Science and Technology

EVIDENCE

NUMBER 008

Thursday, March 12, 2020



Chair: Mrs. Sherry Romanado

Standing Committee on Industry, Science and Technology

Thursday, March 12, 2020

● (1105)

[*English*]

The Chair (Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Good morning everyone.

Pursuant to Standing Order 108(2), we are continuing with the study of fraud calls in Canada.

Welcome to Mr. Matthew Gamble from the Internet Society Canada Chapter, and Mr. John Lawford from the Public Interest Advocacy Centre.

Gentlemen, you will each have 10 minutes to present, after which we will go into rounds of questions from the members of Parliament. If you see me waving this little yellow flag, I'm not surrendering. I am giving you the heads-up that you have 30 seconds before the end of the round of questions. Then we will move to the next round of questions.

I am going to remind folks in the audience that there are to be absolutely no photos taken during committee.

With that, I will start with Mr. Gamble. You have 10 minutes.

Mr. Matthew Gamble (Director, Internet Society Canada Chapter): Good morning, members of Parliament, staff and hearing participants.

My name is Matthew Gamble. I am a director of the Internet Society Canada Chapter and I am pleased to appear before you today to speak about fraudulent and nuisance calls in Canada.

First, I'll say a few words about who we are. The Internet Society Canada is a not-for-profit corporation that engages on Internet, legal and policy issues to advocate for an open, accessible and affordable Internet for all Canadians. An open Internet means one where ideas and expression can be communicated and received, except for where limits have been imposed by law. An accessible Internet is one where persons and all interests can freely access websites that span all legal forms of expression. An affordable Internet is one where all Canadians can access Internet services at a reasonable price. More information about our board, our activities and our publications can be found on our website.

The Internet Society is fully aware of the impact that fraudulent and nuisance calls have on Canadians. According to a study by Truecaller, Canadians receive an average of 12 spam calls per month. My personal experience tells me that number is far higher.

In the case of fraudulent calling and robocalling, such as the CRA scam calls, it's increasing for several reasons. It's inexpensive to do, has little to no consequence and sometimes, albeit rarely, is effective in defrauding innocent Canadians of their hard-earned money. Between the CRA scam calls and the endless calls for duct cleaning services, it has come to the point where people are hesitant to pick up for any unknown caller and have lost trust in their own telephones.

To give some background on my experience in this area, 13 years ago I was the chief developer and architect of Primus Canada's telemarketing guard service, which at the time was a major step forward in the fight against unwanted calls. Based on a community-driven list of known nuisance callers, it was very effective in stopping millions of telemarketing calls from reaching Canadians.

In the years since its development, however, the landscape has changed dramatically and systems that filter based solely on calling line ID are no longer effective. Bad actors now routinely spoof valid numbers or generate random numbers similar to that of the person they are calling, commonly known as neighbour spoofing.

This new wave of bad actors are exploiting principles wired into the DNA of telecommunications networks. They were built based on explicit trust between carriers and set up to make sure that calls get through no matter what. Carriers don't look at the content of calls before connecting them and multiple companies can touch each call, making identifying the source of calls a daunting, if not impossible, task.

On the surface, the solution to the current robocalling crisis may sound simple. Just forbid calling line ID spoofing. The solution, sadly, is never that simple. There are good feature-related, business-related and privacy-related reasons to allow call spoofing.

For example, imagine a women's shelter is trying to contact a domestic abuse victim at home, without the abuser knowing. They may spoof the client line ID to mask the source of the call so that it's not known to be coming from the shelter.

Other even more basic phone features, such as call forwarding or a business having multiple telephony providers, rely on the ability to set calling line ID dynamically. It's an integral feature of how the PSTN operates and something that cannot easily be disabled without significant collateral damage.

As you heard earlier this week, the CRTC is working with the Canadian telecommunications industry to attempt to fight this problem on several fronts, including requiring calls to have valid calling line ID, directing the CRTC interconnection steering committee to develop a traceback process and directing carriers to implement the STIR/SHAKEN framework for the authentication and identification of calls.

Of all of these initiatives, the Internet Society is most interested in the deployment of STIR/SHAKEN for the identification of calls. Born out of technologies borrowed from the Internet standards working groups, STIR/SHAKEN promises to restore consumers' faith in calling line ID through the use of digital signatures placed in call metadata. When implemented fully, it promises to allow carriers to identify the source of calls in real time and could easily filter parties that are spoofing known numbers such as the CRA, RCMP and others.

The major challenge with implementing STIR/SHAKEN in Canada, and why we have been intervening in these respective CRTC processes, is that there are serious policy, technology and privacy issues that have not been addressed yet with this technology.

First, on the policy issues, STIR/SHAKEN standards were developed by the Internet Engineering Task Force and then adopted by several large U.S. providers for use within their own networks. Since this adaptation was done by large carriers, several early policy and design decisions were made that benefit large carriers at the expense of smaller ones.

The largest of these decisions was to limit the ability to fully attest to the identity of the call to the phone company that owns the number. While this seems logical, ownership of phone numbers is not as simple as it sounds. There are over 1,200 entities registered with the CRTC as resellers of telecommunications services. These are generally telephone service providers, or TSPs, that operate without owning any of their own phone numbers. Instead, they rely on wholesale access agreements with larger providers. These providers deliver valuable telecommunications services to Canadians, including services such as business-hosted PBX platforms, residential over-the-top services and other innovative voice products.

The CRTC, as you know, has asked all telecommunications providers, including the non-facilities-based providers, to implement STIR/SHAKEN.

These smaller carriers will be placed at a major disadvantage when the standards and policies developed to date are implemented, if no changes are made. Without the ability to fully sign their own calls, they will be viewed as “lesser” than larger carriers. Over time, this may cause customers to move their business to larger carriers who can provide full attestation for all calls, thereby creating a two-tiered telecommunications system in Canada, of those who can sign and those who cannot. Were this to happen, it could destroy years of competitive gains and innovations made by smaller carriers.

On the technology issues, STIR/SHAKEN poses a challenge, as it requires carriers to interconnect with each other over IP-based interconnections using SIP. While the smaller providers I earlier referred to generally interconnect with their upstream carriers using the SIP technology, the interconnections among Canada's larger carriers are mostly based on legacy TDM-based interconnections. It's almost ironic that the smaller, SIP-based carriers who are best suited to deploy this technology are being left out of the process, but that's the reality of the Canadian market today.

Finally, the Internet Society has some very serious concerns around consumer privacy as it relates to STIR/SHAKEN. Once calls are digitally signed, terminating carriers will have rich, verified data on the source and destination of calls. The promise is that this will allow telecommunication service providers to develop solutions like Telemarketing Guard, but ones that don't just look at the calling number but look deeper, into such things as the source carrier. This is analogous to spam filtering in the Internet space. Analytics are built not just on the source address, but on the reputation of the networks that traffic has traversed.

While this all sounds wonderful, it poses several issues for the privacy of Canadians, as some carriers have opted to outsource this analytics function to third party commercial entities. With this data, these third party companies could easily augment existing commercial data sets to build even more detailed profiles of Canadian households. For example, you could infer from the data collected that a given household was calling for takeout every night, and that data would be valuable to a life insurance provider who might view that as an unhealthy lifestyle and an increased risk factor.

In conclusion, while this may sound as though we oppose the deployment of STIR/SHAKEN, the opposite is actually true. We firmly believe that the introduction of these technologies into the Canadian telecommunications networks is a much-needed step forward to restoring consumers' faith and protecting them from fraud. We just want participants to be mindful that we need to ensure that this technology is implemented correctly and in an open and transparent fashion. As with other Internet-based technologies, we must ensure that all players, including small telecommunications providers, can participate on an equal footing.

Finally, and above all else, we need to ensure that any technology deployed has strong privacy safeguards built into its DNA. As we have learned from the Internet, trying to augment a system for privacy after it's deployed is like trying to repair a plane in flight: It's an impossible task that should be avoided at all costs.

I thank you for your time and I welcome any questions.

● (1110)

The Chair: Thank you very much.

Next we will move to Mr. Lawford. You have 10 minutes.

Mr. John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre): Thank you, Madam Chair, and honourable members.

My name is John Lawford, and I am executive director and general counsel at the Public Interest Advocacy Centre here in Ottawa.

PIAC is a federally incorporated non-profit and a registered charity that provides legal and research services on behalf of vulnerable consumers' interests concerning important public services.

PIAC regularly participates in proceedings before the CRTC and represents consumer interests in retail banking and payment systems with the FCAC, the Department of Finance and the OBSI.

Consumer fraud is a hot potato. Companies avoid it because they do not want the risk of liability for the fraud. Police have insufficient resources to address its overwhelming size and daunting technical complexity, which changes with each vector. Regulators like the CRTC define their jurisdiction narrowly to avoid being responsible for the problem, viewing it as an operational black hole.

On an individual level, fraud is humiliating and often devastating. We naturally avoid this issue like we avoid discussing poverty because we recoil from the obvious injustice and pain that is inflicted on the victims. Avoiding a problem never makes it better, though, so we commend this committee for insisting that we take a look at one aspect of fraud in today's committee hearing, phone fraud.

The statistics we do have about the scope of the “fraud problem” are so fragmentary as to themselves pose a problem for dealing with the problem. There is no definitive and official source for them. We have recent data from the Canadian Anti-Fraud Centre that show about 46,000 reports were made in 2019, with 19,000 victims and a loss of around $100 million.

