HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

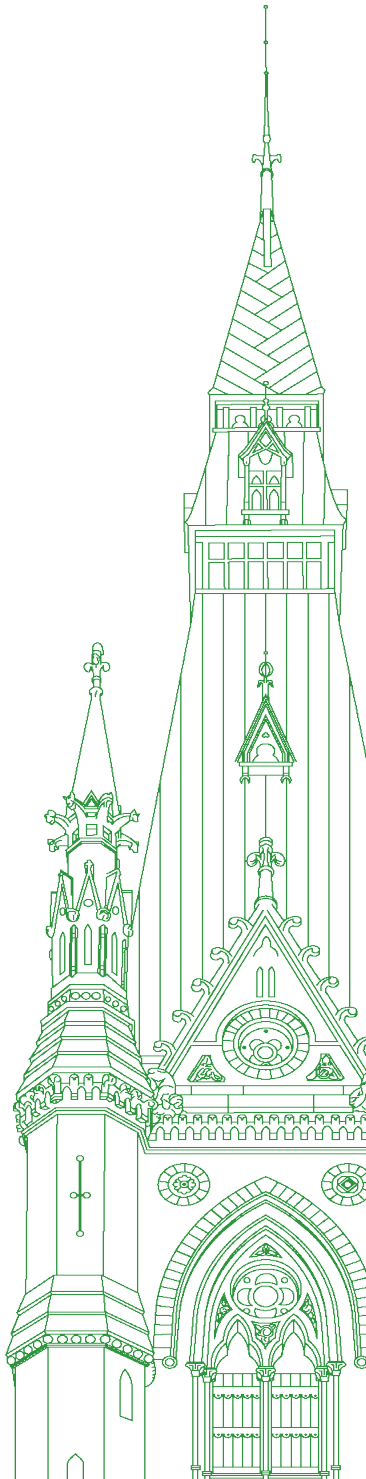
43rd PARLIAMENT, 1st SESSION

Standing Committee on Industry, Science and Technology

EVIDENCE

NUMBER 007

Tuesday, March 10, 2020



Chair: Mrs. Sherry Romanado

Standing Committee on Industry, Science and Technology

Tuesday, March 10, 2020

● (1100)

[*English*]

The Chair (Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Good morning, everyone. Welcome to the Standing Committee on Industry, Science and Technology. We have a tight schedule this morning.

Today we will be having our first panel on fraud calls in Canada.

Before us we have representatives from the Canadian Radio-television and Telecommunications Commission. We have Ian Scott, chairperson and chief executive officer; Steven Harroun, chief compliance and enforcement officer; and Alain Garneau, director, telecommunications enforcement, compliance and enforcement sector. From the RCMP, we have Eric Slinn, assistant commissioner, federal policing criminal operations; Guy Paul Larocque, acting inspector, Canadian Anti-Fraud Centre.

Gentlemen, each witness group will have 10 minutes to present, after which we will go to a series of questions. You can present in either of the official languages. If you see me waving the little yellow card, that means you have 30 seconds to wrap up. I will also remind folks in the audience there is absolutely no photo taking during committee, and I ask that you respect that. This meeting is being webcast live, so folks can follow from home.

With that, we will start with the CRTC. You have 10 minutes.

Mr. Ian Scott (Chairperson and Chief Executive Officer , Canadian Radio-television and Telecommunications Commission): Thank you, Madam Chair, for inviting us to appear before the committee, here on traditional unceded Algonquin territory.

[*Translation*]

My name is Ian Scott, and I am the chairperson and chief executive officer of the Canadian Radio-television and Telecommunications Commission, or CRTC for short.

[*English*]

You've already introduced my colleagues, so I will not repeat that in the interest of time.

[*Translation*]

We appreciate the opportunity to participate in the committee's study of fraudulent calls to Canadians, including robocalls and other types of unsolicited calls.

The CRTC's mandate includes helping Canadians reduce the number of unwanted telemarketing calls they receive. We do this by setting rules for telemarketers, overseeing the national do not call list, and conducting outreach and enforcement activities. While some unsolicited calls are fraudulent in nature, which is a matter outside the CRTC's mandate, we have a collective responsibility to protect Canadians.

[*English*]

We're pleased to be here today to share with you the steps we are taking to better protect Canadians. We recognize that these unsolicited calls impact everyone and are a scourge on our society. For some, however, particularly vulnerable people, they are an even more serious problem, because they often lead to criminal activity, such as fraud and identity theft.

Given the continuously evolving nature of the problem, addressing it requires broad and concerted co-operation and collaboration. To this end, we work closely with industry as well as our domestic and international partners to develop and implement solutions.

[*Translation*]

In 2008, the CRTC created the national do not call list, a tool that balances consumer concerns about unwanted calls with businesses' legitimate desire to communicate with existing and potential customers. It's important to recognize that striking and maintaining an appropriate balance between the two requires the participation of both consumers and telemarketers.

Since we started the national do not call list, more than 14 million numbers have been registered by Canadians who want telemarketers to respect their privacy. Last year, Canadians registered an average of 858 numbers each day—a sign that they have confidence in the list. In addition, more than 20,000 telemarketers have subscribed to the list.

We closely track and analyze complaints about unwanted calls—data that help to inform our outreach efforts and enforcement action. The CRTC regularly imposes monetary penalties on telemarketers and their clients who violate the rules and takes other enforcement action such as issuing warning letters, citations and notices of violation.

I'm pleased to report that the majority of legitimate businesses are following the rules. The challenge we currently face, as I'm sure the committee appreciates, is the illegitimate actors who are using the telephone system to take advantage of Canadians. These people often do not reside in Canada, have no interest in complying with the rules and are using technology to hide their identity.

● (1105)

[*English*]

To combat this problem, the CRTC required certain service providers to implement a system to block types of calls within their networks by the end of last year. Whenever the caller identification information exceeds 15 digits, or doesn't conform to a number that can be dialed, for example, all zeros, the call will not go through. These calls will be blocked before they ever ring on a subscriber's phone. Providers that offer their customers that call filtering service, which provides a more advanced call management feature, were exempted from this requirement.

While the call blocking system will help, it will obviously not stop all the illegitimate calls from getting through. For years, Canadians have used the caller ID function on their phones to identify and ignore unwanted calls. Now, however, some illegitimate actors use technologies that generate fake caller IDs, enabling them to conceal both their identities and intentions. This is often called caller ID spoofing.

I'm pleased to inform you there's a new weapon in the ongoing fight against ID spoofing. It's a framework known as STIR/SHAKEN. STIR is an acronym for secure telephone identity revisited, while SHAKEN stands for signature-based handling of asserted information using tokens. The CRTC expects Canadian telecommunications service providers to implement STIR/SHAKEN by September of this year.

The STIR/SHAKEN framework enables service providers to certify whether a caller's identity can be trusted by authenticating and verifying the caller ID information for Internet protocol-based calls. This new framework will enable Canadians to know, before they answer the phone, whether a call is legitimate or whether it should be treated with suspicion.

Last December, we joined forces with our American counterpart, the FCC, to hold the first official cross-border call using STIR/SHAKEN. This initiative highlighted the joint commitment of our two organizations to reduce unwanted calls and better protect consumers. The timely implementation of STIR/SHAKEN will enhance the security of citizens on both sides of the border.

We also continue to work with the Canadian telecommunications industry to develop a process to trace nuisance calls back to their points of origin in the network.

● (1110)

[*Translation*]

No organization, regardless of its size or power, can combat the negative impacts of illegitimate calls on its own. That is why the CRTC works with a number of federal departments and agencies, including the RCMP, the Canadian Anti-Fraud Centre, the Canada Revenue Agency, the Competition Bureau, Shared Services Canada, Employment and Social Development Canada and the Communications Security Establishment. An important purpose of this collaboration is to share relevant information with Canadians in a timely way to help them avoid becoming victims of fraud.

One challenge that I would like to raise is that we are currently limited in the information we can share with our domestic partners. Greater flexibility would enable a more coordinated response to this issue.

In this era of globalization, illegitimate calls are increasingly an international problem. We recognize the importance of developing a global and coordinated approach to address these calls, along with the threats that they pose to consumers and their confidence in critical communication systems.

To better protect Canadians from unwanted calls originating from outside our borders, the CRTC has signed memoranda of understanding with our counterparts in the United States, Japan, the United Kingdom, Australia and New Zealand. These arrangements allow us to share information and expertise, collaborate on education and training activities, and provide investigative support. Thanks to these activities, our investigators better understand the nature of the challenge and how best to meet it.

[*English*]

The CRTC also maintains partnerships with law enforcement agencies and private sector groups to enable effective enforcement, intelligence gathering and compliance promotion. For instance, as you'll see in our printed remarks, we are members of a number of international organizations. These networks help us to prevent international spam and telephony and encourage enforcement co-operation, and to address problems related to nuisance communications such as fraud and deception, phishing and the dissemination of viruses.

Canadians are rightfully proud of our systems. When these systems are abused by criminal elements, however, it erodes the confidence of Canadians.

The Chair: Mr. Scott, I'm sorry, but you're over your time. I'm sure, though, when we get into the rounds of questions you'll be able to finish your remarks.

Mr. Ian Scott: Thank you. We'll do our best to answer questions at that time.

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

Now we'll move to the RCMP.

A/Commr Eric Slinn: Thank you, Madam Chair. It's a pleasure to appear before this committee as part of its study on fraud calls in Canada, particularly given that we find ourselves in fraud awareness prevention month, in the month of March.

I'm Assistant Commissioner Eric Slinn, responsible for the federal policing criminal operations program.

Joining me today is Acting Inspector Guy Paul Larocque, who is in charge of the RCMP's program to combat mass marketing fraud.

As part of our mandate to protect Canada's economic integrity, financial crime, including fraud, has long been a federal policing priority for the RCMP.

[*Translation*]

The RCMP works with partners across Canada in both the public and the private sectors.

[*English*]

As well, we work with law enforcement agencies around the world to pursue fraud cases, as highlighted by our recent success in Project Octavia here in Ontario. This array of partners speaks to the shared responsibility of combatting fraud not only in Canada but around the world. This is truly a global challenge that requires a global response.

Technology facilitates an increasingly interconnected and borderless world that provides tremendous benefit to Canadians. However, criminals also benefit. They are quick to adapt to the evolving technological landscape and use this landscape to target Canadians.

