HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

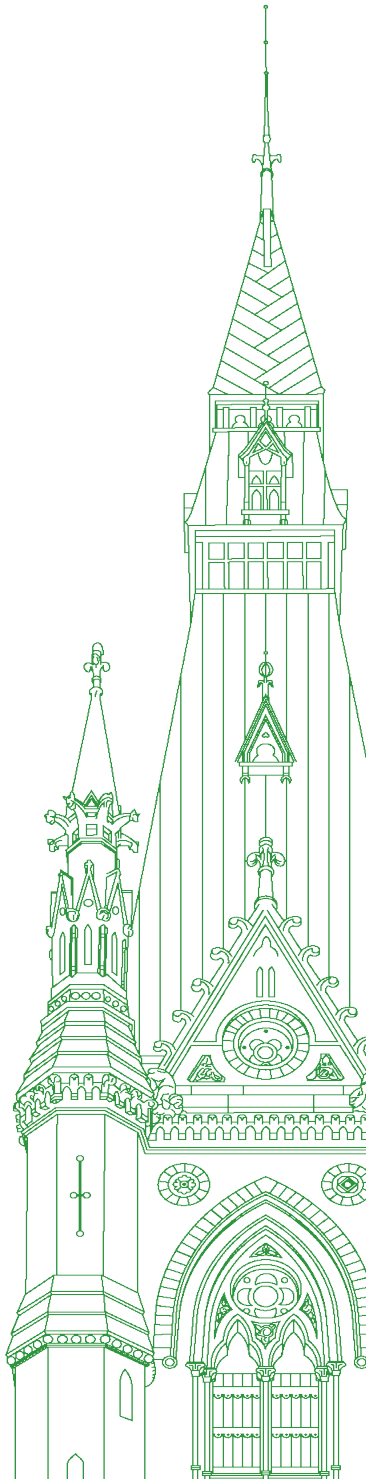
43rd PARLIAMENT, 1st SESSION

Standing Committee on Industry, Science and Technology

EVIDENCE

NUMBER 016

Wednesday, May 20, 2020



Chair: Mrs. Sherry Romanado

Standing Committee on Industry, Science and Technology

Wednesday, May 20, 2020

● (1500)

[*English*]

The Chair (Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Good afternoon, everyone. I now call this meeting to order.

Welcome to meeting number 16 of the House of Commons Standing Committee on Industry, Science and Technology. Pursuant to the order of reference of Saturday, April 11, the committee is meeting for the purpose of receiving evidence concerning matters related to the government's response to the COVID-19 pandemic.

Today's meeting is taking place by video conference, and the proceedings will be made available via the House of Commons website.

As a reminder to the members and the witnesses, before speaking, please wait until I recognize you by name. When you are ready to speak, please unmute your microphone, and then return it to mute when you are finished. Please speak slowly and clearly so that the translators can do their work, and please make sure your questions and comments are through the chair.

As is my normal practice, I will hold up the yellow card when you have 30 seconds left in your intervention, and the red card when your time for questions has expired.

I will now welcome our witnesses.

[*Translation*]

From the Autorité des marchés financiers, we have Jean-François Fortin, executive director of enforcement, as well as Christian Desjardins, director of assessment and inquiry.

[*English*]

From the Canadian Internet Registration Authority, we have Mr. Byron Holland, president and chief executive officer; Mr. Dave Chiswell, vice-president of product development; and Mr. Albert Chang, corporate counsel.

From the Communications Security Establishment, we have Mr. Scott Jones, head of the Canadian Centre for Cyber Security.

From Nuance Communications, we have Mr. Simon Marchand, certified fraud examiner and certified administrator, biometrics and security.

As well, from the Royal Canadian Mounted Police, we have Mr. Eric Slinn, assistant commissioner, federal policing criminal operations; and

[*Translation*]

Guy Paul Larocque, acting officer in charge of the Canadian Anti-Fraud Centre.

[*English*]

Each witness will present for five minutes, followed by our rounds of questions.

We will start today with the Autorité des marchés financiers. You have five minutes.

[*Translation*]

Mr. Jean-François Fortin (Executive Director, Enforcement, Autorité des marchés financiers): Thank you, Madam Chair.

As you mentioned, I am the executive director responsible for enforcement, and with me is my colleague Christian Desjardins, director of assessment and inquiry.