The calls to CAFC largely covered fraud committed over the phone and Internet. However, the FCAC, for example, cited 15 million fraud victims losing $450 million in 2007, likely including other types of fraud, including in person, but more reliable or current numbers are scarce. The CRTC, for example, only has numbers of complaints made in relation to the do-not-call list and not specific fraud numbers.

However, PIAC believes, based on its work in the sector, that the scope of fraud committed by telephone to be one to two orders of magnitude higher than CAFC numbers. That's voice and text fraud, in part using regular phone numbers, but leaving aside Internet-based scams you might get on your mobile phone.

It is also our belief, based on direct contact with consumers and with seniors and low-income groups such as the National Pensioners Federation and ACORN Canada, that phone fraud both specifically targets and inordinately affects seniors and low-income Canadians, some of whom may be newer Canadians. They can least afford to suffer a fraud.

I will not be addressing number porting or SIM swap fraud. It's a recent concern that requires urgent attention, though. Shortly you will hear from Randall Baran-Chong, who is both a victim of this fraud and an eloquent advocate for fixing this devastating hack. I will leave it to him to describe. However, I do note that PIAC has called for an open public hearing at the CRTC with consumer groups, wireless users, CWTA and major providers. However, so far the CRTC and CWTA have refused to have a public inquiry.

Instead, I want to talk today about good old phone fraud, getting a victim to answer their phone, home or mobile, and engage in a conversation with a fraudster which culminates ultimately in the victim transferring money to the fraudster or revealing so much personal information that the fraudster can then transfer money himself, without the victim's knowledge. This sort of fraud can be catalyzed by the spoofing of numbers or call display names to mislead consumers into thinking they are receiving a call from a legitimate agency such as a government department or a local police office number.

However, what makes for really good old phone fraud is volume and automation. The more calls made, and the more efficiently made from the scammer's viewpoint, the more likely it is to ensnare a victim.

I can tell you that billions of calls are made a year to Canadian numbers, and at least tens of millions of those calls are stage one fraud robocalls. Here's how it works. A program written by a fraudster calls thousands of phones in an hour usually with a spoofed originating phone number. No people are involved. Now multiply this by many programs, computers and other scammers doing the same thing and targeting multiple area codes and you get the idea.

● (1115)

In stage two, however, the potential victim answers and does not hang up but listens to the recorded message, possibly because they trust the source, fear the source or are simply lonely and looking for some human contact. If the victim presses “1” to hear the message, a live fraudster walks the victim through the fraud to the point of money transfer.

Robocalls are just fishing lines flung out to the sea of phone-owning humanity. The secondary calls with a live agent are vastly smaller in number. This smaller number is still very large; we just don’t know how large. That is where the fraud takes place.

What's new? What's changed in this area lately to give you the impression that we have a phone fraud epidemic? “Epidemic” is a bad word today. Why are more and more Canadians, especially seniors and low-income Canadians, falling victim to phone fraud?

The answer is that the phone system has been technologically democratized. In the past, to dial multiple numbers, a knowledge of the phone company’s network software was required. This software allowed only a certain throughput of dialed numbers. Now almost the entire phone system runs on Internet protocol. This allows many millions of calls to be made to many millions of numbers and transmitted by a small number of computer operators.

While IP-based telephony has allowed new competitors and services, it has allowed fraud to balloon, in part due to the possibility of spoofing numbers with IP, which is harder than with the old software. The bottom line, so to speak, is that with more fishing lines come more hooked fish.

The phone industry, especially legacy carriers such as Bell Canada and Telus, know this reality all too well, as does the CRTC, which at least views nuisance robocalls as within its telemarketing jurisdiction. It deals, at least in part, with numbers on the do-not-call list. They are all working together on the spoofing part. The CRTC already requires them to block obviously spoofed numbers such as 000-000-0000. They are all working on implementing the STIR/SHAKEN protocol you just heard about, which really works only on entirely IP-based calls. All it really does is provide a confidence rating for each call. That is, it allows the recipient software to automatically block these likely robocalls. Both of these measures will help, but they will not totally stem the tide.

However, there are also new network-level blocking technologies, like those developed by Bell Canada, which has now applied to the CRTC to allow this. They claim to use AI-based algorithms to identify likely robocall sources, along with some confidential extra fail-safes that they have promised, and then to block all such suspicious calls that are transiting Bell’s network. Bell's network is vast in Canada.

While this does raise concerns from other carriers that must use Bell’s network to connect calls and it concerns legitimate customers who may have their calls illegitimately blocked, it does attempt to address the volume aspect of our problem. It attempts to use automation against automation. We believe it is likely, on balance, a positive development, but will it be sold to us or offered for free?

Last, what is missing to combat the actual content of fraud calls is more authority in this area for the CRTC. We suggest looking at the U.S. Telephone Consumer Protection Act, and a dedicated anti-phone fraud act, for example, one more akin to the Telemarketing Consumer Fraud and Abuse Prevention Act in the United States. In this regard, we also noticed that the broadcasting and telecommunications legislative review report seems to have missed a chance to recommend amending the Telecommunications Act to give the CRTC more authority to deal with fraud calls or to recommend a dedicated anti-phone fraud act, whether administered by the CRTC or perhaps by the new data commissioner.

We also need a better, more centralized, comprehensive and reliable set of phone fraud and Internet fraud-related statistics and reports to be gathered and publicly released at regular intervals. Finally, we need continual oversight and democratic encouragement by Parliament of work on phone fraud. It is too important to allow this game of hot potato to be played between regulators, companies and the police.

Thank you very much.

● (1120)

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

Our first six-minute round of questions will go to MP Gray.

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

My first question is for Mr. Lawford.

You had mentioned that people who are elderly and have low income are more vulnerable to phone fraud. I know you've been in my riding of Kelowna—Lake Country. I have heard from people who have been targeted, both in Mandarin and in Punjabi, with fraudulent immigration or revenue matters, especially Revenue Canada matters.

What awareness methods do you think can be promoted to ensure elderly Canadians and vulnerable people don't fall victim to such scams?

Mr. John Lawford: I think consumer resilience, if you want to call it that, could be a lot better in Canada. I think it's only part of the problem, but let's start there.

There have been efforts made to reach out in other areas in which consumers are defrauded in languages other than English and French. It's part of no one's mandate at the moment, and I can't think who would be doing it. The CRTC probably could undertake this type of work—to produce materials for people, to try to reach out to the community—but it's really one of those cases in which you have to get direct contact with consumers in a language they understand.

I'm not sure how getting out into these communities and getting a trusted person to communicate with them would be directly delivered, but it's a great idea.

Mrs. Tracy Gray: Thank you.

You mentioned in your opening comments that you were interested in having a public inquiry regarding people who have been victims of fraud and said you had approached the CRTC.

Can you give some more details as to what the specific ask was and what the response was?

Mr. John Lawford: Sure. That's the issue you're going to hear about from Randall in the next panel. It's the SIM swap.

At the moment, the CRTC has exchanged letters with the wireless association saying to please tell them what they're doing on SIM swap because other countries, for example, Australia, have already set out rules about avoiding SIM swap. There's an exchange of letters on this on the website, and I'm asking, “What are you guys doing? Why isn't there a public inquiry such as we usually have at CRTC?”

So far, the answer from the companies has been that they don't want to talk about fraud in public, because it might be telling scammers what's going on. From the CRTC.... I don't know why they don't want to do a public inquiry. I think they want the industry to solve it quickly. However, I don't understand why that's done, because normally fraud is not helped by obscurity; it's better to discuss it in public. Rules that are made in an open, transparent process usually are better rules.

● (1125)

Mrs. Tracy Gray: Thank you.

I have a couple of questions for Mr. Gamble.

You mentioned that when the development of the STIR/SHAKEN framework was being worked on, it was done with the larger companies, and that you've been bringing the voice of some of the smaller organizations and providing their thoughts.

Has anything changed? Is consultation happening now with the smaller providers? Are they at the table, bringing forth their concerns and their ideas?

Mr. Matthew Gamble: The process right now with the CISC working group of the CRTC is that the concerns of the smaller players are there, although only a few of them are represented.

I will say that many of these smaller carriers don't have the resources to participate in these types of forums. They are things that take time from staff, and if you have a company of two or three people, it's hard to dedicate somebody to work on technical standards.

The CRTC submissions from the carriers to date acknowledge that this is an issue, but they say it's something that should be solved at a later date, with no real understanding of when that date would be.

Mrs. Tracy Gray: It sounds as though they're listening, but they're implementing without considering what the concerns are and what the flow-through is going to be.

Mr. Matthew Gamble: That is correct. The view so far seems to be that we should implement with the big players and then let the small players catch up later. As you know, trying to fix something after you've done it is always problematic.

Mrs. Tracy Gray: Would the small players have to implement at the same time, though?

Technically, they would all have to implement at the same time, yet they don't have the capabilities. Is that what you're saying?

Mr. Matthew Gamble: That is correct; or they would be tied to using a single provider as their wholesale source through which all the numbers would have to go. They would lose the flexibility of choosing which wholesale partners they deal with.

Mrs. Tracy Gray: Okay.

On a related note, one other thing concerned IP phone services being made aware of these spoofing phone calls and the prank websites that actually market themselves as prank websites.

Are you aware how STIR/SHAKEN can identify spoof calls done through these websites? What are your thoughts on that question?

Mr. Matthew Gamble: When fully implemented, every call will have a source of at least some level associated with it. There are three different levels: gateway, partial and full. Gateway just says that it knows where the call came from on the network, so that you basically know where it was injected from the Internet side into the phone network side. At a minimum, you would know which end user it came from.