No one is exempt from these fraud calls. By way of example, just two weeks ago I received three separate calls within an hour from fraudsters pretending to be the CRA advising I was subject to criminal charges and a warrant would be issued for my arrest. This was only on my RCMP-issued cellphone. A lot of fun was had by me that day.

Fraud operations are so pervasive and profitable that relying solely on enforcement is an insufficient response to the scope of this criminal activity.

● (1115)

[*Translation*]

The Canadian Association of Chiefs of Police has made it clear through its organized crime committee that prevention forms a crucial component of the fight against fraud, and we agree.

[*English*]

On the topic of prevention, the RCMP continues to invest in this area. We've undertaken a number of local and national projects and initiatives that focus on prevention.

For example, in response to reports from the public and businesses on gift card scams, RCMP officers in Alberta took the initiative to create a fraud tip sheet, which they distributed to local businesses. A clerk in one store referenced the tip sheet and intervened to prevent an elderly individual from purchasing 50,000 dollars' worth of gift cards. These fraud tip sheets are being distributed to detachments throughout the province of Alberta.

Also in Alberta, officers created posters warning the public about Bitcoin fraud and placed them next to Bitcoin ATMs. RCMP federal policing is now working to expand this initiative to make it accessible across the country.

Nationally, the RCMP has operated the Canadian Anti-Fraud Centre in partnership with the Competition Bureau of Canada and the Ontario Provincial Police since 2009.

The CAFC acts as Canada's central repository for information on mass marketing fraud and other scams impacting Canadians. In recognition of the significant impact and collective role of this, the CAFC disseminates information to law enforcement agencies, private industry and the Canadian public to raise awareness and prevent Canadians and businesses from falling victim to these scams.

The CAFC invests in fraud awareness campaigns, drawing the public's attention to high-profile scams, such as the CRA scam, through a variety of mechanisms, including social media.

[*Translation*]

Beyond prevention, the CAFC, in conjunction with private sector partners, targets the tools of scammers.

[*English*]

When individuals who suspect a scam or who have fallen victim to fraudsters report to the CAFC, the information they provide, telephone numbers, for example, is shared with the appropriate service provider, who can then terminate accounts by these scammers. Similarly, email addresses, bank accounts and merchant information are also shared with the appropriate partners to alert them to fraudulent activities within their own network.

While some victims have indicated that it can be difficult to reach the CAFC by phone, it's important for the public to continue to report, using online tools. Public reporting provides valuable information to the CAFC, but there is also the potential for victims to recover money lost. The CAFC works with such partners as Canada Post to intercept packages, or with banks to prevent money being sent to accounts linked with fraudulent activity, and sometimes to return the cash to those victims.

Under the federal policing priority of transnational and serious organized crime, the RCMP has a mandate to investigate criminal activity, including financial crime that crosses international borders and is carried out by criminal organizations who target Canadians. Under this mandate, the RCMP conducted an investigation recently into the CRA scam called Project Octavia.

Project Octavia commenced in October 2018. It investigated a telemarketing tax scam, better known as the CRA scam, which I'm sure many of you have heard about. In February 2020 the RCMP investigators arrested and charged two people in connection with the CRA scam. Between 2014 and 2019 the CRA scam resulted in cumulative losses, that we know of, totalling over $16.8 million.

Highlighting the complex, borderless nature of modern-day fraud investigations, RCMP investigators, including the RCMP liaison officer in New Delhi, India, worked with law enforcement agencies across Canada; other federal agency partners, including the CRA, Canada Border Services Agency and FINTRAC; and foreign authorities, including the Indian Central Bureau of Investigation and U.S. authorities based in India.

Long-running international cases like Project Octavia are indicative of the challenges the RCMP continues to encounter when investigating fraud. Criminals hide behind technology and international jurisdictions to perpetrate their crimes in Canada. However, where there is a challenge there is always an opportunity. Part of the success of Project Octavia can be attributed to the public awareness campaign undertaken by the RCMP through the CAFC. Since 2015 the CAFC and CRA have released numerous bulletins and public relations documents to inform Canadians of this scam.

● (1120)

[*Translation*]

You may have noticed that I've spoken at length about the CAFC. It is a best practice initiative that provides a valuable service both to law enforcement and to the Canadian public.

[*English*]

However, the CAFC is overwhelmed given the growth in phone scams and other frauds and the inundation of calls and emails it receives every day. As an international best practice and an effective proven model in the fight against fraud, the CAFC and its dedicated team of paid and volunteer staff provide a valuable service to Canadians, particularly such vulnerable populations as seniors and new immigrants.

Telcos have worked with us and taken specific actions to aid Canadians by blocking fraudulent calls from numbers they know are associated with suspected fraudulent activity. Both telcos and ISPs rely, at least in part, on information they receive from the Canadian Anti-Fraud Centre. In turn, the CAFC is only as good as the information it receives from Canadians reporting frauds and scams.

Through Project Chameleon, financial institutions in Canada are working with the RCMP to identify perpetrators of romance fraud and to contact victims to protect their money. This is not to forget our international law enforcement partners, such as the Five Eyes law enforcement group. FELEG members have collectively undertaken work focused on vulnerable populations. These groups are not always comfortable contacting law enforcement, as we know, and are often specifically targeted by scams. Further work and international public and private sector partnerships along these lines could prove invaluable in combatting such frauds as the CRA scam, and offers an opportunity to gain further insight into the methods fraudsters use to bilk Canadians of their hard-earned money.

In conclusion, fraud impacts Canadians in a variety of ways: financial loss; potential loss of property or the ability to gain credit; and, most seriously, a loss of trust in the institutions that make Canada such a desirable place to live. I have highlighted that combatting fraud is a shared responsibility. It is one that we will not shy away from. The RCMP will continue to work with the public and private sectors and our international law enforcement partners to detect, investigate and prevent fraud to better ensure the safety and security of Canada and its citizens.

[*Translation*]

I thank the committee for the opportunity to stand before you and welcome the chance to answer any questions you may have.

[*English*]

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

We will start with our first round of six-minute questions.

The first group of questions comes from Mrs. Tracy Gray.

The time is all yours.

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

Thank you, witnesses, for being here today.

The statistics provided by the CRTC website on enforcement, between 2018 and 2019, on calls to numbers on the do-not-call list, state that only about 500 cases of enforcement were undertaken, such as citations or warning letters. They also state that the CRTC has received over 84,000 complaints in the same time period.

Can you elaborate on why there is such a large discrepancy between the complaints and the enforcement actions?

Mr. Ian Scott: I can begin, and my colleagues may wish to add.

From the outset, it's important to point out the approach that we take on these enforcement matters. It is first about consumer education and the education of those participating in the telemarketing industry, to incentivize the correct behaviour. Our focus isn't on pursuing every single small case, whether or not by using AMPs as penalties; rather, it's a broader approach, to educate and incentivize proper behaviour.

AMPs aren't meant to be a punishment. They're meant to be an incentive to comply with the law. That's the simple explanation for those. What we do is pursue those who grievously offend the rules and who do not comply.

I don't know if my colleagues want to add to that.

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): I'll just add one comment to that, to your volume question.

The 84,000 complaints are not validated complaints. That's what comes in to the national do-not-call list operator, and they say, “Here are your complaints for this year.” We get them on a weekly basis nonetheless.

Those have to be validated and sliced and diced. There may be hundreds if not thousands of complaints about the same campaign. We also have to stay within our mandate. For example, a lot of those complaints may be related to a charity that has called. Well, a charity is actually allowed to call you. They're exempt from the rules. There are those types of things. They may also be strictly fraud related, which would be for our colleagues at the RCMP to tackle.

Five hundred cases do take time. We want to make sure, if we are going after a particular target, that they are the correct individuals.

● (1125)

Mrs. Tracy Gray: Thank you. My time is limited here, so I'd like to go into something else, if I may.

The CRTC states in its report on its website that there have been 2,067 purchases of the do-not-call list by telemarketers. The information in the briefing note you handed us today said that there are 20,000 telemarketers who subscribe to the list. First, what is the difference between someone purchasing and a subscriber?

The second question concerns a survey that was prepared by the CRTC in 2016 which revealed that only 10% of registered telemarketers subscribed to the DNC list. This shows that most are either not aware of their obligations or are not fulfilling them. Is this mandatory, and how are you enforcing these rules?

Mr. Alain Garneau (Director, Telecommunications Enforcement, Compliance and Enforcement Sector, Canadian Radio-television and Telecommunications Commission): I can answer this question.

Just to clarify the distinction between registration and subscription, registration is free, and there is a clear obligation for each telemarketer or client of a telemarketer to register with the DNCL operator, which is Raymond Chabot Grant Thornton LLP.

Basically, a subscription means downloading the list, paying to access the do-not-call list. You can access the valid phone numbers of people who have made a clear choice not to be contacted, and you can access it by downloading the list. You need, first, to be registered, and then you pay for the subscription.

That is the main distinction between the two.

I don't know if it answers your question.

Mrs. Tracy Gray: Well, it answers the first part, but the second part is that, if it's mandatory, why did the report you put out in 2016 say that only 10% of people are participating in it? It seems there is a big gap.

Mr. Alain Garneau: No, I don't think there is a big gap. I think what we mentioned in the report is that since the inception of the do-not-call list, the proportion of telemarketers who are registered with DNCL is just going up. At the moment there are roughly 20,000 telemarketers or clients of telemarketers registered with the DNCL.

Mrs. Tracy Gray: Okay.

I hear from people who say they've registered and yet they're still getting calls. There seems to be a gap.

Mr. Ian Scott: Most of those, the significant percentage, are because consumers don't understand the exceptions. That comes up during election cycles, for example, when they are being contacted by political parties, by charities and so on, or by pre-existing customer relationships. Many Canadians don't understand that it's not a carte blanche there will be no calls.

Mrs. Tracy Gray: Okay.

Mr. Scott mentioned spoofing. A number of spoofing websites are available online that are accessible to anyone. Many of them market themselves as prank sites. I'm wondering if the RCMP is aware of these sites, and if you think there is a prevalent problem.

What actions are being taken against these sites?

The Chair: You have 10 seconds to answer.

A/Commr Eric Slinn: Ten seconds.

We are always trying to keep up with different models, different intelligence, how people are working. It's hard to keep up.

The Chair: Thank you very much. That is your time.

The next round of six-minute questions goes to Helena Jaczek.

Ms. Helena Jaczek (Markham—Stouffville, Lib.): Thank you very much.