The Autorité des marchés financiers, or AMF for short, is the regulating body for financial markets in Quebec, and its mission is to regulate the financial sector.

The AMF proactively monitors issues and challenges related to financial fraud at all times. That monitoring takes many forms and is carried out by a number of teams within the AMF. Those efforts are complemented by the AMF's active involvement in Quebec, Canadian and international committees.

We have multi-sector teams working together to ensure market oversight, cybersurveillance and vigilant monitoring. We also invest heavily in major awareness campaigns and strategic partnerships.

Since March 16, the AMF has been in telework mode. We were able to quickly set up the teams needed to keep enforcement and awareness work going remotely. With a few exceptions, all employees are fully operational from home. We've had to ease up on activities such as in-person interviews and testimony, but it hasn't affected operations. Information-gathering and analysis work, as well as video-conference interviews are carrying on.

During the COVID-19 pandemic, the AMF has stepped up its web surveillance. It also sits on an investment fraud task force that brings together all of Canada's securities regulators to share information on illegal activities identified in connection with COVID-19.

In addition, the AMF is on a task force established by the North American Securities Administrators Association, which represents securities regulators in Canada and the United States. The purpose of the task force is to coordinate the communication of potential investment fraud stemming from COVID-19, coordinate related investigations and make the public aware of potential risks.

Another step we have taken is establishing a market monitoring strategy to better target potential market manipulation and insider trading. Accordingly, we've been keeping a closer eye on pharmaceutical companies that falsely advertise vaccines or quick fixes, for instance.

We've also made a dedicated effort and tailored monitoring activities to detect potential insider trading in connection with the extended deadline for financial reporting granted by regulators in response to the pandemic. The extension for filing market-related information heightens the risk of insider trading, with executives, professionals, advisers and others having access to non-public sensitive information for a longer period.

That's it for the market oversight and enforcement piece.

Now I'll turn to public outreach and education, an area where we've been extremely proactive. The AMF has sought to raise public awareness by posting COVID-19-related fraud prevention alerts on its website, and stepping up the number of fraud prevention posts on Facebook and other social media sites.

We've sent letters to Quebec's leading seniors associations and consumer groups to remind them that our support services are still available and to encourage them to report scams and other problems they encounter.

Lastly, we've issued multiple investor warnings, which are posted on social media sites and often passed on by our partners.

I'd also like to highlight an important initiative. Back in March, after noticing the number of COVID-19-related scams, we started investing in a large-scale awareness campaign that ran from April 6 to May 5 on television and online including on social media sites.

● (1505)

I want to underscore the number of education initiatives we undertook using TV, social media and other means to reach seniors and vulnerable populations.

The AMF is one of Canada's financial regulators, and we constantly work with all regulators in Canada, as well as international regulators.

Thank you.

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

[*English*]

Our next witness is the Canadian Internet Registration Authority.

Mr. Holland, you have five minutes.

Mr. Byron Holland (President and Chief Executive Officer, Canadian Internet Registration Authority): Thank you very much, Madam Chair and honourable members of the committee.

Most people know the Canadian Internet Registration Authority, or CIRA, as the operator of the .ca registry. Our primary mission is the operation of a safe, stable and secure .ca domain space.

CIRA is recognized as a global leader in the domain name industry. In fact, many other countries leverage our infrastructure, services and knowledge for their own domain name registries. Our technology is considered best in class among our peers. In short, CIRA is fully equipped to navigate the COVID-19 crisis. We are confident in our ability to protect the integrity of .ca.

To date, we have tracked just over 2,000 .ca domain names with COVID-19-related keywords. For context, since January we have registered over 200,000 .ca domain names. This is aligned with what we are seeing from our peers in Europe and around the world, where COVID-19-related domains make up less than 1% of registrations so far this year. However, it’s also important to note that many of these domains are perfectly legitimate, and even positive, such as conquercovid19.ca, a campaign to support first responders.

We scrutinize all COVID-19-related domains carefully to ensure that they comply with our rules, particularly Canadian presence requirements, and to ensure that all domains stay Canadian. We are also working with our global domain name community, including organizations like the Council of European National Top-Level Domain Registries, to ensure that we are aligned with the best practices of our peers around the world.