Mrs. Tracy Gray: However, there are no regulations, or no way, moving forward, to actually address these websites. It's more just a matter of knowing where they're coming from.

Mr. Matthew Gamble: That is correct. There are no KYC requirements in telecom.

Mrs. Tracy Gray: Okay.

One of the other things—

The Chair: You have 10 seconds.

Mrs. Tracy Gray: I don't think we'll have time.

The Chair: Sorry about that.

Our next six-minute round will be with MP Ehsassi.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you, Madam Chair.

Thank you, Mr. Gamble. Thank you, Mr. Lawford.

There was a lot of information and it was incredibly helpful.

Mr. Lawford, you expressed concern that seniors are, to use your language, being both targeted and affected, a fact we can all recognize.

Is it possible for the perpetrators of fraud to actually target seniors?

Mr. John Lawford: The messages that are sent out are ones that are designed to elicit fear or something of interest. They can work, for example, targeted at new Canadians, if it's fear-based. The ones that our seniors are sent might be an “interesting offer” kind of approach. They can receive the fear-based ones as well.

Both parties are susceptible to these calls, but seniors have the additional.... Well, there are two things I can honestly say. Generally speaking, as one gets older, one gets more trusting. Also, as one gets older there is some social isolation. That's what our client groups tell us. One is more susceptible just to taking any call. That is known by the scammer. That's why the high volumes get targeted at seniors. They're hoping to phish somebody who is lonely, to be honest.

I haven't studied the messaging, exactly what's said. I think the threats work better on folks who may be newer immigrants.

● (1130)

Mr. Ali Ehsassi: Thank you.

Mr. Lawford, I'm wondering if you had a chance to review the transcripts from the witnesses we had a couple of days ago. As you know, we heard from the CRTC—

Mr. John Lawford: Yes.

Mr. Ali Ehsassi: and the RCMP.

We also heard from Bell, Rogers and Telus.

Each one of those major carriers has distinct approaches and different programs that they are suggesting will block and filter.

Mr. John Lawford: Yes.

Mr. Ali Ehsassi: Did you have any comments on any of the approaches that were outlined by the carriers?

Mr. John Lawford: Sure.

The baseline is, let's block calls that come from an obviously wrong number. Everybody accepts that. That's done.

The second level is this STIR/SHAKEN stuff. What the big companies don't like is that this is a protocol that you just run on any third party app or on your phone. It will block calls. The calls get tagged as suspicious. Then it's up to you whether you want to block them or not with your software and how you set it.

Phone companies don't necessarily make that much money on that, but it works fairly effectively. There may be problems with how it's implemented transparently and equally. But we'll leave that aside for now. STIR/SHAKEN is what should fix things. It doesn't—they're quite right—catch calls that go outside IP and go through the phone legacy networks. But let's leave that aside, too.

What Bell and Telus are both doing at the network level is...systems that have a sort of different approach. Telus will require a caller to punch in extra numbers in an effort to put a speed bump there. I believe you can get around that if you're a good programmer. It may or may not work. They may or may not be selling that to other providers or to other people who have an involvement with the phone system. They may be selling it directly to customers. The end game, I think, is that they probably want to sell it to customers.

Bell has a different approach, which is network-level blocking which comes with more concerns about how it's being blocked, why it's being blocked, what the system is. That's the secret proceeding going on at the CRTC right now. I think Bell would also like to sell it to consumers at the end. But I don't know. They have the control, as was mentioned, unlike some other carriers because most stuff transits their networks.

Mr. Ali Ehsassi: Mr. Gamble, it's the same question.

You identified the reality that this is really going to skew competition. It will disadvantage smaller carriers.

Based on the merits of the disparate approaches that were outlined by the carriers, do you have any comments?

Mr. Matthew Gamble: I believe they're trying their best but they are working in a system where they have imperfect data. With the telemarketing integrated system we had years ago, it was only based on a phone number. That's really the only point we have. Until we add more points to the system, such as where calls are coming from, like the actual sources, then filtering will be just trying, with our best effort, to pit machine against machine.

Mr. Ali Ehsassi: Thank you.

Mr. Lawford said that he would be in favour of open and public hearings by the CRTC. Is that something you would favour as well?

Mr. Matthew Gamble: On the issue of SIM swapping, yes.

Mr. Ali Ehsassi: Yes, you would, okay.

Mr. Lawford, you identified that the U.S. has done a better job. Specifically, you referred to the U.S. Telephone Consumer Protection Act. Would you be in favour of a similar approach being adopted in Canada?

Mr. John Lawford: Yes, I think that the CRTC needs a little more jurisdiction to try to address fraud more directly. At the moment, wire fraud, if you will, isn't an offence in Canada. It's an offence to do fraud after you make a connection with somebody on a phone call. What CRTC can only do now is go after you for the facts of the robocalls, but when it comes to the fraud, they don't really, like Mr. Scott said, have any jurisdiction there. I think that's the missing piece.

Mr. Ali Ehsassi: Okay, and—

The Chair: Unfortunately, that's all the time we have for you, Mr. Ehsassi.

[*Translation*]

Mr. Lemire, you have six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Madam Chair.

Thank you for your presentation. I would like to say that it comes at a time when I have just run into a senior citizen in my riding who told me that she was the victim of a major fraud. I don't think it was over the phone, but this conversation confirms the importance of our work.

I would also like to introduce Simon-Pierre Savard-Tremblay, who is the Bloc member for Saint-Hyacinthe—Bagot and who also deals with issues related to industry and international trade.

My first question is about your expectations of the CRTC, and of us, the lawmakers.

Mr. Lawford, you mentioned legislation against telephone fraud in particular. What concrete measures could be taken to help you or to ensure that the situation is regularized?

● (1135)

Mr. John Lawford: First, the CRTC should be encouraged to launch an inquiry into the SIM swap. It's a fairly minor problem at the moment, but soon it's going to get worse.

Second, as I said, the CRTC is sort of caught by the legislation, which doesn't give it enough power. I'm not exactly sure what to suggest for this organization, other than more tools to help them study fraudulent activities. There are some small weak spots in the current procedures, but they are too [*inaudible*] for you.

Mr. Sébastien Lemire: Mr. Gamble, do you have anything to add about your expectations of the CRTC and of us as lawmakers?

[*English*]

Mr. Matthew Gamble: Not right now, thank you.

[*Translation*]

Mr. Sébastien Lemire: My second question is for both of you, given your respective areas of expertise. Do you feel that the CRTC and the RCMP understand the significance of IP telephony and automated calls in relation to fraud?

[*English*]

Mr. Matthew Gamble: I believe they're trying their best to do so, but technology is always moving faster, and the minute they understand one, a new one happens.

[*Translation*]

Mr. Sébastien Lemire: Perfect.

Mr. Gamble, earlier, you mentioned that small companies were at a disadvantage compared to the large companies. I specifically asked the representatives from the three telecommunications companies who appeared on Tuesday whether they were prepared to provide assistance. They all answered that they were prepared to take action.

Do you feel that this is actually the case? Furthermore, how could we help the small players more?

[*English*]

Mr. Matthew Gamble: I believe they want to help, but the way the standards were designed makes it very difficult to do so. There needs to be some fundamental changes in how we design STIR/SHAKEN to make that a reality.

[*Translation*]

Mr. Sébastien Lemire: There is also the whole issue of the time these companies need to meet the standards, since the technology is difficult to implement. Do you believe that they are acting in good faith right now?

[*English*]

Mr. Matthew Gamble: As someone who knows most of the technology vendors they use, yes, they're working the best they can.

[*Translation*]

Mr. Sébastien Lemire: Mr. Lawford, do you feel that the CRTC has been slow to respond to people's concerns on this issue? Do you think the organization could have been more proactive from the outset?

Mr. John Lawford: The CRTC is quite proactive about spoofed numbers.

In terms of SIM swap, however, it's a real mess. The CRTC assures us that there will be a solution, but that it will be communicated to the companies only, with no transparency. So I do not trust the CRTC in this matter, and I am calling for a public inquiry to find out what it is doing.

Mr. Sébastien Lemire: My next question is about seniors.

In the opinion of both of you, are enough preventive measures being taken, and how can we ensure that we better protect our seniors?

Mr. John Lawford: My opinion may not be nice to hear. I don't think it's possible to go beyond a certain level of technological education when it comes to seniors, despite everything we may teach them or the examples we may give them when we meet with them. We get too many calls for there not to be victims. Email exchanges are more significant.

● (1140)

Mr. Sébastien Lemire: This is what I'm gathering from your comments: the volume of calls is too high, which means that there are a lot of victims even though the official number of fraud cases is low.

Mr. Gamble, do you have anything to add with respect to seniors?

[*English*]

Mr. Matthew Gamble: No. I would agree with John on all the challenges he mentioned.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

The Chair: Thank you very much.

[*English*]

Our next six-minute round goes to MP Masse.

Mr. Brian Masse (Windsor West, NDP): Thank you, Madam Chair.

All the evidence right now is that this disproportionately hurts seniors and people in the low-income sphere. Is that correct?

Mr. John Lawford: That's certainly my understanding. In particular, it's newer Canadians, who may be more scared of calls.

Mr. Brian Masse: I'd ask both of you this. We heard the companies outline some of the things they were doing, but they also get an escape from CRTC from not having to offer free call blocking. It would seem reasonable to me that call blocking would be offered as a universal system or that this should all be employed and not cost Canadians. They were unclear about what they offered and didn't offer in packages.

We're going to do more research on this. Basically, as a consumer, you have to pay more to get more filtration and protection from fraud. Is that a correct statement, yes or no?