Witnesses, thank you so much for coming in.

My questions are going to relate mostly to the CRTC. A lot of them are being asked on behalf of my very elderly spouse who is incredibly frustrated with the nuisance calls that are clearly fraudulent in nature.

He is certainly able to use the Internet, and his first complaint is that he looked at the CRTC website and found it incredibly hard to navigate. In other words it is not a telemarketer call and he has not been subject to fraud, but he wants to tell you about a call he's received and what the number on the call display has shown. He wants to simply tell somebody about it because he doesn't want someone to be scammed in the future.

Have you looked at trying to simplify your directions?

I know you mentioned 84,000 complaints and that many relate to legitimate organizations.

Have you looked at in some way clarifying this for vulnerable seniors who wish to do their duty and report to you, but frankly give up trying to navigate your web page?

● (1130)

Mr. Ian Scott: That's a very fair question.

In a second I'm going to ask my colleagues to answer about the improvements.

The challenge is it's not easy to explain. There isn't a single button because we want them to add information when reporting to us because the more information we get, the better the information we share with enforcement and other colleagues. It's this balance between having a button that says to forward an email as opposed to adding additional levels of detail that will give us more information in the process of intelligence gathering.

I acknowledge it's probably not the simplest thing to navigate through sites. Part of it is also Government of Canada format requirements, accessibility requirements and the like. We don't have total flexibility in what we can do with our site.

Steven, do you want to add on the information itself?

Mr. Steven Harroun: Absolutely.

Definitely, keeping our websites up to date is a constant battle. We certainly have taken measures on the anti-spam side, which is my wheelhouse, as well as the email side. We're revamping our telemarketing website as well so if someone types in "telemarketing call" it will pop up to a page where all the relevant information will be.

The one thing I would tell your husband and all your constituents is that you can always call the client services number on the front page of the CRTC website.They will direct you to the DNCL operator whom you can make your complaint to. We have a really cracker jack client services team. They will make sure you get to the right place.

Ms. Helena Jaczek: Okay. I'll make sure he knows about that number.

In your presentation, Mr. Slinn, you talked about STIR/SHAKEN. I think we're all aware that there has been a delay. A delay was requested. Originally I think it was supposed to be instituted in March 2019, and now it's September 2020. From some materials I've received, I understand that some of the telecoms want to delay further.

Could you explain the delay?

Mr. Ian Scott: I don't think it's a question of their wanting to delay. It's a question of getting the systems completely interoperable and working.

Even in the United States, and we are in a fast follow mode, the United States had an edict. The FCC said they had to be in place by the end of last year. By and large they have been put in place but they are not fully operational. They are still working to perfect the system. At the moment we have a deadline of September of this year. We have not extended that. We expect the carriers will meet that but we have to be open and understand there may be technical challenges. If there are, they will present them to us and only if necessary add additional time.

Ms. Helena Jaczek: Just so I'm clear on how it will actually work, you said in your remarks, "This new framework will enable Canadians to know, before they answer the phone, whether a call is legitimate or whether it should be treated with suspicion."

How will they know? What will appear on the call display?

Mr. Ian Scott: That's one of the things that's still being worked out. There are a number of possibilities that you can imagine. It could be a check mark. It could be a check mark accompanied by an audible sound. Think of a green light and a yellow light. The green light would mean it's authenticated. The yellow light would indicate that you should approach the call with care. Or a red light that says—

Ms. Helena Jaczek: How about "do not answer"?

Voices: Oh, oh!

Mr. Ian Scott: Hopefully, we would have screened out something that was clearly fraudulent, and the carriers will, but we also have to take into account accessibility issues. We have to deal with sight-impaired and hearing-impaired individuals.

Ms. Helena Jaczek: Also, we know that in 2015 the CRTC initiated proceedings on this whole topic and some stakeholders—we have this from our library researchers—argued that telecom companies should have the responsibility to manage nuisance calls since they have the greatest insight and technical ability to do so.

Since then, from the perspective of our household, certainly things have increased dramatically. Could you explain how the telecoms have been involved?

● (1135)

Mr. Ian Scott: Look, this is a co-operation. We are setting expectations. The carriers are trying to deliver on them. We both have the same objective. It is not in the interest of service providers to have their customers annoyed at the calls, and it's certainly not in our interest. We're trying to protect the public interest. We are working together, and it is co-operative, not combative.

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

[*Translation*]

Mr. Lemire, you may go ahead.

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

To start, I just want to point out that one of the benefits of being a francophone in this country is that, when you get a fraudulent call and you don't recognize the number, your initial reaction is to hang up when the person on the other end of the line talks to you in English. That doesn't mean it's not a problem. I imagine there are statistics.

Mr. Ian Scott: That's not a solution, in our eyes.

Mr. Sébastien Lemire: I agree, but I just wanted to throw out the observation.

I want to thank Mr. Masse for raising the issue. It's a serious concern for seniors, and it's absolutely shameful. I am glad credible organizations like yours are tackling the matter.

My questions are for the RCMP officials. In your presentation, you didn't talk about the use of IP technology by fraudsters. Do we understand how it works? What are their tactics? Do they use the technology, and if so, how can we combat it?

[*English*]

A/Commr Eric Slinn: I'm maybe going to put it over to my colleague, Guy Paul, who lives that every day. He can provide that.

Mr. Guy Paul Larocque (Acting Inspector, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police): Of course, as was mentioned earlier by Assistant Commissioner Slinn in his elocution, scammers or fraudsters are always using opportunities to achieve their means. That's one thing they will do, and not just in using regular phone technologies, but also in abusing the IP technologies to commit their fraud and hide behind the technologies to actually avoid being detected. They like to create layers. They'll use technology to that effect.

[*Translation*]

Mr. Sébastien Lemire: Is there anything tangible we can do up front to combat the way scammers operate? Are Canada's systems sophisticated enough to detect their use of IP technology?

Mr. Guy Paul Larocque: That's more of a technical question, so I can't say a whole lot about getting ahead of the technology on that level. We do, however, know that one of the best ways to fight fraud is to keep people informed of the latest tactics in use to prevent more people from falling victim to scammers. The more aware people are and the more able they are to recognize scams, the better equipped they will be to deal with the threat.

Mr. Sébastien Lemire: I completely agree, and I want to highlight your efforts on that front.

My next questions are for the CRTC officials.

The CRTC's procedures apply in large part to big providers, but small providers in the regions can't necessarily afford to put in place the technology needed to create an effective firewall. That concerns me.

Do you consult small providers? Do you reach out to them for their expertise and knowledge? What part do they play in the fight against scams?

Mr. Ian Scott: Thank you for your question, Mr. Lemire.

I'm going to let Mr. Garneau answer that.

Mr. Alain Garneau: All telephone and voice messaging service providers are invited to take part in the process. Whenever we put out a notice of consultation, they are informed.

The costs associated with upgrading the network can definitely be a challenge. However, should the industry have the resources to bring small providers together, or will some providers depend on a large provider on the back end? It shouldn't necessarily be a barrier if the company is small. There are benefits in moving from time division multiplexing to the IP network. It's possible to save money by doing so.

I'd like to answer your question about the technology and the approach, if I may. Telephony over IP relies on broadband Internet. It's easy for a teenager sitting in a basement somewhere in India to connect to the Internet, obtain a dialling device online and use it to make millions of phone calls.

The return on investment is so appealing that, even if they reach only one per cent of their target, getting one person to fall for the scam is extremely advantageous.

● (1140)

Mr. Sébastien Lemire: That's what worries me about IP technology.

Mr. Scott, you also mentioned in your presentation that you wanted more flexibility to better respond. What type of flexibility are you looking for? Is it something we, as parliamentarians, need to provide?

Mr. Ian Scott: It may be necessary to allow for the pooling and sharing of information that federal agencies have.

Mr. Alain Garneau: I'd like to add something, if I may.

Mr. Scott mentioned at the beginning that having an explicit information-sharing provision in the legislation would be beneficial. As parliamentarians, you would need to give the CRTC specific direction.

If we had the freedom we needed to share information with other law enforcement agencies, or government bodies, it would be a good thing.

The Chair: Thank you.

[*English*]

The next round of questions is from MP Masse.

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

Thank you to the committee and to our guests.

I'd like to raise the next point with regard to enabling legislation. Can it be done through regulation to allow the CRTC to share with more agencies like the Competition Bureau and others?

Mr. Ian Scott: Thank you. We need to be more crisp in our responses.

No, it needs to be done through legislation.

Mr. Brian Masse: Okay.

Mr. Ian Scott: We can't regulate—

Mr. Brian Masse: We had this discussion on the do-not-call issue when we first did this.

I want to get a clarification in terms of the culture that you're dealing with.

The way that I view it, Canadians are equally frustrated about phones and landlines in that they pay a lot of money for this. For the phones, the government has received over $20 billion in assets from the spectrum auction from the telcos over that time. They've also paid some of the highest prices, and they're still bothered by a lot of this activity.

Do you differentiate between somebody who uses the do-not-call list for unsolicited calling—sometimes they can be given AMPs for that—versus that of the CRA fraud scam or somebody internationally? I view all those activities as the same type of fraudulent activity because they are not even following a rule that's supposed to be in place for Canada or they're using activity that is unscrupulous with regard to trying to solicit them.

Do you distinguish between any of those types of activities that take place?

Mr. Ian Scott: We do in particular because some of them are criminal, and we don't prosecute or pursue criminal matters. We share that with our enforcement colleagues and pass those off.

You're right that all of these offences are equally problematic. I wouldn't say equally; the fraudulent activities are worse.

Mr. Brian Masse: I get your point.

Mr. Ian Scott: It's also, if you wish, a spectrum.

A decade ago we were focused on spam emails, phony emails.

Mr. Brian Masse: Yes.

Mr. Ian Scott: The systems are now working to reduce that.

Today, the focus is on spoofing, and it's growing, not just in calls, but on texts. These things evolve, and we have to pursue all of them. The real distinction, to answer your question, is criminal versus civil.

Mr. Brian Masse: I have a little bit of concern with the low level of AMPs that you have from last year. The largest one was $90,000. It doesn't seem much of a dissuasion to the businesses that get caught.

For instance, if a business that goes through your program and goes through the process gets caught, and you register an AMP on it, is there a screen to see telcos' relationship with this with regard to their activity and if there's any connection to whether they were co-operative in the process to try to block some of this? Perhaps they should have been more attentive than they demonstrated.