However, it is not within CIRA's mandate to review or authenticate the content of .ca websites, nor would such authentication be effective, as the Internet, and related threats, is global. While .ca domain names are bound by Canadian law, thousands of other threats come from outside our borders. There are well-established existing tools and processes in place to deal with fraud online and cyber-attacks. If Canadians come across any domain they suspect of being used fraudulently or maliciously, they should contact the Canadian Anti-Fraud Centre or the Canadian Centre for Cyber Security. We work closely with both of those organizations.

When it comes to fraud on the Internet, it is important to remember that hackers love a crisis. While technical solutions form an important barrier to online fraud and cyber-threats, the biggest attack vector is human frailty. Cyber-thieves exploit anxiety, uncertainty and fear to prey on Canadians when they are at their most vulnerable. Unfortunately, the current COVID-19 pandemic provides fertile ground for these criminals.

In this environment, we launched CIRA Canadian Shield. This is a free security and privacy solution for individual Canadians and their families. Working with our partner, the Canadian Centre for Cyber Security, we are already protecting more than 50,000 Canadians with Canadian Shield as they work, learn, teach and socialize while at home during the pandemic. Canadian Shield reflects CIRA's commitment to build a trusted Internet for Canadians. We look forward to the opportunity to protect every Canadian with this free service.

CIRA is helping to protect Canadian hospitals, schools, universities and municipalities through our enterprise cybersecurity service DNS Firewall. It has an install base of more than 1.1 million users, which includes students, teachers, doctors, municipal workers and first responders across Canada.

● (1510)

The Chair: Excuse me one moment, Mr. Holland. I believe we have a point of order.

[*Translation*]

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Madam Chair, the interpreters flagged some sort of whistling noise two or three minutes ago. The interpretation isn't coming through because of the poor sound quality. It would be unfortunate if the francophones weren't able to hear what Mr. Holland had to say.

The Chair: Very well.

Thank you, Mr. Lemire. We'll see what we can do.

[*English*]

We'll go to the next witness, just to see if we can fix Mr. Holland's microphone so that we can go back to him for his testimony.

With that, we will move to the Communications Security Establishment. Mr. Jones, you have five minutes.

● (1515)

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Good afternoon, Madam Chair and committee members. Thank you for the invitation to appear today, from my dining room, to discuss pandemic-related cyber-fraud.

I am Scott Jones and I am the head of the Canadian Centre for Cyber Security at the Communications Security Establishment. CSE is one of Canada's key intelligence agencies and the country's lead technical authority for cybersecurity. Launched in October 2018, the cyber centre is a relatively new organization, but one with a rich history and over 70 years of cybersecurity experience, having previously functioned under CSE's long-standing IT security mandate. The cyber centre is a unified source of expert advice, guidance, services and support on cybersecurity operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn to for cybersecurity advice.

Specifically, the cyber centre focuses on five main areas. We first inform Canada and Canadians about cybersecurity matters. Second, we protect Canadians' cybersecurity interests through targeted advice, guidance, hands-on assistance and strong collaborative partnerships. Third, we develop and share specialized cyber-defence technologies and tools, resulting in better cybersecurity for all Canadians. Fourth, we defend cyber systems, including government systems, by deploying sophisticated cyber-defence solutions. Fifth, we act as the operational leader and government spokesperson during cybersecurity events.

That point brings me to the specific topic of today's discussion, to speak to you about cybersecurity when it comes to COVID-19. As we noted in the national cyber-threat assessment in 2018, the biggest threat facing Canadians online is cybercrime. I would like to provide the committee with an update on the work that the cyber centre is doing to protect Canadians from cyber-fraud occurring before, during and after the pandemic.

During these uncertain times, cyber-threat actors are attempting to take advantage of Canadians' heightened levels of concern and fears around COVID-19. Many Canadians are naturally feeling fearful and stressed, and those emotional responses can be exploited online. We've seen an increase in reports of malicious actors using COVID-19 in phishing campaigns and malware scams.

COVID has presented cybercriminals and fraudsters with an effective lure to encourage victims to visit fake sites, open email attachments and click on text messaging links. These websites, emails and links frequently impersonate health organizations and can pretend to be from the Government of Canada, among others. They are trying to spread malware and scam Canadians out of their money or private data.

The cyber centre has assessed that the COVID-19 pandemic presents an elevated level of risk to the cybersecurity of Canadian health organizations involved in the national response to the pandemic. I want to reassure you that CSE and the cyber centre are working hard to mitigate these threats and protect Canadians.