Mr. John Lawford: I would say yes and no, and then let me explain.

For the blocking of spoof numbers, that's free. It's a CRTC ruling. For STIR/SHAKEN, it depends on the way they implement it. For the network thing, I really think Bell and these guys are going to charge you $10 a month.

Mr. Matthew Gamble: I would just add that there are some carriers in Canada that do charge and some that do not.

Mr. Brian Masse: Yes. That's one thing I'm looking for recommendations for. Until STIR/SHAKEN is implemented, that should actually be provided to consumers right away. This is a clear abuse pattern we're seeing. If they're asking for more time for STIR/SHAKEN, there needs to be a benefit back to Canadians to stem the tide of this abusive behaviour, which is also, I'd argue, a bane on our economy. We saw that with spam in the past, and those were some of the reasons we brought in those laws.

Would it be unreasonable for consumers to expect something similar to a J.D. Power ranking of some of these carriers in terms of how they deal with fraud? We do that for the auto sector, where I come from. It allows an independent voice to take a look at each. They can decide, as a consumer, what they're getting charged for and what they're getting benefit from.

My concern is that if you have a higher income and more money in your pocket, you can actually get a better benefit and protection than lower-income Canadians. I think that informing consumers and letting them decide would be something that might be helpful.

Mr. John Lawford: If you end up with a system where consumers are paying for some of this protection, then I think that having some kind of ranking would be one way to do it.

If it's a regulatory requirement that it be offered, then the CRTC should still collect statistics to see if they're complying and how good their systems are. If they're below standard, then we could look at ways to try to improve each carrier.

Mr. Matthew Gamble: Once STIR/SHAKEN is there and made available, the end result will be close to what spam filtering is today. We'll be able to judge based on how much spam we receive. There would be metrics available.

Mr. Brian Masse: The key, though, with some of the systems is that if you can't afford to have someone upgrading the system, you're not going to be a candidate for that. The new devices that are going to be capable of this either have to be mandated or you'll have to replace them, which is also going to be an economic boon for some and a detraction for others. It's also more complicated for some people who don't have the ability to swap their phone plan program out sooner than others. That's going to be a big issue.

At this point, should we ask the Privacy Commissioner for commentary? The problem we have with the CRTC, quite frankly, is that it hasn't had a major overhaul in over 20 years. Expecting them to make some of these changes alone without a legislative change from Parliament is going to handicap them very significantly.

Should we be asking for advice from the Privacy Commissioner on STIR/SHAKEN and this issue?

Mr. Matthew Gamble: I believe we should. There are serious implications when data is passed to third parties for analytics that have not been addressed yet.

Mr. John Lawford: I'd just add that thinking about digital policy in a more holistic way will help us a lot. We're not quite there yet. Involving the Privacy Commissioner would assist with STIR/SHAKEN, but with the other network-level blocking as well, to see whether there are any concerns. Perhaps it should also include, if it comes into being, the digital commissioner office.

● (1145)

Mr. Brian Masse: When we are looking at some of our international obligations for trade agreements, should this be a thing we include as one of the actual components? The new USMCA has the digital charter as part of it, but is this something we should be looking at with regard to our trade agreements with other countries?

Mr. John Lawford: By that, do you mean protecting any regulations we set up so as to require this?

Mr. Brian Masse: Yes, I do, and maybe to require some type of oversight or some type of side agreement related to telephone and Internet abuse and fraud.

Mr. John Lawford: I would say yes, from our group's point of view, but getting it to be part of an overall digital policy that goes with trade policy and makes sense is the trick.

Mr. Brian Masse: You mentioned more work on fraud from Parliament Hill. Can you give me more specifics about what you think we can do under the context we currently have and maybe suggest some regulatory improvements?

Mr. John Lawford: The point of the comment at the end of my remarks was that the fraud provision in the Criminal Code may need to be made more specific for telephone-delivered or phished fraud.

The Chair: You still have 10 seconds.

Mr. Brian Masse: That's okay. Thank you.

The Chair: Thank you very much.

Now, we will move into five-minute rounds.

The next round will go to MP Van Popta.

Mr. Tako Van Popta (Langley—Aldergrove, CPC): Thank you.

My question is for Mr. Lawford and follows on what Mr. Masse was just asking about.

The CRTC is obviously a key player in this whole thing of fighting against telephone and Internet fraud. You were suggesting that perhaps it's time for an investigation into the effectiveness of the CRTC.

Is there something missing in its enabling legislation or is it just ineffectiveness of the organization?

Mr. John Lawford: I won't go quite as far as to say it's ineffectiveness of the organization. They have a mandate, which is limited now, to stop telemarketing that's illegal and to do the do-not-call list. That's it. Their job is not to stop fraud, as Mr. Scott said very clearly.

Mr. Tako Van Popta: Would it be helpful for the CRTC to have its mandate expanded? What can parliamentarians do to help?

Mr. John Lawford: Yes, it would help.

Mr. Tako Van Popta: Specifically, what could they do?

Mr. John Lawford: This is the question of how to design a law that would specifically call something phone fraud, or wire fraud, as they call it in the United States, so that it's a separate fraud offence. You could think of things.

For example, at the moment, getting somebody to prosecute a fraud is difficult because you can't go back up the chain and make everybody who was involved in the calling—the actual person talking, and then the people who own and run this thing, whether they're in Canada or not—criminally liable for it. We might design a law that makes everybody in the calling operation have some level of criminal liability, so as to make it less attractive, less consequence-free, as Mr. Gamble said.

Mr. Tako Van Popta: Good.

One of our presenters earlier this week said that despite having identified hundreds of thousands of fraud callers, they need approval of the CRTC to actually block them from reaching their customers.

Would you agree with that?

Mr. Matthew Gamble: The current interpretation of the Telecommunications Act supports that view.

Mr. John Lawford: Here's the weird thing about this whole area. The calls that are made as robocalls are illegal. You're not allowed to call for commercial purposes with robocalls—the end. The only exceptions are for hospitals and schools and such things. The calls are illegal, but once somebody answers by pressing "2" or "1" and talks to somebody, that call only becomes fraud when you finally send the money. While the person is trying to scam you, there's no crime going on.

That's the trick. How do you make that part easy to solve and stop? The companies can't listen to the content, because they need a warrant. That's the conundrum we're facing.

Mr. Tako Van Popta: Is there an easy solution to it?

Mr. John Lawford: There is not an easy solution, but I'm suggesting that perhaps there could be a well-crafted law that might, if there are actual victims who lose money, trace it back to the calling operation. If you can prove that all those calls were sent out as stage one phishing—"Look, I got this fish on the hook"—and there were enough fish on the hook that we should prosecute the whole operation, there might be some way to do so.

● (1150)

Mr. Tako Van Popta: In this fight against telephone fraud, we have talked about the CRTC and its regulatory power, but how effective a tool can technology be? I'm thinking specifically of STIR/SHAKEN. One of our presenters earlier this week said that they are ready to roll it out, but that people's personal devices don't have the technology yet.

Mr. Matthew Gamble: There are two sides to STIR/SHAKEN. There's the network side, which we're more interested in, which is what we can do at the network level, blocking the calls before the consumer's phone even rings. Then there's what they refer to, which is the presentation layer, that checkmark or that notification to the end user on the phone that it's a blocked call.

There's a lot we can do to prevent the obvious stuff at the network level. Then the more fine-grained stuff will require new handsets and things such as that.

Mr. Tako Van Popta: How long is this likely to take?

Mr. Matthew Gamble: That's unknown at this point, because the standards are still being worked on for that display level of things. Then we have the issue of all the Canadians who don't have even digital phones, such as the elderly and others, who still have analog devices that are incapable of even displaying augmented data.

Mr. Tako Van Popta: The timing of this is obviously going to rest significantly on consumers' ability or willingness to buy into the new technology.

Mr. Matthew Gamble: That's right, so that we will get some benefit from day one from the network level of things.

Mr. Tako Van Popta: I have a question for Mr. Gamble.

The Chair: You have 10 seconds.

Mr. Tako Van Popta: I will defer, then. Thank you.

The Chair: Thank you very much.

The next five-minute round goes to MP Jowhari.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Madam Chair.

I will be sharing my time with MP Casey, so I have a quick two and a half minutes for the question and response.

Mr. Gamble, you talked about STIR/SHAKEN. You talked about the policy, the technology and consumer privacy specifically around data source outsourcing for analytics. You also talked about the disadvantaging of the smaller carrier. What you said that stood out for me, though, was that there should have been some design consideration at the outset which was somehow missed that may have resulted in the disparity.

Can you shed some light on what those design changes should be to bring the two back together?

Mr. Matthew Gamble: I'm not going to try to dive really deeply into the level of the technology design decisions that would warrant this, but the real challenge is that there's no easy way to move the ownership of a phone number from one party to another and delegate that responsibility. This is being worked on now, but in digital certificates it's highly difficult.

It really comes down to how we treat the reseller phone companies. They have always, in the phone networks of Canada, been lesser than the parents, but there's never been a reason for that to be an issue. If we allow more carriers to rise up to the facilities-based level, with SIP interconnections and such things, we can solve some of these issues.

It really goes back to the way the whole resale system was designed, and it can't easily be overhauled.

Mr. Majid Jowhari: Do I still have some time?

The Chair: You have three and a half minutes.

Mr. Majid Jowhari: Well, no, I'm sharing two and a half, so I have about a minute.

Can we talk about consumer privacy and the outsourcing of the data for analytics? Is that again going to be disadvantaging any of the small players?