Mr. Ian Scott: Mr. Harroun is responsible for enforcement, so I'll ask him to add something.

Obviously, we would investigate thoroughly. That's not usually the case. Usually, it's a telemarketer that's not following the rules.

Steven, do you have something to add?

● (1145)

Mr. Steven Harroun: I can't really answer your telco question or make the connection there. On the AMP side and the investigations that we make, it's important to note that under our civil regime, administrative monetary penalties are to promote compliance versus to be punitive. That is very clear in the direction we have to follow under the legislation.

We promote compliance through a significant amount of administrative monetary penalties to the Crown. We also ask them to put in place compliance programs and we do follow-up audits, etc. It's to ensure that the inappropriate activities of the telemarketer don't continue.

Mr. Brian Masse: I'm going to give a little time to Commissioner Slinn. It's too bad because I still have questions on STIR/SHAKEN and so forth.

Commissioner, I noticed you have a lot of different programs out there, but they seem to be kind of scattered or project-based. Are there supports that could be provided to do more of a pan-Canada type of thing? You mentioned a series of really good initiatives in Alberta. I know that in Ontario they did some really good work.

Are there the appropriate resources to be able to do a more robust cross-Canada approach to this?

A/Commr Eric Slinn: I think there's a recognition out there that in the Canadian law enforcement community writ large—not just the RCMP because one has to remember we're not the police of jurisdiction in many spots in Ontario—we need to do more in the space of fraud. We need to be more coordinated.

Through the organized crime committee of the Canadian Association of Chiefs of Police we are looking at ways to share best practices and to get more engagement of law enforcement around fraud than there has been. That all revolves around the whole cybercriminality. We're used to working in a model that doesn't work in that cyber area.

Policing is changing dramatically, but I think through the Canadian Association of Chiefs of Police there is a greater willingness to do more collaboratively there.

Mr. Brian Masse: A lot of the time, economic models put this amount in and they get this in return. You gave an example of $16.8 million in proceeds that you know of from one crime activity. There's all the stuff you don't know of.

If there were more resources and if it were taken—I don't want to say more seriously because I don't want to say it's less serious.... Maybe there's a more organized approach to dealing with this that actually has a specific, defined strategy. Do you think we'd make our money back by stopping other criminal activity from taking place?

A/Commr Eric Slinn: Resources are always an issue. We're actually looking at technology and how we can use big data analytics to hone in more to make a greater impact on those specific groups that are having the greatest impact. Lots of people are doing this, but who are those key facilitators or enablers that we can whack through criminal disruption?

Mr. Brian Masse: I have a last question for the CRTC. Is there a penalty for not putting STIR/SHAKEN in place?

The Chair: Mr. Masse, I'm sorry, but that's your time.

We will move now to the next round of questions of five minutes. My colleagues have a strategy of not looking at me so they can't see the yellow card. I know my witnesses are seeing it. This means wrap it up because you have 30 seconds left to respond.

The next five-minute question goes to MP Patzer.

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

Since we're considering fraud calls, I also wanted to raise another means of fraud that can come to people through their mobile phones. You referenced it in your last statement, Mr. Scott. A lot of people, especially younger Canadians, increasingly communicate through online social media and text messaging. I have a family member who was a victim of fraud through Facebook, as well. They accessed bank information and withdrew funds. Fortunately, we got that back.

As a result, scammers are shifting to text-based and online methods. Out of the tens of millions of dollars that are being lost to fraud every year, I'm wondering what share of that is being lost to text or online messaging fraud.

Mr. Ian Scott: I don't know that we have data on the share of those losses. You're absolutely right that the pattern.... Calls are only part of the problem now. Texts are increasingly a problem. They're used very cleverly, frankly, by bad actors. You get a text from your bank saying that they need an instant response.

First, you need to understand that texts fall under CASL, the anti-spam legislation. The processes we follow will be very similar. STIR/SHAKEN and other technologies like this will be used. At the end of the day, if it's fraudulent, we collect the information through our intelligence gathering group. We share it with law enforcement and other partners and, if it's fraudulent, law enforcement will go after them.

I hope that answered your question.

● (1150)

Mr. Jeremy Patzer: Yes.

A/Commr Eric Slinn: I can shed some light for you really quickly, in a 15-second response.

From what we're seeing through the Canadian Anti-Fraud Centre in 2019, it's roughly $25 million from telephone fraud and $54 million from Internet, so double. We're seeing more activity in online frauds than the phone calls saying, “There's a warrant for your arrest. Come on down.”

Mr. Jeremy Patzer: Right. Building on that, then, is there actual data that suggests fraud messages are occurring as much as or more than phone call situations?

Mr. Ian Scott: I will give you some frightening numbers. The U.S. follows this closely—there are a number of commercial firms. There were 100 billion calls in the last two years. For February of this year, the latest data says that 4.8 billion calls were placed in the United States. Of those, 43% were fraudulent. Those 4.8 billion robocalls equate to 1,900 per second. It's 43% of those, so it's something in the order of 1,000 a second. That's the kind of volume of problem we're confronting.

Mr. Jeremy Patzer: Seeing the number of Canadians who are receiving these spam or text messages, then, and who have reported losing money as a result, how can we work with Canada's major telecom companies to prevent these messages from being sent to Canadians?

In fact, we have an example of one just being received by one of the members of the committee here right now.

Mr. Ian Scott: I receive them and my mother receives them. I have my own special complainant whom I have to pay special attention to.

As I mentioned earlier, the carriers have every incentive to work with us and for themselves in their own self-interest to solve this problem. They don't want unhappy customers.

What are we doing? I mentioned we have universal call blocking. They are implementing STIR/SHAKEN. They are working at our behest on a call trace approach. They are also working on customized approaches for their own customers. For example, a white list is something they're developing. Some of the companies are exploring how they could use algorithms or artificial intelligence to begin screening.

This is an ongoing problem, but as my colleagues from the RCMP mentioned earlier, it's fundamentally a technology problem and each time we close a door, somebody finds a new opening and comes up with a new approach. This will never go away. It's about controlling and dealing with the biggest problems.

Mr. Jeremy Patzer: For sure.

Innovations in artificial intelligence have allowed companies to develop screening services to filter out unwanted calls and problematic numbers. For example, Google has developed a screening service using AI technology.

Has the CRTC looked into using similar technology at a national scale to help reduce further calls? I kind of touched on that a bit here.

Mr. Ian Scott: We are exploring some of those things. We have an application for a trial using such an application of artificial intelligence in front of us right now.

The Chair: Thank you.

The last round of questions for five minutes starts with Madam Lambropoulos.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you.

I'd like to thank both the CRTC and the RCMP for being here to answer our questions. I'll try to be as brief as possible.

I've had quite a few constituents of mine complain to my office about the fraud that they've fallen victim to. Some of them have lost all of their retirement savings and are in debt at this point because of these calls. When they come, they've completely lost all hope because they've already gone to the police, and the police have basically told them there's nothing they can do.

Could you maybe give us some insight as to what process is actually gone through once people have made a complaint and whether it's possible ever to identify where these calls are actually being made from, whether they're international? Do we find the location of these callers?

A/Commr Eric Slinn: Sure. First and foremost, again, law enforcement needs to do a better job. A lot of the times you're quite right in that they take a call from a complainant who's been victimized, lost some money. What they're hearing sometimes from law enforcement, RCMP included, is they should call the Canadian Anti-Fraud Centre. That's not the correct thing to do. That's one step to do. The Canadian Anti-Fraud Centre is not an investigative body. It collects intelligence, trends and so on.

When a complaint comes, what they should do is take the complaint, take as much information as possible and then work an investigation like any other investigation, working backwards, with ISPs, getting the phone numbers. Some police officers will say it's a difficult charge to prove because oftentimes these are call centres in India or elsewhere in the world. There are extradition challenges. All these are investigative challenges, but from an RCMP perspective where we are responsible for transnational organized crime, we do have the reach that we can do it.

We can't solve every complainant's victimization, but we can let them know that their complaint is important, it's received and we will do what we can. Sometimes it's merely the intelligence that we can take, and then we find out that it is a specific call centre, as Mr. David Common did in some great work on CBC once.

That's essentially what is supposed to happen, but improvements are needed within the broader law enforcement community in how we handle these complaints.

● (1155)

Mr. Ian Scott: I would add very briefly that we also, collectively, need to do a better job to prepare consumers to defend themselves, to educate consumers. You shouldn't be pressed to respond instantly. You should think carefully about why someone is asking you to respond or give your data instantly, and then think about other ways of going back to your bank or whomever to verify. Canadians need to protect themselves against fraud, and it behooves us to better prepare them to do so.

Ms. Emmanuella Lambropoulos: Of course, prevention is key, and that would be the best-case scenario, but in cases where it actually does happen, and obviously it happens quite often....

As you mentioned earlier, it happens more internationally; it's more of a global problem. You did mention that you're working with several countries around the world to help solve these issues. Is there opportunity for more collaboration with more countries so that when you do find out that it's coming from a call centre in India, it's actually punishable, and the criminals can be charged?

A/Commr Eric Slinn: We do the best we can. We work with the Five Eyes Law Enforcement Group. We work quite well with U.S. agencies that have quite a broad reach. In the case of India, we have worked with the Indian authorities in a couple of cases. However, we're at their whim because the RCMP has no authority in a foreign country, so we have to work with them and encourage them that this is important to our citizens, encourage them to please take action on this. They have other priorities of their own, so it poses a significant challenge.

I think that, at the political level, we need pressure from government to government to say, “You're affecting our people.” The RCMP, the CRTC and others can do our best, but we can only work within our authorities, and we don't have authorities extraterritorially, with the exception of a few offences.

Ms. Emmanuella Lambropoulos: Thank you very much.

That's it for me, but I'm going to pass my time to my colleague, Ms. Dabrusin.

The Chair: You literally have 40 seconds.

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

I want to pick up on what Mr. Patzer was asking before about email scams and texting scams. In my community, that's where I actually see the most action.

You talked briefly about numbers. I'm almost out of time, so what I would ask is whether there is any information you can provide—maybe links to your websites—about what you're doing to inform Canadians and how we can better inform Canadians to protect themselves from those scams because that's where I see the most activity when I talk to people.

A/Commr Eric Slinn: The CAFC is probably your best resource. We update on new scams and what can be done. There are senior support people to call back. The CAFC is one, and the other would be the RCMP site. However, CAFC is where people should go for information.