I am pleased to share with you the steps we're taking to protect the Government of Canada, systems of importance, and all Canadians from cyber-fraud during these times. We continue to leverage all aspects of our mandate to ensure that Canada is protected against threats and that the Government of Canada has access to information that can help inform decisions on our approach to COVID-19. The cyber centre is working tirelessly to continuously raise public awareness of cyber-threats to Canadian health organizations by proactively issuing cyber-threat alerts and providing tailored advice and guidance to Canadian health organizations, government partners and industry stakeholders.

In addition to our advice and guidance for Canadian organizations, we continue to enhance the Get Cyber Safe campaign to help all Canadians take action to help themselves be safe online. In coordination with industry partners and the international network of cybersecurity organizations, the cyber centre is contributing to the removal of fraudulent sites and other materials used to lure Canadians, including sites impersonating the Government of Canada.

To support programs of importance to the government, we have also continued to monitor and protect important Government of Canada programs against cyber-threats, including the Canada emergency response benefit web application. [*Technical difficulty—Editor*]

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): My audio cut out, Madam Chair.

The Chair: Unfortunately, I think the witness's Internet has frozen.

Mr. Glen Motz: He must be in Ottawa.

Mr. Brian Masse (Windsor West, NDP): It will be good in 2030.

[*Translation*]

Mr. Sébastien Lemire: Mr. Masse, do I detect a bit of irony in your voice?

[*English*]

The Chair: Mr. Jones, are you still with us?

We seem to have lost Mr. Jones, so we will move on to the next witness. We will come back to Mr. Jones as soon as we're able to reconnect him.

Our next witness is Nuance Communications.

● (1520)

[*Translation*]

Mr. Marchand, you have five minutes.

Mr. Simon Marchand (Certified Fraud Examiner and Certified Administrator, Biometrics and Security, Nuance Communications): Members of the committee, good afternoon and thank you for having me today.

My name is Simon Marchand, and I am the chief fraud prevention officer at Nuance Communications Canada. Nuance is an American company with a strong presence in Montreal. It develops technologies that rely on artificial intelligence and voice biometrics for use in fraud prevention, among other things. My specific role is to apply those voice biometric technologies to identity theft prevention. Nuance's products are widely deployed throughout Canada, with most of the big banks and telecommunications carriers using its biometric-based technologies. Nuance also has an extensive international clientele, including major U.S. banks and most of the world's big companies. We develop solutions for law enforcement agencies and government service providers, as well, to help them gather evidence and identify citizens.

I am here today to share with you some of our observations. In my capacity, I'm obviously abreast of all the major scams around the world. I'd like to tell you what we've seen in relation to the COVID-19 pandemic and flag some of the risks that need to be addressed, to help ensure Canada's legislation is equipped to deal with fraud-related issues that may be imminent.

I'll start with some of the internal risks. In response to the COVID-19 pandemic, companies quickly reorganized their operations to accommodate telework. I'm not here to praise or criticize telework, but I will say that it poses real risks, especially in connection with customer service. All customer service representatives who usually work in call centres are now working from home, in an unsupervised environment. Despite having few tools, they now have access to sensitive information about consumers, ranging from information about their assets to information that someone could use to impersonate someone else.

The current socio-economic reality will no doubt put pressure on many households. When it comes to internal fraud, we know that pressure and opportunity are the two basic factors that drive an employee to go against their employer's interests and commit fraud, including stealing information belonging to the organization. Let us not forget that some organizations collect highly sensitive information about Canadians.

These changes in how work is organized raise the possibility of information being stolen and eventually posted on the dark web. That will definitely serve identity thieves well.

Other witnesses have talked about phishing scams, a problem that's already well documented. Sophisticated criminals have adapted to the pandemic and are using COVID-19 as a cover to trick people into providing their information. Some areas have seen a 600% increase in the number of phishing scams involving COVID-19; attachments, links to websites and other methods are being used to lure victims.

Fraudsters will be able to get their hands on vast amounts of consumer information, which they won't use in the next few weeks. Rather, they'll wait six to 18 months before opening up accounts, taking out financial products and acquiring products from telecommunications carriers.