Mr. Matthew Gamble: That's difficult to say. The players don't all say whom they outsource their data processing to, and some may not. There's no requirement to outsource to a third party analytics company. If you want to offer the best spam filtering, however, you're going to get the best analytics you can get, which may require you to share data with third parties.

Those parties right now are generally American, and while they say they may not share data, you have to worry about, first, the data's leaving the country, and second, the potential for data breaches and for data to be compromised.

Mr. Majid Jowhari: Okay. Thank you.

Mr. Sean Casey (Charlottetown, Lib.): I want to come back to the same point, that there is a weakness in the STIR/SHAKEN framework because of its unfairness to smaller players. You've indicated that this is not easily solved. Is this a case in which the perfect is the enemy of the good?

Is this a fatal flaw and one that would justify our not pursuing this, given that it appears that only the Bell network-blocking solution is one that might work?

Mr. Matthew Gamble: It's not a fatal flaw. There are currently two or three proposals for solving this floating around the working group known as ATIS. There just hasn't been a consensus on it yet.

I believe the groups will get to a consensus, probably in the next six to eight months, but when the CRTC says it wants it done by September 30 of this year and the solutions to fundamental issues are still six to eight months away, those two conditions don't really line up together.

● (1155)

Mr. Sean Casey: That also ties into something you said earlier about trying to stay ahead of the fraudsters. For this framework, I take it the history in other jurisdictions has been positive. Are we yet at the stage that the fraudsters are catching up and we need the next generation?

Mr. Matthew Gamble: I don't believe so. I think there may be some regulatory changes needed once STIR/SHAKEN is done.

Currently carriers are not responsible for the calls they place on networks. Once STIR/SHAKEN allows you to identify which carrier is the source of a call, then you could probably empower the CRTC to.... If a carrier were known to be the source of a large majority of fraud calls, they might then somehow be found liable for those calls.

Mr. Sean Casey: Mr. Lawford, I'm quite interested in your comments about something else that holds promise: this technology that's available through Bell. Your question was whether it will be sold to us or offered for free.

What would be the societal risk of its being offered for free? What sort of reaction can we anticipate from Bell? Would we be deprived of it if it were mandated to be free?

Mr. John Lawford: No, not necessarily, because I believe Bell also wants to stop fraud calls, because people are cancelling their land lines. One of their reasons for doing so would be just to stop the bleeding.

They thus may well do it anyway. They may want to sell it in certain contexts; non-consumer contexts, I believe, would be fine. At the consumer end, my only concern is about some people having this technology and others not.

The Chair: Unfortunately, that's all the time we have.

I would like to thank you both for being here today.

We have to wrap this up a few minutes early, because our next group requires some technical things to happen. It will take us about 10 minutes to set up for the next group.

Thank you again for coming. I hope you have a great afternoon.

● (1155)

_____(Pause)_____

● (1205)

The Chair: Ladies and gentlemen, welcome to the Standing Committee on Industry, Science and Technology. We are doing a study on fraud calls.

With us today we have Mr. Randall Baran-Chong, co-founder of Canadian SIM-swap Victims United.

Via video conference we have Kate Schroeder, board member of the Canadian Network for the Prevention of Elder Abuse.

Welcome, both of you. You will have 10 minutes each to present to the committee, after which we will go through tours of questions from the members of Parliament.

If you see me waving the yellow card, you have 30 seconds. That doesn't mean don't look at me so that you don't see the card. It means you have 30 seconds to wrap up your response.

To make sure that we don't lose Ms. Schroeder who is coming in via video conference, we'll start with her.

Madam Schroeder, you have 10 minutes.

Ms. Kate Schroeder (Board Member, Canadian Network for the Prevention of Elder Abuse): Good morning, Madam Chair. Thank you and thanks to the committee for including us in the conversation surrounding this important topic.

The Chair: Madam Schroeder, I'm sorry, I would ask you to hold for one second. We're having some technical difficulties. We can't hear you.

Okay, please continue.

Ms. Kate Schroeder: Perfect.

My name is Kate Schroeder. I am a board member for the Canadian Network for the Prevention of Elder Abuse, which is also referred to as the CNPEA.

The CNPEA is a pan-Canadian network supported by leaders in the field of aging, research, health care, and elder abuse prevention and response, among other matters. The CNPEA connects people and organizations, fosters the exchange of reliable information and advances programs and policy development on issues related to preventing the abuse of older adults. We do this at local, regional, provincial-territorial and national levels through our knowledge-sharing hub at cnpea.ca.

We are pleased to have this opportunity to bring to light the challenges and impacts of fraud calls on older adults in Canada. The CNPEA's work focuses on gathering and disseminating adaptable resources, best practices and current research and policy development by Canadian expert stakeholders in order to increase our collective capacity to address and prevent the abuse of older adults. The following comments and recommendations are based on the extensive work of some of these experts.

Fraud calls are an attempt to deceive an individual to gain control over some aspect of that individual's life, whether financial or related to identity or some other aspect. These types of criminal attempts have an impact upon all Canadians, regardless of age, race, education or background. Vulnerable health, fledgling finances and a rarefied social network, among other factors, can heighten the risk of falling victim to potential scams, and this risk only increases as individuals age.

The rapidly shifting demographic in Canada is having impacts upon all aspects of our country and its economy. By 2031, some 23% of Canadians will be over the age of 65. By 2061 there could be 33% more seniors than children living in Canada. This shift is already presenting us with troubling new statistics in relation to fraud, and we expect these statistics to continue to increase as our population ages, since seniors are often identified as easier targets.

As of February 29, 2020, available statistics from the Canadian Anti-Fraud Centre indicate that so far this year there have been 7,804 reports of fraud or attempted fraud, and year to date over 4,119 Canadians have been confirmed victims of fraud, with more than $9.2 million lost.

According to the Canadian Anti-Fraud Centre, phone scams defrauded Canadians of an estimated $24 million between January 1 and October 31, 2019. Available statistics indicate that losses experienced by older adults account for as much as 25% of the total losses related to reported fraud and that this number is rising considerably.

The troubling aspect of these numbers is that they only reflect the fraud that's been reported. From available studies we know that the rate of fraud reported may be as low as 13%, often because older victims are afraid or ashamed to be deemed incompetent or otherwise deficient for falling prey to these calls.

Fraudulent calls are running rampant across Canada. Current scams include but are not limited to phone spoofing scams—numbers that imitate legitimate phone numbers—Canada Revenue Agency scams, grandparent scams, warrant calls, free reward calls offering trips and cruises, natural disaster scams, technology scams.

The grandparent scam, technology scam and the Canada Revenue Agency scam may be more likely to affect older adults. One major factor contributing to this is social isolation, which is considered a heightened risk factor for elder abuse in general. Isolated adults craving human connection, missing their family or lacking a support network may be more likely to fall for these scams and be more easily preyed upon.

The reasons that older individuals fall for these scams are often complex and interconnected. Potential risk factors that put individuals at greater risk may include the recent loss of a loved one; the lack of a support network; social isolation; economic insecurity; poverty; potential cognitive impairment; lack of awareness or understanding or the nature of these calls; and sophisticated, ever-changing technology.

Falling for these scams often leads to individuals feeling stigmatized. The complicated process of reporting and investigating these types of fraud lessens the chance of individuals completing the reporting process.

● (1210)

Some of the issues we've noticed that impede the reporting process are the fear of appearing incompetent; the fear of having their autonomy or decision-making abilities questioned; the fear of admitting to their children or loved ones that they made a mistake, as talking about money and technology often can be a fraught experience in families between parents and children; the potential lack of awareness of where to report; and, the potential to encounter ageism when trying to explain their situation.

What we are certain of is that these types of fraud calls are on the rise and are impacting all Canadians. Solutions must be unique and intergenerational in approach as well as collaboratively arrived at between private and public sectors, consumer groups, financial agencies and law enforcement. Some of the biggest keys to prevention and detection are awareness, education and easy access to reporting, as well as a respectful and informed approach to communicating with and supporting older victims.

Our overall recommendations from the CNPEA include the following: to develop awareness campaigns in all forms—social media, web based, print, TV—to help people, regardless of age, to understand the different scams and forms of fraud currently circulating; to support and promote bystander intervention training programs at financial institutions, law firms and other consumer groups; to support the development of programs not only to help Canadians navigate the complexities of reporting fraud but to markedly improve the access to support after reporting to prevent revictimization; to encourage the development of awareness and support programs that are accessible from home or other living arrangements; to improve access to regular and affordable transportation in rural areas to prevent social isolation and to facilitate access to necessary resources; and, ongoing proactive communication from various stakeholders—CRA, banks, telecommunication companies, senior service providers—to provide updates on current scams impacting older adults.

Thank you.

● (1215)

The Chair: Thank you so much.

Next we will go to Mr. Baran-Chong.

You have 10 minutes.

Mr. Randall Baran-Chong (Co-Founder, Canadian SIM-swap Victims United, As an Individual): Good afternoon. My name is Randall Baran-Chong. I'm an entrepreneur from Toronto, hence why I wanted to articulate myself through a PowerPoint.

I'm here to represent Canadian SIM-swap Victims United, a grassroots organization of victim advocates from across Canada and across all walks of life, formed as a result of what's described as one of the phone frauds that experts fear most. As victim advocates, we take our harrowing experience into hope for greater awareness, combine that with expert advice, and engage industry and leadership like you to promote action, with the sole objective of not adding another name to our roster.

Though my story starts back at the end of October 2019, this really begins back in 2007, with one of your former colleagues, Maxime Bernier, minister of industry at the time, announcing wireless network portability. In essence, what that was all about was to provide consumers the power to essentially vote with their dollars in terms of moving from carrier to carrier without being encumbered by losing their number.