Ms. Julie Dabrusin: If you could actually send it to the committee if there is—

A/Commr Eric Slinn: I will do that.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you very much.

Unfortunately, that's all the time we have for this panel.

I would like to thank all of you for being here.

With that, we will suspend momentarily to allow the next panel to arrive.

Thank you.

● (1155)

(Pause)

● (1205)

The Chair: I would like to welcome you back for the second panel at the Standing Committee on Industry, Science and Technology

[*Translation*]

as part of our study on fraud calls in Canada.

Joining us now from Bell Canada, we have Jonathan Daniels, vice-president of regulatory law, and from Rogers Communications, Howard Slawner, vice-president of regulatory affairs, and Deborah Evans, chief privacy officer.

From TELUS communications, we have Jérôme Birot, vice-president of development operations, and John MacKenzie, director of regulatory affairs.

[*English*]

Ladies and gentlemen, because we have three groups with us today, we'll ask that your presentation be eight minutes in length, and at that point we will be going to the round of questions.

[*Translation*]

When you see the yellow card, it means you have 30 seconds left to finish your presentation.

[*English*]

With that we will start with Bell Canada. Mr. Daniels, you have eight minutes.

Mr. Jonathan Daniels (Vice-President, Regulatory Law, Bell Canada): Good afternoon, Madam Chair.

My name is Jonathan Daniels. I am Bell Canada's vice-president of regulatory law.

It is my pleasure to be here today to share with you the steps we have taken and continue to take in an effort to combat nuisance and fraudulent calling. We are strong proponents of protecting Canadians against these types of calls.

Specifically, I will speak to the three issues you asked us to discuss in this invitation: the national do-not-call list; fraudulent and nuisance calls; and STIR/SHAKEN protocols.

To begin, I'd like to address the issue of the national do-not-call list. While we agree that the list is a good tool that can help reduce the number of telemarketing calls received by Canadians and we are glad to have the benefit of such a tool in Canada, this tool does have limitations. Specifically, the national do-not-call list is only effective if everyone adheres to it. Unfortunately, the vast majority of nuisance calls received by Canadians come from callers outside of Canada that do not adhere to the national do-not-call list. Thus, we have to continually come up with new ways to stop unwanted calls.

This brings me to the issue of the recent influx of nuisance and fraudulent calls being experienced by Canadians. It is important to note that there is a difference between nuisance calls and fraudulent calls. Nuisance calls are calls that you do not want to receive. These types of calls are generally trying to sell you a service, such as duct cleaning. They are a nuisance and likely unwanted, but they are not necessarily illegitimate or fraudulent. Fraudulent calls are much worse than nuisance calls, as they are specifically designed to defraud Canadians. For example, you may receive a call offering to fix your computer, which is really an attempt to install a virus and lock you out of your computer, leading to a ransom demand. Other scams relate to credit cards. I have lost count of the number of times I have received a call from the so-called Visa/Mastercard centre, not to mention the infamous CRA scam. These fraudsters are sophisticated and intelligent, and stopping them will not be easy.

The industry has been working with the CRTC on a number of fronts in order to reduce both nuisance and fraudulent calls. ln that regard, I am pleased to be sitting on a panel today with representatives from both Rogers and Telus. It is unusual for me to take the time to acknowledge two of my competitors, but in this area of trying to reduce fraudulent and nuisance calls, it is important to note that we and many other players have been working together. In fact, our experts meet at least weekly, and often multiple times a week, to discuss these important issues.

When we deliver a call to you, we often display the number that is calling you. That is called a calling line ID, or CLID. In December of last year, the CRTC ordered carriers to start blocking calls that had a calling line ID or CLID that did not look like a real number. We refer to these calls as non-conforming calls. For example, if a call comes in on our network and has a CLID that exceeds 15 digits or is all zeros, we will block that call. To be clear, a non-conforming call is not necessarily a nuisance or fraudulent call, but having a non-conforming CLID is a very good indicator that a call may be problematic. On our network, we are now blocking approximately 220 million calls a month.

Another initiative the CRTC is pursuing is STIR/SHAKEN, which is the third topic the committee specifically asked about. STIR/SHAKEN works by letting consumers know that they can trust the telephone number that is being displayed. In other words, with STIR/SHAKEN, you will be able to know that the calling line ID you see on your phone is actually the real number calling you.

The CRTC recently sought comments on a proposal to require all carriers to implement STIR/SHAKEN. We support such a proposal. We think that we and all other carriers should be required to provide STIR/SHAKEN. However, we see STIR/SHAKEN as a long-term solution, as there is a variety of issues that need to be addressed before the benefits of a STIR/SHAKEN framework can be realized. It is for this reason that we, along with most of the industry, proposed that the CRTC STIR/SHAKEN mandate be delayed until we get the rules of the regime figured out. A lot of work needs to be done, and we are ready to do that work, but the industry and the CRTC must take time to do that work properly or else the solution will be flawed.

Let me give you an example. I think this is really an important point about STIR/SHAKEN. It's a long-term solution rather than a quick fix. Most phones today cannot display STIR/SHAKEN. Think of your land line telephone at home. Where would you see a check mark on your phone to confirm that the calling line ID displayed is actually the real number calling you? In fact, even most cellphones are not capable of displaying STIR/SHAKEN, although that will change in the next few years.

● (1210)

While we believe a mandate should be contingent on first finalizing the technical details, Bell has still committed to launch STIR/SHAKEN on portions of our network this September, but just because we launch it doesn't mean most Canadian consumers will be able to use it. There are a number of requirements that must be met in order for STIR/SHAKEN to fulfill its potential.

STIR/SHAKEN has promise, and we are fully committed to implementing it, but it is far from the only answer and will not materially address the problem of nuisance or fraudulent calls in the short term. Let me turn to something that I think will make a big difference.

ln addition to initiatives directed by the CRTC, we at Bell are committed to trying to protect our customers from fraudulent calls. Although we cannot identify all fraudulent calls, we have developed modern technology that allows us to identify millions of calls as being fraudulent.

ln identifying those calls, we work closely with the Canadian Anti-Fraud Centre, an affiliate of the RCMP. However, even when we can definitively identify a call as fraudulent, we are not allowed to block that call without CRTC permission.

Thus last year we applied to the CRTC for permission to conduct a three-month trial process we had developed for identifying and blocking fraudulent calls. I believe that's what the chair was referring to when he mentioned that there's an application; that's from us.

We have not publicly disclosed the details of this process so that we do not provide fraudsters with a how-to manual on the best way to circumvent our proposed trial; however, we have provided the CRTC with the full details of the process, and we've also shared the details of this process with our competitors, public interest groups and individuals who signed a CRTC-approved non-disclosure agreement.

If granted permission, we anticipate that this process will block approximately 120 million fraudulent calls a month on our network. That is in addition to the 220 million calls we're already blocking as a result of non-conforming calls. We suspect, however, that most of the 220 million non-conforming calls currently blocked are nuisance calls rather than fraudulent calls.

Our proposed trial will only block fraudulent calls in an attempt to protect Canadians from bad actors trying to illegally defraud them. We look forward to launching our trial as soon as we receive CRTC approval.

Fraudulent calls and nuisance calls are a pressing and growing concern for Canadians. We at Bell are fully committed to addressing this issue, including by asking the CRTC for permission to implement our new proposal to actively block these fraud calls. However, there is no one solution. We will continue to work with the CRTC, our competitors and our consumer groups to find new and innovative solutions to address this issue.

With that I will conclude.

Thank you.

The Chair: Thank you very much.

I'll just ask folks to every once in a while look up so they can see me waving at them.

The next group will be Rogers Communications.

Mr. Howard Slawner (Vice-President, Regulatory Telecommunications, Rogers Communications Inc.): Madam Chair, good afternoon. I'm Howard Slawner, vice-president, regulatory telecom at Rogers Communications. I am joined here today by my colleague Deborah Evans, Rogers' chief privacy officer. We appreciate this opportunity to appear before the committee and to provide input into the study of fraud calls in Canada.

Rogers fully supports the efforts of the Government of Canada and the CRTC to address the problem of nuisance and fraudulent calls. At best, these calls interrupt the peace and privacy of Canadians. At worst, they constitute crimes, often preying on the most vulnerable. Together these calls undermine the integrity of our national telecom system.

The unsolicited telecommunications rules, including the requirement to register with the national do-not-call list operator, have become well-established practices within the legitimate Canadian telemarketing community. In the 10 years that have passed since the introduction of the national DNCL, over 18,000 telemarketers and their clients have registered with the operator, respecting the privacy of the more than 13 million Canadian telephone numbers that have been enrolled.

There is, however, an important distinction between nuisance calls and fraudulent calls. Many nuisance calls are placed by legitimate parties, including not-for-profit and commercial organizations. While we can appreciate the frustration of Canadian consumers resulting from some of these types of calls, it's the growth in fraudulent calls that drives most concerns today.

The parties placing spam, fraudulent and blatantly spoof calls are aggressive and unrelenting, despite the established rules in place to protect consumers. Since they operate without fear of retribution or sanction, the mere existence of a national do-not-call list will not be sufficient to eliminate the issue. That is why Rogers, like its peers, is doing its utmost to eliminate these types of calls from our network. In fact, Rogers is diligently working to rid our network of all forms of unwanted mass calling. Over the last five years, Rogers has taken a leadership role in the industry, helping to spearhead several initiatives to tackle the problem.

Since 2015 we have worked with the CRTC enforcement branch to provide network resources, including telephone numbers and call routing, for the Canadian telephony honeypot project. This initiative collects data about fraudulent calls targeting Canadians in order to identify the methods used and assist with enforcement. For the last four years Rogers has also actively participated in the CRTC Interconnection Steering Committee, CISC, to review call blocking, STIR/SHAKEN and call traceback solutions. Rogers has taken a leadership role in many of these processes, including co-chairing several of these CISC working groups.

In 2017 and 2018, Rogers also took the lead in exploring and scoping an industry-wide filtering solution to reduce unwanted calls. Over 18 months, Rogers led a committee of 12 major carriers to assess various options. This culminated in an RFP to find a national analytics engine database, as well as a Rogers-specific RFP to potentially upgrade our network.

Finally, in 2019 Rogers worked with other Canadian telecom service providers to develop and deploy universal call blocking at the network level.