Since banks and telecommunications carriers are federally regulated, lawmakers need to be aware of these risks. Much of the focus is on the company's responsibility to protect the data entrusted to it. I think, though, the focus should be on accountability and the responsibility companies have in relation to the information they use to deliver services. When a bank's system is hacked and client information is stolen, it calls into question the bank's responsibility, which is protecting that information. No one asks about what will happen to the information once it's collected. There's a huge accountability gap.

● (1525)

I would be happy to answer any questions you have on the subject.

The Chair: Thank you, Mr. Marchand.

[*English*]

We will go back to Mr. Jones, who has been able to reconnect with us.

Mr. Jones, you had about a minute left in your testimony. I'm not quite sure where you cut out, but we'll let you take the floor again.

Mr. Scott Jones: I've been alerted to where I was. Thank you. I'm sorry about that. Technology affects us all.

In coordination with our industry partners and the international work of cybersecurity organizations, we have contributed to removing of fraudulent sites, and I talked about the protection of the CERB, the Canadian emergency response benefit.

Cyber-attackers are now looking to exploit teleworking connections because so many people are now working outside of their organization's traditional IT security perimeters. In response, the cyber centre has partnered with the Canadian Internet Registration Authority, or CIRA as you've heard, to create and launch CIRA's Canadian Shield. This is a free DNS firewall service that will provide online privacy and security to Canadians. CIRA has shown tremendous leadership in giving Canadians an option to better protect themselves online, and I thank them for their partnership.

To further protect Canadians, the next important step we've taken is informing Canadians about cybersecurity matters. Through targeted advice and guidance, the cyber centre is helping to protect Canadians' cybersecurity interests. We shared cybersecurity tips on video teleconferencing tools and telework to help inform and educate Canadians about how to stay safe online, particularly while many of us are working from home.

The cyber centre has created a collection of advice and guidance products, many of which are now more relevant than ever. I encourage Canadians to visit our website to learn more about our specific guidelines and best practices that can be applied to protect yourself from cyber threats.

Finally, it is important to note that the Government of Canada has a strong and valuable relationship with our international cyber partners. We regularly share information, which has a significant impact on protecting our respective countries' safety and security. CSE and the cyber centre are working to address cyber threats facing Canadians during these times; however, cybersecurity is everyone's responsibility and will take all of our expertise to protect Canada and Canadians.

Thank you again for the opportunity to appear before you today, and thank you for your patience with technology. I am pleased to answer any questions you may have.

The Chair: Thank you so much, Mr. Jones. Thank you for being able to get back on this call.

We'll go next to the RCMP, and then back to Mr. Holland.

With that, I turn the mike over to the RCMP. You have five minutes.

Assistant Commissioner Eric Slinn (Assistant Commissioner, Federal Policing Criminal Operations, Royal Canadian Mounted Police): Good afternoon.

[*Translation*]

Thank you, Madam Chair.

It is a pleasure to appear before this committee as part of its study on the Canadian response to the COVID-19 pandemic.

Appearing with me today is Sergeant Guy Paul Larocque, who has a leading role in managing the Canadian Anti-Fraud Centre, or CAFC.

[*English*]

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. In the face of the COVID-19 pandemic, our work with public and private partners in Canada and around the world in combatting and preventing fraud have only become more important. This shared responsibility speaks to the trust Canadians place in the RCMP to keep them safe and provide an effective and timely response to the COVID-19 pandemic.

As the measures to contain the crisis continue, the strain on Canadians and the institutions that serve the country will only deepen. Criminals will seek to exploit vulnerabilities in the system, as well as in Canadians themselves, as we have unfortunately witnessed. We must be diligent in combatting attempts to victimize the most vulnerable by those who prey on Canadians' fears and uncertainty around the pandemic. To be clear, criminals are actively exploiting fear, uncertainty and doubt around the COVID-19 pandemic. We know this because the CAFC has seen a dramatic increase in reporting on fraud from January to April when compared with the same period last year.

Since March 2020, we have seen almost 1,000 complaints of fraud related to COVID-19. Most of these are phishing attempts, where criminals will seek to gain personal information through emails or text messages pretending to be linked to Canada emergency response benefit claims, or attempts to install malware on victims' devices. However, the biggest monetary losses stem from the fraudulent sale of goods related to COVID-19, such as masks, testing equipment or miracle cures.