It was all about empowering consumers and their choice to go to the carrier they wanted, but while well intended—like the road to hell, it was paved with good intentions—it led to the hell that many of us victims know as the SIM swap scam, also known as the unauthorized customer transfer or unauthorized porting. What that essentially describes is the transfer of someone's phone number from their own SIM to another SIM without the authorization of the account holder.

Let's dissect generally how SIM swapping works. The vast majority of SIM swaps are financially motivated. These fraudsters begin by doing their homework to gather the goods. What I'm referring to is the fraudsters getting a real understanding of who these victims are at a personal level and trying to find some identifiers about them, but really, if they're trying to do it through an unauthorized porting, they want to get the key pieces of information that are required to execute the port. These are, first, the phone number itself, and then one of the following, as described by the Wireless Network Portability Council, which has defined these rules: the account number of the holder, the device ID or a PIN. If you think about it, you only need the phone number plus one of those identifiers, and the phone number is highly accessible for most of us, so you already have half the job done.

How do you get the rest of it? This is where the methods of these fraudsters take place.

One of the major methods they use is social engineering, which means taking advantage of the human fallibility of the customer service reps. Oftentimes, they'll pretend: "I'm the customer, I lost my phone, I desperately need to get a phone back." They'll play the system. They might even say that they forgot their PIN and will provide other types of information that are even more accessible, such as postal code or maiden name and things like that, to get around it and get access to the porting information.

They'll use phishing, fake phone numbers or fake emails purporting to be from Rogers and saying to enter your account number, but it's really the hacker who is getting your information. They can also use social media to find personal information about the person and, recently, even through data leaks. Telus and its flanker brand Koodo announced that their customers from 2017 and prior had their account information compromised by an unauthorized user, and they all had to get port protection put on their accounts.

Finally, and most nefariously, they have inside employees. This is something that we've seen in the United States, where employees at companies like AT&T and T-Mobile actually sold account information for $20 or less to these fraudsters.

That is how they execute the port.

Now that they have the information, what they'll often do is get a prepaid phone account. There's no identification required to get a prepaid phone because of PIPEDA; it's essentially untraceable to these people. Now that they have the information, they'll call and execute the port with that carrier and, under the CRTC decision from 2005, this has to be executed within 2.5 hours or less.

I saw on Tuesday that one of you got a CRA scam text, and I hope you never see on your phone that your SIM is no longer in service. That's how the victim finds out that they've been ported over. The victim has not really been involved. When I had mine happen, it was at 11:40 at night, and I suddenly saw that my phone was no longer working. I thought it was technical, but it turns out that I was being ported.

● (1220)

From that point forward, any calls that are outbound or inbound—texts, anything like that—are in the possession of the fraudsters themselves. For this next stage, which we call "forget it and reset it", I'm sure many of you have text-based factor authentication with your social media accounts, bank accounts and things like that. If you forget your password, you click on "I forgot my password", and it will send you a text for a one-time password to reset your password. Then, essentially, they can redefine the password.

Now that the fraudster has your phone number, they are receiving those texts or calls, and they are going in and locking you out of your very own account. It then comes to the plundering. Oftentimes, these fraudsters will work in teams to create this havoc. It manifests itself when you see emails flooding into your inbox saying that your account password has been changed and a new contact has been added to your account, and all you can do is watch.

In my particular case, which happened at night, as I've mentioned, I called my carrier and was told, "Thank you for calling customer service. Our hours are from 8 a.m. to 8 p.m., Monday to Friday." They put up a 12-hour defence for an enemy that fights a 24-hour war. To get the phone number back, it oftentimes takes several hours or, in some of the cases we've seen, up to a few days.

How is the damage done? There are three key ways in which they try to take advantage of this. One is the direct theft. In particular, crypto is a flavour they prefer, because it's very hard to trace them afterwards, but there are average victims, such as the Johnson family of Peebles, Saskatchewan, who lost hundreds of thousands of dollars from their farm account. Others take advantage of the apps that have credit cards linked to them, as in the case of nurse Sheila O'Reilly from Oakville.

In my case, they tried to extort and blackmail me. They got access to my cloud drive. Essentially, as a small business person, with my small business account and my personal account all being on this cloud drive, five years of my life are now in someone else's hands. I told this story to someone in the United States who lost a million dollars—90% of his life savings—and he said, "Your offence that you had against you was much worse." He feels bad for me.

Oftentimes what they'll do is take this data and monetize it on the dark web for the low low low price for log-in credentials of $20 to $120 and to $3,000 for full identification. In other cases, they will take over accounts. Jack Dorsey, for example, the founder of Twitter...if the founder of Twitter can be a victim of a crime like this, who amongst us is safe? Even celebrities such as Mariah Carey and Adam Sandler have been victims of this. In other cases, they target accounts that have desirable user names. There's a man in Toronto named Jack Hathaway, who lost his Instagram handle "cosplay", which is a highly valued target.

Unlike things like phone spoofing or these other frauds that you heard about earlier, these aren't necessarily done from call centres overseas that we feel we're helpless to take action on. As recently as November an arrest was made of an 18-year-old from Montreal who has participated in the theft of $300,000 from Canadians and over $50 million from Americans.

What this really demonstrates is that these aren't sophisticated programmers, hackers and coders who are doing this. These are the people who know how to play the game. These are commonly done—in the arrests that have been made in the United States, for example—by people under the age of 25.

We came to the realization that our phone numbers are our new form of identity. Our SIM is like our new SIN, and security is as strong as the weakest link, whether it's technical or human. Finally, when it comes to unauthorized porting, it can have lifetime impacts, so we need to change the way we think about these things.

● (1225)

How is it being dealt with elsewhere? In the United States, they're treating it as a national security risk. In places such as Africa, they're using co-operation between the banks and the telcos to identify fraud risk. In Australia, they have actually taken regulatory action to introduce pre-porting processes to identify whether or not you have actually validated the requests. They've even introduced buy-ins for telcos that don't comply with the authorized porting process.

The Chair: Mr. Baran-Chong, unfortunately, that's your 10 minutes for your presentation.

Mr. Randall Baran-Chong: Okay.

The Chair: I want to thank you, though, for sharing your story. We have your documentation and I hope that in the rounds of questions you'll have a chance to give us more information.

Mr. Randall Baran-Chong: Thank you.

The Chair: With that, we will start the six-minute round.

Our first round of questions is with MP Patzer.

You have six minutes.

Mr. Jeremy Patzer (Cypress Hills—Grasslands, CPC): Thank you very much.

My first question will be for you, Mr. Baran-Chong.

With what you've gone through with your own incident, you have always done a lot of thinking about different measures that could have prevented scammers from hijacking your number and how Rogers could have protected you. I think you were kind of building to that here before you ran out of time.

What are some of the things providers could do to prevent unauthorized number transfers? Maybe you could elaborate on where you were going with what you were about to say.

Mr. Randall Baran-Chong: My apologies for that.

In terms of what we think, from the Canadian perspective, first, there need to be changes to the regulations and something similar to what Australia has done with pre-porting authorization needs to be introduced. It's as simple as getting a text from the new carrier that says, "Did you request this porting over?" With what Australia introduced, essentially you have to get either a call or a text from the new carrier. 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. But as John Lawford from PIAC kind of alley-ooped me there in setting things up, there needs to be more transparency as well around the process.

The CWTA has requested that a lot of the information about processes be redacted or not shared, but it's widely known within cybersecurity that security through obscurity doesn't work. As an example of that, one of the things that Rogers did was to text people to say, "We received a request that you wanted to port your phone number. If it wasn't you, call us." This fails on three different levels.

First, there are instances when people, because of the distrust that's been caused by all these frauds, think that it's a fake text in itself, so they just ignore it. Then the port still gets executed within that two and a half hours. In the second case, there have been instances of people trying to reach them through the hotline and they are never able to get through. One port was executed within 12 minutes of receiving the text. In the third case, if a really smart fraudster looks at it, they'll look at your social media, find out when you're on vacation, and then execute the port so you don't even have your phone on you.

There are obvious ways in which we can at least temporarily get rid of this, and then we need to move away from SMS-based two-factor authentication entirely.

Mr. Jeremy Patzer: Right. What other modes of two-factor would you...or would you like to see a whole other means that is different from what Australia is doing?

Mr. Randall Baran-Chong: There's something called soft-token authentication. There are things like Google Authenticator or Authy or things like that, which are available for quite a few different types of apps and things that we use. A lot of social media offers it. But often it's a secondary offered form of authentication. It's not widely known. It's accessible only to smart phone users unfortunately. But there are still a lot of things we use in which they promote two-factor authentication by SMS, and still banks often promote that only.

● (1230)

Mr. Jeremy Patzer: Thank you for that.

My next question will be for you, Kate.

During the last meeting, I raised the growing problem of scammers, which are increasingly targeting people through online social media or text messaging. We know that young Canadians are present on these platforms, but could you say something about how this issue might be particularly affecting seniors?

Ms. Kate Schroeder: It is not a misconception and definitely social media is extremely prevalent with our younger generation, but it is also extremely prevalent with senior Canadians. Facebook is a very, very hot popular thing for aging Canadians. It is unfortunately a breeding ground for fraud, romance scams and all of those types of things. It all stems from that need for connection, that want for a relationship, the need to feel connected. It's that social isolation piece we focus on that is stemming from those connections that our senior population are trying to build in that social network.

Mr. Jeremy Patzer: Yes, for sure.