More recently, Rogers started to deploy STIR/SHAKEN. This technology will authenticate caller ID and is expected to be network ready by the end of 2020. Rogers has led many cross-industry committees to establish the best practices and mechanisms that will support its deployment, including the creation of the Canadian Secure Token Governance Authority to manage STIR/SHAKEN operations in Canada. In fact, we funded the initial work of the CSTGA.

Unfortunately, these solutions are time-consuming and complex to deploy. Telecom networks are designed to permit call completion, not prevent it, and blocking illegitimate traffic without interfering with legitimate calls is harder still. For example, while the telecom industry is working very hard on delivering STIR/SHAKEN this year, it still remains far from being launched on a commercial basis. Some standards remain to be defined, including how to display STIR/SHAKEN on the end-user devices. STIR/SHAKEN also requires end-to-end IP interconnection, which is a long time away.

Moreover, even as the industry adopts increasingly more countermeasures, the criminals are not resting. Their tactics and techniques continually evolve and change so that stopping unwanted mass calling becomes even more difficult. Most importantly, they are almost all situated offshore.

There is, however, much that can be done to combat unwanted mass calls. It will require the co-operation of industry, the CRTC and the Government of Canada.

First, the telecom industry must continue its current work instituting universal call blocking and STIR/SHAKEN. While these efforts will not end nuisance and fraudulent calls on their own and they will take time to fully implement, they do provide a foundation upon which other efforts can be based.

Second, the industry must continue to develop new methods of targeting these types of calls. Unwanted mass calling is an arms race, with each side continuously upgrading their efforts. New technologies and processes are being developed each year, and carriers must be quick to adapt and adopt.

● (1215)

Third, the CRTC should expand its enforcement of the rules. As the primary regulator of the telephone system, the commission must ensure that bad actors are punished. Since carriers are prohibited under the Telecommunications Act from simply blocking calls, the CRTC must be proactive in shutting down fraudulent calls when observed.

Fourth, the commission should target the points of entry in malicious calls. A large portion of international nuisance calls are coming into Canada through a small number of points of entry. The commission should therefore focus its efforts on why and how such calls appear to be entering Canada in this manner and what can be done to prevent it. It could emulate, for example, the efforts by the FCC, the U.S. Department of Justice and the Federal Trade Commission, which have recently worked together to stop incoming international robocalls at domestic telephony traffic gateways, that is, specific entry points into the United States.

Fifth, the CRTC can accelerate the deployment of SIP trunks. SIP interconnections allow carriers to adapt better technologies that can combat malicious calls, STIR/SHAKEN in particular. SIP, however, is not mandated at this time, and some carriers are deploying it sooner than others. The commission should be pressing for its widespread adoption.

Sixth, the Government of Canada itself has a crucial role. The overwhelming majority of nuisance and fraudulent calls originate abroad. The government, through Global Affairs Canada and the RCMP, must work with its foreign counterparts to shut down the call centres and robocall platforms that originate these fraudulent and spam calls. As long as these parties continue to operate with impunity, they will simply find new and alternative ways to circumvent the protections and measures implemented by telecom service providers to defeat this problem. There is no better way to stop these calls than at their source.

Last, there is an important educational component. Every stakeholder can help Canadians become more aware of how to avoid the scams that are driving these fraudulent calls. Rogers has resource materials available on our website to help consumers spot a telemarketing scam, how to protect themselves from caller ID spoofing and spam calls and how universal call blocking helps protect them.

At the same time, organizations such as the Canadian Anti-Fraud Centre are active in educating consumers about frauds, including those that abuse the telephone system, and in improving awareness of the techniques employed by the fraudsters, but they, along with all of us, should do more on this aspect, especially with vulnerable people and immigrants.

Rogers looks forward to working with its peers, the CRTC and the government to address this critical issue for Canadians. Thank you for the opportunity to participate in this review. We are happy to answer any questions you may have.

● (1220)

The Chair: Thank you very much.

Our next eight-minute round will go to Monsieur Birot with Telus.

[*Translation*]

Mr. Jérôme Birot (Vice-President, Voice and Services Development Operations, TELUS Communications Inc.): Thank you.

Madam Chair and honourable members of the committee, my name is Jérôme Birot, and I am the vice-president of development operations for telephone and value-added services at TELUS.

I'd like to begin by thanking you for the opportunity to address the committee today on the important topic of fraudulent telephone calls. With me for this discussion is John MacKenzie, TELUS's director of regulatory affairs.

[*English*]

As part of our first promise to customers, Telus has been devoting significant resources over the last few years toward finding a solution to the issue of fraudulent calls. However, it's not an easy issue to solve.

Companies around the world are struggling to find a solution. Global telecommunication networks have evolved to seamlessly connect people and data wherever they may be in the world. With the emergence of a truly global economy, these networks are being exploited by thieves and criminals at home and abroad intent on defrauding Canadians through fake and fraudulent phone calls.

I am often asked, “Why can't you just stop calls from the scam artists?” Unfortunately, fraudsters use sophisticated methods to mask the origin of their calls. They are extremely effective at blending their fraud calls with normal, legitimate network traffic as it is routed around the world. By the time they reach our shores, it is very difficult to distinguish between a fraudulent call and a legitimate call.

Since we have a regulatory obligation to allow legitimate calls to either terminate on our network or transit through it, the calls are routed to their intended destinations. When we are able to identify fraudsters, we do our best to block their calls. These are often static methods, and are not effective in a dynamic environment. So what can we do?

There are third party apps and capabilities provided by smart phone manufacturers, allowing users to block or filter their calls. They can prove cumbersome for consumers to use or may not be very effective. In addition, there are several types of systems that telecoms use to limit fraud calling in the network, such as call blocking and call filtering.

Call blocking systems, such as universal call blocking, or UCB, involves the telecommunications service provider blocking suspicious calls originating or terminating on its network, or passing through its network. For example, a calling number with all zeros would be blocked. On the other hand, call filtering systems are controlled by customers. They filter calls based on their preferences, and do not affect calls to anyone else.

At Telus, we offer a call control service, a proprietary call filtering system provided free of charge to most of our home phone customers. Call control is designed to be simple for our customers to activate and simple for them to use.

To explain how it works, I will use the hypothetical example of me trying to call you, Madam Chair. You will be a Telus customer. You will have activated call control on your phone. When I call your phone number, my call will be intercepted by the network before it reaches you. I will then hear the following message: “This number is call controlled. To get through, please press...”. Then it will prompt the caller, me, for a random number between zero and nine. We call this the challenge. I then have to press the correct number. When I do that, my call to you will be connected and your phone will ring. If I press the wrong number or do not press any number at all, my call will be rejected. I'll hear a voice recording indicating that you are not receiving calls. More importantly, your phone will not ring.

It's proven very effective at filtering out fraudulent calls, because those calls are typically autodialed by a computer system, and computer systems lack the ability to follow the instructions from the challenge.

Call control can also be customized through the use of personal lists, such as accepted callers and blocked callers. If a phone number is on the customer's accepted callers list, it will bypass the challenge. If, on the other hand, a phone number is on the customer's blocked callers list, it will be rejected.

We also have another list unique to each customer called the recent callers list. The recent callers list, which is controlled by Telus, comprises the last 10 phone numbers that have successfully passed the challenge. Phone calls from these numbers do not get challenged until they are overwritten by more recent calls.

In my previous example, this will mean, Madam Chair, that your friends and family who call you often would not have to pass the challenge every time they call you.

● (1225)

The results of call control have been impressive. Since its initial introduction in May 2018, we have determined that call control is significantly more effective than UCB, blocking 40% of incoming calls to customers who have activated the feature. Call control is also almost immune to spoofing, namely, where fraudsters hide their identity by faking a genuine number, like the one here today or one from a local area code. Due to the success of call control, we have been working on enabling it for our wireless customers. We expect to make it available to them in the coming weeks.

Switching gears, I would like to conclude by talking about STIR/SHAKEN. STIR/SHAKEN is neither a blocking system nor a filtering system. It is a set of protocols designed to validate the integrity of the caller ID and to provide the customer receiving a call with the assurance that the calling number belongs to the caller. Voice service providers who fail to support STIR/SHAKEN will likely find themselves at a competitive disadvantage. It is clear that STIR/SHAKEN has momentum in North America, and I expect it will be adopted shortly thereafter in Canada.

Telus is among the Canadian service providers that established a new corporation, the Canadian Secure Token Governance Authority, to support the implementation and operation of STIR/SHAKEN in Canada. However, there are still many issues that prevent STIR/SHAKEN from fully addressing the problem of fraudulent calls. The most significant of these issues is that STIR/SHAKEN standards will apply to calls within Canada initially, and at best within North America. However, many fraudulent calls originate from outside Canada. Another issue is that the system does not work if there is legacy circuit-switched equipment anywhere in the call path, which is common across networks that have been in operation for decades. Finally, we do not know how smart phone manufacturers will embrace STIR/SHAKEN standards or display STIR/SHAKEN information on their devices.

As a result of these challenges, and until STIR/SHAKEN standards are adopted globally, we do not know when STIR/SHAKEN will meet the high expectations that many have for the technology. Notwithstanding these issues, Telus is supportive of STIR/SHAKEN. We're confident that its capability will continue to improve. While we likely cannot offer STIR/SHAKEN sooner than in the U.S., we expect that Canada will follow shortly thereafter. In the meantime, we're confident that call control will provide effective protection for Telus customers.

That concludes my opening remarks. I welcome any questions you may have.

● (1230)

The Chair: Thank you very much.

Before we begin our six-minute round, I want to remind people in the audience that there is absolutely no photo taking allowed during committee.

With that, we'll start the first six minutes with MP Gray.

Mrs. Tracy Gray: Thank you, Madam Chair.

Mr. Birot, you mentioned STIR/SHAKEN. I have noticed through my research on the issue that it's in emulation of a model that was implemented in the U.S. for fraudulent calls. Has your corporation studied any other models, or fraud calls being used locally? If so, are there other models that you feel might emulate this a bit better, or any components that you think might be useful to add?

Mr. Jérôme Birot: Yes. We have the call control service, which we believe can tackle the vast majority of those fraudulent calls. STIR/SHAKEN is a great way to augment this, but call control, for now, helps us and helps our Telus customers.

Mrs. Tracy Gray: Great. Thank you.

Mr. Daniels, you mentioned that Bell has proposed that the CRTC STIR/SHAKEN mandate be delayed until we can get the rules of the regime figured out. The process for the model was started back in 2015 by the CRTC. That was five years ago. How much more time do you think you need?