While we've seen a large number of COVID-19-related fraud reports, criminals continue to use traditional scams and frauds to exploit Canadians. These frauds take a terrible toll on Canadians. For example, estimates of fraud against seniors last year were over $700 million. These types of fraud have grown during the pandemic as these heartless criminal groups continue to target human and institutional vulnerabilities. Finally, organized crime groups are attempting to defraud the government and undermine efforts to get financial aid into the hands of those who are genuinely in need of aid. The escalation of fraud activity related to COVID-19, as well as traditional fraud, really shows the ability of criminal groups to adapt to and exploit these circumstances for personal gain.

In direct response to the frauds committed in relation to COVID-19, the RCMP have enhanced intelligence enforcement efforts toward this illegal activity as we recognize, more than ever, that at all levels of policing the RCMP have a significant role to play. To coordinate the RCMP response, in March we began running a program specific to COVID-19-related fraud. Coordination efforts are under way at national headquarters, while intelligence analysis and statistical gathering, as well as outreach, are done by the CAFC. Disruption and enforcement are conducted by members in the divisions, who also have the responsibility of liaising with the police of jurisdiction to further coordinate responses at the local level.

In recognition of the shared responsibility between public and private agencies to combat fraud, the RCMP are working collaboratively with key partners and stakeholders, domestically and internationally, to exchange intelligence and coordinate enforcement efforts as they relate to the pandemic. While the initial focus was on online frauds, this has quickly expanded to cover all fraud and criminality with a nexus to COVID-19 to better ensure public safety.

A crucial component in the fight against fraud is prevention, as these fraudsters and their operations are so pervasive, insidious and profitable that relying on enforcement alone is like pulling weeds. As my grandmother often relayed, an ounce of prevention is worth a pound of cure. Continually enhancing public awareness is a vital tool in the prevention strategy that must continue. As you may recall from our last appearance before the committee, the RCMP have operated the CAFC in partnership with the Competition Bureau of Canada and the Ontario Provincial Police since 2005. This centre has been a leader in prevention initiatives, including being extremely active on a variety of media platforms to communicate with Canadians.

As well as operating the CAFC, the RCMP maintain a federal policing prevention and engagement unit. This unit plays a key role in coordinating meetings with multiple police agencies, Government of Canada agencies, private sector vendors and financial institutions from across Canada.

● (1530)

With that, I will cease. I could probably go on, but there are other people who want to talk.

I look forward to your questions.

[*Translation*]

Thank you very much.

[*English*]

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

With this, we'll move back to Mr. Holland.

I'll ask him if he could start over with his testimony and speak closer to the microphone, because there is a whistling sound in the background.

Mr. Byron Holland: I have changed my mike and headset. Hopefully, that will be better.

Madam Chair, thank you for the opportunity to present yet again. I will start at the beginning, as you've asked, to make sure that the folks who were not able to hear can.

My name is Byron Holland. I'm the president and CEO of the Canadian Internet Registration Authority. Our primary mission is the operation of a safe, stable and secure .ca domain name registry.

We are recognized as a global leader in our space. In fact, many other countries leverage our infrastructure, services and knowledge for their own domain name registries. Our technology is considered best in class among our peers. In short, CIRA is fully equipped to navigate the COVID-19 crisis. We are confident in our ability to protect the integrity of .ca.

To date, we have tracked just over 2,000 .ca domain names with COVID-19-related keywords. For context, we've added more than 200,000 .ca domain names since the beginning of the year. This is aligned with what we are seeing from our peers around the world where COVID-19-related domains make up less than 1% of total registrations. However, it is also important to note that many of these domains are perfectly legitimate, and even positive, such as conquercovid.ca, a campaign to support first responders.

We scrutinize all COVID-19-related domain names carefully to make sure that they comply with our rules, particularly our Canadian presence requirements. We are also working with our global domain name community, including organizations such as the Council of European National Top-Level Domain Registries, to ensure that we are aligned with best global practices.

However, it's important to note that it is not within CIRA's mandate to review or authenticate the content of .ca websites, nor would such authentication be effective, as the Internet and related threats are truly global. While .ca domains are bound by Canadian law, there are thousands of other threats that come in from outside our borders. There are well-established existing tools and processes in place to deal with online fraud and cyber-attacks. If Canadians come across any domain names that they suspect are being used fraudulently or maliciously, they can contact the Canadian Anti-Fraud Centre or as we've heard, the Canadian Centre for Cyber Security. We work closely with both organizations.