For the education and even the awareness side of things as well, what more needs to be done? Are there already steps being taken by groups such as yours to get that education and awareness for seniors? Are there programs out there that they can understand, that can help them be aware of these things?

Ms. Kate Schroeder: I think there are certainly programs out there. I know the Canadian Competition Bureau has “The Little Black Book of Scams”. It's available. It talks about all of these things.

It's really about promoting these resources that are available and having them widely available in all sorts of different social services, banks and agencies. I think there is a need.

Again, because our senior demographic is so robust, one person may see it online and another may see it in print, so we really have to cover off all of those areas. I would say there is a need for a more robust promotion of those materials that are out there.

Also with regard to the new things that are coming out, to speak to what Mr. Baran-Chong just said, I think we're really good at promoting information about the CRA scams, romance scams and things like that, but there needs to be more robust communication from telecommunication companies and things of that nature, on the emerging scams and the things people need to be aware of.

The Chair: Thank you so much.

Our next round of questions will go to MP Jaczek.

Ms. Helena Jaczek (Markham—Stouffville, Lib.): Thank you, Madam Chair.

Ms. Schroeder, I really appreciate what you've had to say to us and I totally concur with all you've said.

One of the previous witnesses, Mr. Lawford, made reference to the fact that perhaps some seniors are actually giving up their land lines because they are so fed up with phone scams, nuisance calls and so on. Are you aware of any of that? Has that been an issue at all for your clients?

Ms. Kate Schroeder: Yes, it is happening. I think as our demographic continues to age, our world is moving to a more mobile cellular network type of environment certainly. I think we can all concur that this doesn't necessarily eliminate the problem.

I think it's twofold. If they're simply eliminating their land lines, there's obviously concern that only adds fuel to the fire of social isolation and to the concern that if something is wrong, how we will get in touch with these people to make sure they're safe and okay.

Again, with regard to the cellular network piece of it, we get just as many fraud calls on our cellular devices as we do on our land lines. I definitely think we're seeing that. I think it's concerning, because it only adds more concern regarding the potential risks to those individuals.

Ms. Helena Jaczek: Exactly. As Mr. Baran-Chong has alerted us, if they give up their land line, they're obviously going to start relying on cellular phones and presumably they will be just as vulnerable to this SIM-swap scam that we've just heard about, which was totally new to me as of yesterday, so I'm extremely grateful to have heard a lot about this.

Mr. Baran-Chong, you weren't quite able to finish your presentation. You talked to us about Australia and how if somebody claims to have lost their phone, they have to personally attend and show their government ID, etc. Could you talk about what you feel the CRTC should be doing, given the facts?

● (1235)

Mr. Randall Baran-Chong: Absolutely. I think first codifying that within the regulations is important, because what we've often seen the carriers do is to fall back on saying they're complying with the regulations. However, the decision was made back in 2005, and obviously the kind of threat environment has changed quite significantly.

As Mr. Lawford alluded to earlier, the CRTC also needs to be much more transparent in asking the CWTA and the industry to be more transparent about the prevalence of this. Are they effectively dealing with this?

We appreciate that the CRTC issued the letter back on January 15 of this year, but the letter that came back from CWTA was highly redacted with regard to anything that was interesting to us, such as the measures being taken and the prevalence. As well, there was no sense from us of what the CRTC would assess as effective measures from the industry, the kinds of potential enforcement measures they'd take if they didn't act upon this or the implementation schedule, because the longer this persists, the greater the number of victims that will be racked up.

Ms. Helena Jaczek: Would one recommendation be a public airing of the CWTA's response? How do you see this going forward practically?

Mr. Randall Baran-Chong: I think there at least needs to be recognition, especially for the customer-facing elements in terms of the protections that are introduced, that there should be more disclosure about that and participation of customers in that. I mentioned the issue with the texts that went through. People weren't aware that a new protection was introduced, so they were immediately skeptical of it. These kinds of measures need to be more publicly aired.

I can understand, though, that one part that needs to be addressed is around training their staff more. I can't tell you how many times I've called my telcos and had to teach these customer service reps about their porting policies—in fact, up until last night; I almost used social engineering to get my pin from someone who really didn't.... I provided information that's very easy to obtain.

There needs to be training of employees too. I can understand if that part is not necessarily publicly disclosed, but there needs to be two sides to this.

Ms. Helena Jaczek: We pulled up an article on SIM-scamming yesterday. Apparently, there's some advice from the OPP on how people can protect themselves.

You talked about the personal information—do not answer phishing emails and text messages—but using an off-line password manager is something that's completely new to me. Could you explain what that is?

Mr. Randall Baran-Chong: That's the soft-token authenticator I was alluding to earlier. It's like Google Authenticator. It generates a code on your phone and asks you to essentially replicate the number you're getting on your app and put it in. Instead of getting a text message, you're using that number. You can also use a hardware token. Some people might have seen those RSA keys that generate a number as well. A hardware or soft token could be used to authenticate. Essentially, you just don't want to tie it to your phone.

Ms. Helena Jaczek: Thank you so much.

The Chair: Thank you.

[*Translation*]

Mr. Lemire, you have the floor.

Mr. Sébastien Lemire: Thank you, Madam Chair.

I will continue with Mr. Baran-Chong.

[*English*]

I'm sensitive to your reality and I appreciate your push to use your experience to help other people out in terms of prevention.

[*Translation*]

You have come up with several expectations of the CRTC. They are at the end of your document, and I thank Ms. Jaczek for pointing them out.

Do you have any other expectations of the CRTC? Also, do you have expectations of the RCMP and the telecommunications companies?

● (1240)

[*English*]

Mr. Randall Baran-Chong: I'll give you an example. There was recognition, I think, by the different law enforcement agencies that have been dealing with this that there needs to be more coordination. Even though maybe these criminals are working in teams that are close to each other, these victims span across the country. The RCMP is launching a national cybercrimes coordination unit, which will be launching this year, I believe at the end of April. They will be able to better coordinate these cases. When we as victims share our stories, we're often able to almost hear these common denominators between these crimes. We pass that off onto the law enforcement agents who are working on our cases.

As we said, we need codification of these new types of pre-porting notifications and verifications and more transparency around what's going on with the porting. We need to ensure that the telcos are implementing policies and doing it consistently. Finally, I think governments and industry should be studied, in terms of the ones that have sensitive data, on whether they're using SMS-based 2FA, and how we can transition away from that. Otherwise, we put ourselves at the peril of SIM-swapping.

[*Translation*]

Mr. Sébastien Lemire: In your situation as a victim, did you receive any support or assistance from anyone at all?

[*English*]

Mr. Randall Baran-Chong: I was offered $100.

[*Translation*]

Mr. Sébastien Lemire: Is that all?

[*English*]

Mr. Randall Baran-Chong: Yes, I think that speaks volumes.

[*Translation*]

Mr. Sébastien Lemire: This is appalling.

You talked about the illegal sale of data by employees. How can we help companies adopt better security measures to prevent them from selling client information so easily? I am thinking of Desjardins, which is receiving a lot of attention in Quebec. Should we increase searches of intranets or patrols by security guards, or take other measures? What do you suggest that we do at the source?

[*English*]

Mr. Randall Baran-Chong: Individuals are partly responsible as well in terms of their data, for example, what they put into things like the cloud. To some degree, I'm paying a top-bracket idiot tax for uploading almost everything. I actually wasn't even aware that all that stuff was being uploaded, because I didn't really use it.

I wanted to come forward with my story to let people know that you should be careful about what's being put on there. Cyber experts, ironically, are saying to go offline, don't use cloud, save on an external hard drive. They're even saying to not save passwords on your browsers; write it down on paper, and write with a marker, so that the pen doesn't imprint on the paper. We're making a 180° turn in terms of how we are becoming more careful about the stuff we store. On the consumer side, that's the most important part, to be aware of what we have there.

[*Translation*]

Mr. Sébastien Lemire: Your message has been heard.

I have one last question. Earlier, Mr. Lawford talked about the need for a public inquiry. Do you agree with him?

[*English*]

Mr. Randall Baran-Chong: Absolutely. We're almost kindred spirits on that. I came across his letter when we were doing our look at the stakeholders who were interested in this. If we had given our feedback of some of the solutions we thought of—it was very similar to the Australian solution—and if this was introduced months ago, back when they introduced their text message thing in November, we would not have some of these members in our group because it would have been prevented. They would have known about it in advance.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

My next question is for you, Ms. Schroeder. You talked about a prevention campaign and the challenge of transportation, particularly in rural areas. Could you tell us more about that? Is it actually more serious in rural areas? Are there proportionately more victims in rural areas? Could an assistance and awareness program for online shopping be part of the solution? Is there some technology that is more appropriate for seniors and that could better protect them?

● (1245)

[*English*]

Ms. Kate Schroeder: Further to that comment, my recommendations would be.... In rural communities, they do not necessarily have access to many different social services. The greater the population, there are more social services, more facilities and more activities that people can be involved in. When we're looking at rural communities, where awareness, programming, documentation and all of those things are out in print, again—

The Chair: Ms. Schroeder, unfortunately that's your time. Maybe the next person will let you continue.

Mr. Masse.

Mr. Brian Masse: Thank you.

Ms. Schroeder, if you want to finish, please go ahead.

Ms. Kate Schroeder: There is a need for a campaign, or to make sure that those resources.... It speaks to the need for a collaborative approach. There is a need to ensure the information that is out there and available is shared among all different social services, including banks, insurance companies and telecommunication companies. In places that are less populated or more rural in nature, that same information and those same resources must be made available to everybody in that demographic.