Mr. Jonathan Daniels: We actually proposed to the CRTC that there be a firm deadline of June 2022. We think it will be worked out before then.

Just to be clear, we're still planning on launching it in September. I guess what we're trying to say is that in the rush.... There's lots of talk, as you've heard from everyone, about STIR/SHAKEN. There's a lot to be figured out. But most importantly, with the phones right now, if you turned on STIR/SHAKEN today or tomorrow on our network, very, very few people would have phones that could actually benefit from it. The whole point of it is that the phone end-user would see it and say, “Oh, the number that's coming is verified. It's accurate. It's okay.” If you don't have a phone that can do that, as most of our phones can't—we have to wait for the manufacturers, the Apples and the Samsungs, to create phones to do that—then there's no rush to put it out. Very few people could actually use it.

I just want to make it clear that when we say “delay”, and it sounds.... There is a lot to be worked out, but even if we all turned it on tomorrow, very few customers could actually benefit from it. So we're going to take the time to get it right. I think what you're hearing is that we're all supportive. We're in fact turning it on in September.

Mrs. Tracy Gray: Thank you.

I have another question for you, Mr. Daniels.

Do you have the telecommunications fraud website in other languages? I'm especially thinking of new Canadians and vulnerable people in our society. Do you have that in other languages?

Mr. Jonathan Daniels: Are you talking about in terms of a Bell website? I honestly don't know the answer. I'm sure we have it in both official languages, but I don't know, so I'll have to take that one away and get back to you on that.

Mrs. Tracy Gray: Okay. Thank you.

The prevalence of unauthorized porting and SIM swapping has recently been brought to my attention as a scam rising in proportion in Canada, which is locking individuals out of their phones and giving scammers access to their phone apps and personal data. What are you doing to ensure call centre employees and staff employed by your corporations properly verify your clients?

I open it up to anyone who might want to address that.

Ms. Deborah Evans (Chief Privacy Officer, Rogers Communications Inc.): Thank you for your question.

As an industry collectively, first of all, I'd like to say we've come together to put some solutions in place to help consumers not be subject to porting fraud. There are things that we're rolling out. Obviously, we don't talk about them publicly because we don't want the fraudsters to know what they are.

With regard to porting fraud, just porting in general is meant to be as easy as possible. You're meant to go in and get your port done without having an interaction with your existing telephone provider. It's really to enable the port to go as quickly as possible. Most of the ports are done over the phone or online, so from that perspective you go into your new service provider and you request your port, and then it goes back to your old service provider.

The way the porting rules have been established by the CRTC and the porting guidelines from the industry that came together collectively, you're required to have a phone number, a postal code, and then either an IMEI or an account number. Unfortunately, it's pretty simple for fraudsters to gain some of that information from various sources around the world. This isn't an issue that's common to Canada. It's a global issue and all carriers are facing it around the world, so it's challenging. Fraudsters are constantly evolving and changing their techniques and we're trying to stay ahead of it and put things in place. As my colleague mentioned earlier, fraud is an arms race. We put things in place and then the fraudsters come and circumvent them. We're continuously evolving and working collectively as an industry to address the problem.

● (1235)

Mrs. Tracy Gray: We haven't seen a lot of statistics on that. Do you know how many cases of unauthorized phone porting have been logged by your organization or as an industry?

Ms. Deborah Evans: I do not.

Mrs. Tracy Gray: Okay.

One other question I had was with regard to communicating to at-risk groups such as seniors and new Canadians around potential phone scams and fraud calls. I'm wondering if you can let us know what outreach you're doing to those communities.

Ms. Deborah Evans: For our company what we do is if we notice a particular scam targeting a particular community group, we will put ads in local newspapers in their language of choice. For example, we had a scam recently targeting immigrant communities from mainland China, so we had our IVR updated in their language so it could alert them.

The Chair: Thank you very much.

Unfortunately, that's the end of the first round.

The next six-minute question goes to MP Jowhari.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Madam Chair, and thank you to all of you for coming in and shedding some light on something that everyone is concerned about.

All three of you spent a fair amount of time talking about STIR/SHAKEN as the tool, the method, that's being looked at in helping us. Also, there seems to be a commitment that this thing will go forward in September 2020 in some shape or form. However, you also all highlighted that there are many dimensions to this, and this is not going to be the be-all and end-all tool. As well, we're not ready at our end from a device point of view, from an education point of view, and all of that, to be able to roll this out.

Each one of you individually touched on, whether it's the education piece, whether it's the technology piece, whether it's the device model, is there a set of well-defined criteria that is needed for this thing to be fully rolled out? Do we have an idea of the timing for each one of those criteria to be completed so we'll have a wholesome solution?

Any one of you can answer.

Mr. Jérôme Birot: I can take this one as the only technical guy on the panel.

It is complex. First, any legacy network, normal IP network, will not work with this technology. That's a big challenge for all the carriers within Canada to upgrade every part of our network, or work with the carriers we interconnect with to upgrade our networks. That's one challenge, and obviously we can't mandate another carrier to do it faster for us so we can have better service for our customer. We don't have that reach or that jurisdiction.

Second, the devices are not the carriers' devices. They are the manufacturers' devices. They choose when they need to implement a certain feature within their devices. It's very hard for any of us to tell when the smart phone manufacturers will decide to implement this. Then what do we do with the wireline part? How do we handle home phones and provide similar service for home phone users?

As an industry we need to come together. We already set together the CSTGA. That's the governance of it. There's the policy administrator. There is the token administrator for all these parties to exchange and make sure there is an authority that will validate these calling numbers.

I'm afraid I can't answer your question in a straight fashion because many components are outside our control in all our cases.

● (1240)

Mr. Majid Jowhari: I get it that the main issue you are highlighting is the back-end network and also the customer facing, which is the device.

Mr. Jérôme Birot: That's correct.

Mr. Majid Jowhari: Okay.

Mr. Jonathan Daniels: I totally agree with everything that was just said. I realize it's dangerous here because we're getting technical and so on. All three of us did an excellent job of explaining that for a non-technical person.

I think the message you're hearing from all three of us today is that there's no one solution. Even if we had STIR/SHAKEN and every phone was capable of doing it and we all had the technology, all STIR/SHAKEN does is tell you that the number that's calling has been authenticated as truly the number that's calling. That's all it does. That doesn't necessarily mean that a fraudster can't be calling, that you pick up the phone and can't start doing fraud.

That's why we have to look at more than one solution. In our case we're saying that the quickest one is.... We know we have 120 million fraudulent calls a month. We could block them today as soon as we get permission—

Mr. Majid Jowhari: Thank you.

I was hoping you'd go there because you highlighted the fact that it takes some time to work with the CRTC to get permission. What do you suggest? I think I heard that the CRTC automatically blocks or allows you guys or the big carriers to block those calls immediately. What are the challenges facing the CRTC or facing you that that permission isn't allowed? ?

Mr. Jonathan Daniels: The CRTC has to do a public process. I don't want to be laying this as criticism.

We applied. We're going through the process and we're waiting for the decision. Comments just closed. The reason they have to do all that is we are making decisions based on the content of the call. We're saying these are fraudulent calls. As people know, we have to be very careful. We shouldn't be making decisions based on the content of calls. I'm sure this committee has had other issues about that. For that reason we have to ask for permission.

We've asked to do a trial so we can learn the lessons. We will be happy to share that information from the trial with both the CRTC and our competitors as well.

Mr. Majid Jowhari: Thank you.

I think my time is over.

The Chair: Pretty much.

[*Translation*]

Mr. Lemire, you may go ahead.

Mr. Sébastien Lemire: Thank you, Madam Chair.

I'd like to thank the witnesses for being here today and contributing to our study.

It's tough to ask pointed questions with this panel. I know that you're all in competition with one another.

I would ask you to keep your answers brief.

About how much would you say all the measures you need to put in place cost?

Does the war on fraud affect your service providers? Will the cost ultimately be passed down to customers?

What can you do to help small providers, who have more trouble offering these services for financial reasons?

[*English*]

Mr. Jérôme Birot: I can start.

We are investing in technology to help prevent nuisance calling. Call control is there. It's offered free of charge to our customers who subscribe to it.

Would we offer this to other carriers? We would absolutely consider wholesaling this as a service for smaller carriers that wish to adopt this service.

Mr. Howard Slawner: I agree, to put all of it in place.... As Jon said before, it's not one single solution, so I think it's incumbent on all the carriers to actually keep looking at all of the various technologies that are out there right now. We are implementing STIR/SHAKEN. We have implemented UCB and we're actually currently evaluating other technologies that we can bolt on to these things.

There is no one quick solution that will do it, so for everything to happen, we have to keep looking at the broad selection. I do think that the smaller carriers will be able to benefit from the experience of the bigger carriers going forward, because the technology will then be applicable to them as well. It's in everybody's best interests that the entire industry is protected, so it's in our interests as well to have the small carriers included.

Mr. Jonathan Daniels: I agree with that.

From our perspective, when we look at our trial, our intention is to sign agreements to share the details with big players and small players. It is very clear that, if we get permission, we will be blocking calls, regardless of where they're going on our network, for no charge. I don't think any of us is looking for any money to be made. This is about a service to our customers and to Canadians.

● (1245)

[*Translation*]

Mr. Sébastien Lemire: I'm very glad to hear that. Thank you.

It is often said that you have to fix problems at the root. Tangibly speaking, are you adopting any specific strategies in light of the techniques being used?

Is it an option to block calls from identified countries such as India, which we were talking about earlier?

Can we bring more pressure to bear on countries where fraud calls originate?

[*English*]

Mr. Jérôme Birot: One challenge with this approach is that there may be legitimate calls from legitimate people in those countries trying to reach our shores, trying to reach Canadian families here. That's the danger of making arbitrary decisions in a network at the tail end. At the source, yes. Can we enforce that? It's outside of everyone's jurisdiction here, unfortunately. Should we all work together? Absolutely.

Mr. Howard Slawner: I would echo that as well. I think the RCMP, Global Affairs Canada and the CRTC should continue working with their partners abroad. We understand the challenges they may have, but I think we have to continue putting pressure and attack this problem by every method possible.

Mr. Jonathan Daniels: I also agree. We actively work not just with our Canadian counterparts but with U.S. carriers. We sit on forums with them. We try to exchange. We've done some experiments to learn from them. However, in terms of getting to the source, that's really at a government level.