When it comes to fraud on the Internet, it's important to remember that hackers love a good crisis. While technical solutions form an important barrier to online fraud, the biggest attack vector is human frailty, which cyber-thieves exploit. Unfortunately, the current pandemic has provided these criminals with an atmosphere of heightened anxiety in which to operate and has simultaneously forced most Canadians to work, learn, teach and socialize from their home networks and personal devices, most of which are not equipped with enterprise-grade security.

It is in this environment that we've launched CIRA Canadian Shield, a free security and privacy solution for all Canadians and their families. We've done this, as you heard, in partnership with the Canadian Centre for Cyber Security. We currently protect more than 50,000 Canadians, with a growing user base. Canadian Shield reflects CIRA's commitment to build a trusted Internet for Canadians, and we look forward to providing the opportunity to protect every Canadian with this free service.

We also help protect Canada's hospitals, schools, universities and municipalities through our enterprise cybersecurity service, CIRA's DNS Firewall. We have more than 1.1 million users, who include students, teachers, doctors, municipal workers and first responders across Canada. We are providing this service free of charge to all Canadian health care facilities and small businesses until September, hopefully when this crisis will be starting to recede.

Finally, the most important factor in protecting Canadians from fraud on the Internet is knowledge. Much like how your parents taught you to look both ways when crossing the street, Canadians need street smarts on the Internet to be able to identify fraud, fake news, misinformation and scams. The best way to do that is through awareness and education.

At CIRA, we have partnered with Beauceron Security, a great New Brunswick success story, to launch CIRA cybersecurity awareness training, a platform that provides education, benchmarking and ongoing testing to ensure employees have the most up-to-date cybersecurity street smarts. We have also launched a free cybersecurity course, Cybersecurity for Remote Workers, to help the thousands of Canadians now working from home to keep themselves and their organizations safe from cyber threats.

● (1535)

Everything I've mentioned so far represents elements of Canada's leadership, innovation and expertise in the area of cybersecurity. However, as Canada and the world enter an era when the Internet is proving to be the lifeboat for the global economy, we believe Canada must do more to be a global leader in cybersecurity. We would encourage the Government of Canada to dedicate more funding to cybersecurity research, solutions and platforms to protect Canadians and ensure the security of our digital economy. Only through investment can we ensure Canadians have the education, tools and platforms to protect themselves and their businesses from online fraud and malware.

There is no silver bullet. The threat landscape is constantly evolving, and our cybersecurity awareness and technology must keep pace. At CIRA, we're eager to help any way we can.

Thank you for your time.

● (1540)

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

With that, we will move into our rounds of questions. In our first round, the questions are for six minutes and our first MP is MP Motz.

Welcome to INDU. You have the floor for six minutes.

Mr. Glen Motz: Thank you very much, Madam Chair.

Witnesses, thank you for your great introduction to this topic today.

I'm going to focus primarily in this round on Mr. Jones and the Communications Security Establishment.

If I heard you correctly in your opening remarks, as you advise on cyber-related attacks and frauds, you have been advising the government on foreign attacks and areas of cyber-related concerns throughout this COVID pandemic.

Mr. Scott Jones: Yes, that is correct, absolutely. We continue to advise on all aspects, although the majority of activity we have seen is related to cybercrime.

Mr. Glen Motz: When there is a cyber intrusion, do you know off the top whether it's fraud related, cyber espionage, corporate espionage, a random attack or another purpose?

Mr. Scott Jones: Typically, when there is a report of some type of breach, our first action is to really look at how we can somehow do containment versus some type of attribution, meaning looking for the actor behind it. We always assume that it's the most sophisticated actor possible and that the actor is looking to take information or implement some type of advanced technique, but the fact is that almost every compromise we've seen or every incident we've seen reported is related to cybercrime right now.

We look first to contain, to help the victim make sure they're able to lock down their defences, improve their security, take action to prevent that adversary from spreading throughout their network, then work back from that and engage the right organizations, such as law enforcement, or our partners in the Canadian Security Intelligence Service if it is a foreign actor, and then, of course, CSE's own foreign intelligence mandate as well.

Mr. Glen Motz: Right.

Attacks on our front-line health workers could be designed to steal information, to sell personal information or to facilitate fraud. Has CSE been called in to deal with any of these intrusions or attacks on our health care institutions and front-line health care workers since the pandemic began? If so, how many times?