Mr. Brian Masse: How do the seniors you're working with right now take advice from the companies with regard to their privacy? I'm less convinced this has been a high priority for them with regard to the frustration, and where we are with regard to a particular spot. In fact, we know there are not a lot of resources for fraud prevention. Even the RCMP admitted here that sometimes police direct people to the wrong place.

Given the fact that people are paying so much out of their pockets for this type of device, whether it be a land line or a mobile device, are you hearing any support coming from the telcos to help with fraud directed at seniors?

Ms. Kate Schroeder: To be honest, I haven't seen a ton.

Unfortunately, my experience is usually after the fraud has occurred. It has already happened, so that prevention piece hasn't really worked in those cases.

However, I would definitely agree with your comments that there appears to be a lack of support in terms of reporting, dealing with that fraud: where to go, how to report. I think there is a lack of support from the telecommunication companies in terms of providing guidance on the primary scams that are impacting their clients currently. I definitely think there could be a more collaborative approach in terms of their running those campaigns for their client base.

Mr. Brian Masse: That's where I'm looking for balance. There's an immense amount of wealth being generated from consumers on this, an immense amount of money going to organized crime or fraudsters, whether it be petty or not, and there doesn't seem to be a proportionate response in dealing with this issue for the people who continue to be victims.

For the victims in your community, what supports are they provided? Is there any counselling? You have people who not only become victims—as Mr. Lawford mentioned, it's not a crime until you actually lose it—but also I know there are people who won't even go public about it. They feel shame. Their self-esteem is lost. They're embarrassed.

Do you know of any supports out there? I know our Windsor police and a few others try to do what they can, but there aren't any core services. Victims services are needed.

Ms. Kate Schroeder: What I've noticed in the cases we've been involved in is that it differs from province to province and territory to territory. It's very jurisdiction-based. I believe they have specific dedicated hotlines for people in Alberta and B. C.

However, I think there is a definite need for an overarching support system, a centralized support system for people. Based on the situations we've had, when we've reached out to police to report fraud, we've had varying degrees of success. We've had really great local detachments that have gone to see these clients, to help them, to provide guidance on what to do. We've also had the opposite, to be frank.

I definitely think we need a more robust, streamlined approach on what individuals can expect, what seniors can expect, in terms of what to do.

The process to report fraud at financial institutions is also very difficult. The forms are long and confusing to people, and there's not a lot of support there either.

There's a definite need for all of these people and all of these agencies to come together to provide better support.

● (1250)

Mr. Brian Masse: Mr. Baran-Chong, you mentioned the $100, but I guess your message is what we've heard from many other experts already, that prevention is the best strategy.

How would you rank the response and prevention in terms of when you've reached out on this? Where do you think you are along the road to gaining some of the things you noted here, which could prevent some of the things you were a victim of, in the coalition that you support?

Mr. Randall Baran-Chong: Other victims and I have offered our support to the telcos numerous times and have received nothing but silence so far.

If it's an industry that is truly service-oriented and talks about how its best interest is in how to serve and protect us, it isn't involving us at all. So far when they've tried to roll things out...without the fingerprints of the users themselves, it has clearly failed.

Mr. Brian Masse: You're putting some warning bells out there.

With regard to where we're headed now, where do you think the opportunity lies, if we do something now—I know it's calling for a prediction—in six months from now or a year from now? What do you think is going to happen if we ignore those warning bells from the people who have been taken in by fraud on this?

The Chair: You have five seconds

Mr. Randall Baran-Chong: As Senator Wyden in the United States has identified, this is just waiting to be a national security risk, with the takeover of officials' accounts, for example.

The Chair: Thank you.

I'm going to check with the committee on whether they would like to continue with the next round. We have some study business to approve.

Is it okay to go with the next round and then stay a bit past one o'clock, or would members like us to stop and deal with the committee business with respect to studies?

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): I'm okay with stopping.

The Chair: Okay.

Mr. Brian Masse: I have one last question if I could get it in.

The Chair: Unfortunately, you're completely out of time, Mr. Masse.

Mr. Brian Masse: Then I would like to continue with the witnesses since we have them here.

The Chair: Okay.

MP Gray.

Mrs. Tracy Gray: Sorry, Madam Chair, but I have another commitment so I won't be able to stay later.

Mr. Majid Jowhari: It's the same for me, Chair.

The Chair: We can go quickly. We can do maybe two and a half minutes for the next two rounds. Is that fair? Okay.

MP Dreeshen, go ahead for two and a half minutes.

Mr. Earl Dreeshen (Red Deer—Mountain View, CPC): Thank you very much.

First of all, Ms. Schroeder, from listening to the testimony that you presented, I think one of the things is that once a senior has been duped, no matter what the situation is, there's always that fear that the kids are going to say, “Well, you can't handle your money so we're going to have to look after it for you.” I really think there has to be more of a campaign, a “you are not to blame” campaign, because we can see this happening all around.

I think that's one of the things you were alluding to, but I'll just try to say it a little more bluntly. I really think that's something we should think about in our discussions.

Mr. Baran-Chong, you talked about various things that we can do, and as I mentioned before, with the seniors, I think investing in public education is worthwhile, so that those folks understand that.

You did have a section on this, the Canadian call to action. You've talked about how the CRTC doesn't seem to be interested, and you just mentioned how the telcos seem to be hiding their heads in the sand as well.

What would you suggest, in the next minute and 10 seconds, that would help us in that regard?

Mr. Randall Baran-Chong: I think it's worthwhile that there be further study into industries and how they're using authentication methods.

In particular, for example, a lot of banks still promote text-based two-factor authentication which, as we mentioned, we're really trying to move away from. We need to really encourage these industries that possess either financially or personally sensitive information to not only introduce these non-SMS-based two-factor authentication methods but also proactively encourage their customers to use them. A lot of these apps ask you for your phone number, and that's the first thing they come out with. You could maybe anticipate that it's because they want this extra data part of you, but we need to get the industry agencies to really promote non-SMS-based 2FA.

● (1255)

Mr. Earl Dreeshen: Thank you.

The Chair: Thank you very much.

The last two and a half minute question will go to Madam Lambropoulos.

Ms. Emmanuella Lambropoulos: Thank you.

I'd like to thank both Mr. Baran-Chong and Ms. Schroeder for being with us today to answer our questions. As most of my questions have been answered, I'm going to ask Ms. Schroeder a couple of more specific questions.

You were talking statistics before and you said that this year approximately 4,000 fraud cases have been committed in Canada. Were those specifically involving seniors or just generally?

Ms. Kate Schroeder: Do you mean for these specific statistics?

Ms. Emmanuella Lambropoulos: Were these seniors who were defrauded or the general population?

Ms. Kate Schroeder: Those were Canadians in general.

Ms. Emmanuella Lambropoulos: Do you know how much the senior population has been affected specifically?

Ms. Kate Schroeder: I don't have the statistic available at this particular moment, but I think the scary part of that is that, based on what we know, the reporting rates of fraud are extremely low.

Ms. Emmanuella Lambropoulos: Are the ones you have worked with specifically complaining mainly about cases they've received on an actual land line or on a cellphone? What's the more—

Ms. Kate Schroeder: I think it's a combination of both. There are a lot of land lines still, but I do think it is still cellphone based and then.... Yes, it's both, certainly.

Ms. Emmanuella Lambropoulos: Thank you.

Mr. Baran-Chong, you said something that struck me. You said that cellphone companies are often open, especially for the business accounts, from 8 a.m. to 4 p.m., and this is a 24-hour war that these people are fighting.

What are your specific recommendations with regard to this that would help people in your situation in the future?

Mr. Randall Baran-Chong: After that incident happened with my cellphone, I was able to reach Visa immediately. They have a 24-hour hotline to report fraud. Why is it not the same for the telco companies? I even tried calling the consumer line, which is 24 hours but they don't have access to my business information.

If you possess financially or personally sensitive information, you should have some form of access to a 24-hour hotline to report that and to block that so it can't go further.

Ms. Emmanuella Lambropoulos: Is there any time left?

The Chair: Ten seconds.

Mr. Brian Masse: On a point of order, Madam Chair.

I don't want to be disruptive, but the schedule we have says we meet until one o'clock. I have one short question to ask the witness. I would ask for your indulgence, or unanimous consent, to ask that question. It's a simple one, and then we can move on. I would appreciate that.

The Chair: Is there unanimous consent?

Some hon. members: Agreed.

The Chair: Proceed, Mr. Masse.

Mr. Brian Masse: Thank you very much, Madam Chair.

Very quickly, with regard to the CRTC study, how important do you think it is that it be done right away?

Mr. Randall Baran-Chong: As long as the door is open, there will be more victims. The CRTC needs to get the plan from the telcos. It needs to understand how it plans to implement it. It needs to enforce the execution of it. It should involve the public, the users, and the people who are facing these threats.

The Chair: With that, I'd like to thank the witnesses for sharing their stories and educating us on the realities that are facing Canadians today.

I'd like to ask the members to stay momentarily. We need to have a quick review of the three study budgets, including the one on Bill C-4, which has already been concluded, so that we can reimburse witnesses for some of their expenses.

I will let the clerk explain the documentation in front of you with respect to the three study budgets.

The Clerk of the Committee (Mr. Michael MacPherson): I really don't have much else to add. These are all mainly estimates based on aggregate witness expenses, and any money not spent is clawed back.

Mr. Brian Masse: I would move the three budgets together in one motion.

(Motion agreed to)

The Chair: Thank you.

The meeting is adjourned.