[*Translation*]

Mr. Sébastien Lemire: Originally, you were required to deploy the STIR/SHAKEN framework in March, but the deadline was pushed to September 30.

Do you think that's a realistic deadline?

Your reactions appear rather mixed. Should we anticipate another request for an extension?

[*English*]

Mr. John MacKenzie (Director, Regulatory Affairs, TELUS Communications Inc.): At Telus, we think that the September 30 deadline will be earlier than will allow...it won't allow any particular consumer benefits for the reasons that Mr. Daniels has pointed out, and Mr. Birot—

[*Translation*]

Mr. Sébastien Lemire: I'm going to reword the question. You had until February 24 to submit a status report. Did you submit the report?

Did you formally advise the CRTC of the limitations?

[*English*]

Mr. John MacKenzie: Absolutely, we reported that. We identified the limitations and what we thought was a better schedule.

Mr. Howard Slawner: I agree. It is doable to get the network equipment done at that time, but a better timetable would give us the sufficient amount of time to actually get the standards correct and get the equipment rolled through.

Mr. Jonathan Daniels: I have the same answer.

[*Translation*]

Mr. Sébastien Lemire: Great. That's all for me.

[*English*]

The Chair: The next round of questions goes to MP Masse.

Mr. Brian Masse: Thank you.

I'll follow up with that questioning.

There's nothing on your network side in your capabilities that's stopping STIR/SHAKEN then. Is that correct?

Mr. Jonathan Daniels: No, that's not correct. I've talked about the devices for the end-user, but in our network, which is what you're asking about, our actual switches themselves have to be upgraded to be able to handle that. We're in the process of doing that with all of our vendors, so not all of our switches are ready to do that.

Mr. Brian Masse: That would be the only—

Mr. Jonathan Daniels: It would not be the only thing. I'm trying to avoid getting more technical or into more things. There are many other things.

Mr. Brian Masse: What I'm getting at here, though, is that there seems to be a reluctance to some degree. Some of this can be consumer-driven, on a positive end, for consumers wishing to take advantage of STIR/SHAKEN by replacing outdated equipment and so forth. I guess I'm getting mixed signals on this. There's a right for consumer choice. It shouldn't be the excuse not to do something or to slow something down if somebody chooses to update their own telephone system and so forth.

I want to make sure I get this one correct. This question is for everybody.

Do I understand that everybody here provides free caller ID or identification or blocking? Is there no charge to any of your customers for any of that type of thing?

Mr. Jérôme Birot: That's correct.

Mr. Brian Masse: Rogers.

Mr. Howard Slawner: I'm not sure. I don't believe we have any fees for caller ID or anything like that. I'll double-check, but I don't think we do.

Ms. Helena Jaczek: You do.

● (1250)

Mr. Howard Slawner: We do? Okay. I'll check.

Mr. Jonathan Daniels: I believe we do, in terms of.... I just want to be clear. That's a bit different—

Mr. Brian Masse: I'm sorry, but this is my time. I just want a straightforward answer on that. For some of my constituents—and I know with my service provider that I have to bundle that with something else that I don't want or not get it. That's an economic barrier for some Canadians. I think allowing for protection for some people who can afford it and not for others who can't is patently unfair. I'd ask you to revisit those policies, because even if they are offered for free, sometimes they're bundled with other things.

When it comes to the CRTC enforcement systems in place, Rogers—I'm calling you by your company's name; Sorry, Mr. Slawner—you mentioned, and I'm a big fan of this, too, that if you break the rules, you get punished for it. The CRTC has used AMPs in a way that I don't think is terribly effective at times and they can be a loss leader for some businesses. It's better to plead for forgiveness than to ask for permission. What more could they do that would actually get the bad actors out of the way?

Mr. Howard Slawner: On the one hand, I want to express that they are trying their best. I do believe that. The problem you have with the bad actors out there is that they don't care about the rules. That was kind of the point we were trying to make. You have these DNCL rules, but the people, especially the ones who are abroad, aren't listening and are never going to listen to them. They simply ignore the law and there's really nothing for the CRTC to actually do. That was the real point I was trying to make.

With regard to broadening their efforts, I just think that when they do find Canadian connections to these mostly international schemes, they do need to pursue them, working with our RCMP partners, and make an example of them.

Mr. Brian Masse: There has been lots of testimony over the years about the CRTC needing an update and also having some timelines for decisions. You don't even have a timeline for your application, in terms of the CRTC. Is that correct? It's going to go through its regular process, but that could take quite some time.

Mr. Jonathan Daniels: That is correct.

Mr. Brian Masse: That's the thing.

I just want to ask one other question regarding the filtering services you have available right now. Is there any interest in some type of a universal system being employed or in benchmarking?

One of the recommendations I'm looking at is whether consumers or consumer agencies or even Industry Canada can benchmark the different operators in the system in terms of their protection of privacy, information and consumers' trust related to calling.

Let me start with Telus and go across.

Mr. Jérôme Birot: Just to make sure I understood correctly, are you asking whether we should benchmark our call filtering technologies?

Mr. Brian Masse: Yes.

Mr. Jérôme Birot: We certainly have statistics. I shared with you that our call control service blocks 40% of the calls to people who have activated it. Should it be benchmarked? Everyone is using different technologies, so it may be difficult for an independent party to generate more nuisance calls to validate whether they are being captured. This may come as an annoyance to people. But by all means we are already subject to benchmarking in the speed test and in many other forms. I can't comment beyond this.

I'll take away your comment around the caller ID, as well, just to make sure it's not bundled with anything else.

Mr. Brian Masse: Okay. Thank you.

Mr. Howard Slawner: Yes, and I'll echo a lot of that.

Another thing, for example, is that for universal call blocking, when we first implemented it we kept the net wide, like a big mesh. Slowly, over time, we're shrinking the mesh as we understand it better.

I think it's kind of hard to try to measure people carrier to carrier or even to international standards, because we're already constantly improving what we're doing. I think it's difficult for us to actually do that.

Mr. Jonathan Daniels: Yes. I'm not quite sure what you would be benchmarking in terms of how you would judge the standards.

I guess I'd put it this way. We want to be the best at providing service to our customers, and customers are annoyed by these calls, as well as scammed. Therefore, I think it's in our interest to work with the industry to actually get the best solutions and to share our learning amongst ourselves. This is a weird area, where we're actually sharing solutions amongst ourselves.

The Chair: Thank you very much.

We'll now move into round two. We have enough time for one group of questions for five minutes.

MP Dreeshen, the time is yours.

Mr. Earl Dreeshen (Red Deer—Mountain View, CPC): Thank you very much, Madam Chair. If I get a chance and don't talk too long, I'll see whether Mr. Van Popta would like to ask a question as well.

In the Rogers brief, there was a discussion about these groups that are operating with impunity. It's as though there's no way to help. We had the RCMP in earlier and there were discussions there. I'm just curious about how close your co-operation is with them when they need it. It would be a bit of a discussion, perhaps.

Ms. Evans.

● (1255)

Ms. Deborah Evans: We co-operate with the RCMP, absolutely, when they need it. Sometimes we take the initiative ourselves. We have gone to them and have reported issues that we've been seeing on our network. I've met a couple of times with one of the RCMP gentlemen who was here and we've discussed some commonalities that we're seeing, so yes, absolutely.

Mr. Earl Dreeshen: Okay. I guess where I wanted to go on the other part is that we're looking at 5G networks and so on coming into play and, of course, the cities are where the best coverage is right now. The rural areas are always concerned, in that more money continually goes into where the cities are, and it's harder and harder to get coverage out in rural and remote areas. With the 5G part, of course, come some of the other players that might be interested in this.

Some of the other discussions we've had were about how you have people from other countries looking to cause some sort of damage in your system. It could mean that they listen in on you, and if they can do that, they can then target different ways to scam, so there are the cyber-risks that are associated with that.

I'm running around in a circle on this one, but I wonder if you could comment on how people can be sure, as we expand our networks, that we're able to maintain the type of security that's needed, so that this isn't also being used as a back door for issues.

Mr. Jérôme Birot: I can tell you that at Telus how we run works from the premise of security by design. Our security office is involved right from the design of every single service in everything we do. That's one of our fundamental values at Telus.

Mr. Howard Slawner: I'll echo that. We work with our technology partner, Ericsson, in making sure that all of our network is safe and secure so that our 5G network will be the most reliable and most trusted in the country.

Mr. Jonathan Daniels: Obviously, security is first and foremost. As we roll out 5G, we are going to ensure that we have the best network. That includes having top security and ensuring that people aren't able to listen in, as you've described, in those manners.

Mr. Earl Dreeshen: Thank you.

Mr. Van Popta, do you want to take some time?

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

Thanks for your presentations.

Several of the presenters made the distinction between nuisance calls on the one hand and illegal calls on the other. I think we could probably define those terms, but do the telecoms have the technology to distinguish one from the other and to stop one but not the other?

Mr. Howard Slawner: I don't think there is a technology that can do that. I think fraudulent calls are a subset of nuisance calls. I think they're all nuisance calls, whether or not they're legal.

We're paying a lot more attention, though, to the fraudulent calls, because they've been growing so much lately and the idea is that they hurt people more. Being disturbed on a Sunday morning is bad. Having your life savings stolen is a lot worse. I think that's the difference in the focus.

Mr. Jonathan Daniels: From our vantage point, we can't detect and determine all calls without.... You'd have to listen to a call, and we're not listening to anyone's calls.

We are using the latest technology and we're able to identify a large subset of fraudulent calls. We confirm that those are fraudulent calls, and those are the ones that we are seeking to block. It's only those that are really trying to defraud.

That's our particular proposal, which we would like to do as the trial. If successful, I'm sure we'll be sharing the benefits with the rest of this panel.

Mr. Tako Van Popta: Do I still have a moment?

The Chair: You have 30 seconds.

Mr. Tako Van Popta: Mr. Slawner, you were saying that perhaps the CRTC or Canadians could emulate what's been happening with the Federal Communications Commission and the Federal Trade Commission to stop international robocalls. Why haven't we done that yet?

Mr. Howard Slawner: I don't know. I think we're just learning some of these statistics now.

Since we've instituted call blocking, we've been learning more about what types of calls are coming, where they're coming to and how they're entering the country. I think now is a really good opportunity, after universal call blocking has been implemented, to find out more and take some better measures.

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

I want to thank all of you for being here and I thank the members for their excellent questions.

With that, we will adjourn.