Mr. Scott Jones: There have been instances of cyber-incidents in health care-related fields, research and development organizations. We've intervened in a small number in terms of responding to the incident and giving advice and guidance.

The majority of our activity, though, has been focused on trying to provide information in advance, alerting to vulnerabilities, for example, that are growing or being announced, so that health care organizations can take proactive action. We really try to get information out about what an actor is doing to protect organizations in advance. We really are trying to be proactive in preventing any breach.

Mr. Glen Motz: Good.

Has CSE been called in to deal with any attacks on our own government's research into COVID vaccines?

Mr. Scott Jones: The Government of Canada defences are something that we have integrated into the ongoing operations. The way the government has been able to layer its defences over the last decade as we've built them out, it really is to proactively stop any malicious activity. There haven't been any breaches of the government, because our defences are layered in such a way that it is heavily protected.

Mr. Glen Motz: To reiterate what you just said, we have had attacks but there has been no intrusion, which is good to hear.

What's their intent in these attacks? Is it to take intellectual property or is it to gain economic opportunity? What is your assessment of that?

Mr. Scott Jones: Our assessment with regard to cybercriminals is that it really is about financial gain. They're looking to see what they can leverage. If you're looking at nation-states, we are seeing that everybody is trying to understand what's happening in the world. This is something that we've become alerted to, that there's a general increase in nation-state interest around these topics.

Mr. Glen Motz: Okay.

● (1545)

Mr. Scott Jones: Then, of course, we've seen that targeting Canadian industry intellectual property has been an ongoing activity.

Mr. Glen Motz: You commented that obviously intrusions into research have occurred. Do you recall back in 2014 the cyber-threat that occurred inside the systems of the National Research Council? It resulted in a complete shutdown of their entire network and, in fact, it had to be entirely replaced right down to the wiring. This intrusion is said to have cost in excess of $100 million to remedy. Do you think the motive behind that was fraud as well or some other purpose?

Mr. Scott Jones: We assessed that the National Research Council breach was very much focused on intellectual property theft.

Mr. Glen Motz: You guys were involved in that investigation. Did you also help secure the new network?

Mr. Scott Jones: We absolutely did both.

Mr. Glen Motz: Okay, good.

The government of the day pointed the finger at Chinese-state-sponsored actors. Would that be correct in your assessment?

Mr. Scott Jones: That was the statement given by the government at the time.

Mr. Glen Motz: Okay, so now, moving forward, was your organization, Mr. Jones, as an adviser on cybersecurity and computer security, consulted on the new partnership agreement between the National Research Council, the Chinese-owned CanSino Biologics and the Chinese Academy of Military Medical Sciences for the development of the new COVID vaccine?

Mr. Scott Jones: We are regularly working with the research partners across the government, including all of the health sector, to make sure that we're providing the most up-to-date cybersecurity advice so that defences continue to be right at the cutting edge.

Mr. Glen Motz: Okay, so you were involved in that particular agreement.

Mr. Scott Jones: We've been involved in working on all matters of cybersecurity with the research areas.

Mr. Glen Motz: Thank you very much.

The Chair: Thank you very much.

Our next round of questions goes to MP Jowhari.

You have six minutes

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

Thank you to all of our witnesses for coming in and providing a lot of helpful information.

I'm going to start with CIRA.

Mr. Holland, you've indicated that roughly 2,000 .ca domains have been registered since the start of COVID-19. Can you share some statistics around the following: How many of them have been registered within Canada? Is it possible to register a domain from outside of Canada, and if so, how many have been registered? Also, with regard to these 2,000, you mentioned that most of them are legit. How many of them have you found to be not legit?

Mr. Byron Holland: There's an important policy we have in place, which I think merits attention vis-à-vis your question, and that's our Canadian presence requirements. All .ca domain names must be registered by somebody or an organization with a legal tie to Canada, and so every single domain name is bound to Canadian legal jurisdiction and Canadian law.

In terms of the domain names that have been registered with COVID-related terms—and we use a fairly wide search when we do that to make sure we capture them—we've had, as I mentioned, just over 2,000.

I'm going to ask our corporate counsel, Albert Chang, who's also here, to comment regarding some of the specifics in terms of the reviews we've done that have turned up suspect domain names.

Albert.

Mr. Albert Chang (Corporate Counsel, Canadian Internet Registration Authority): As Byron mentioned, we do a daily review of all the COVID-19-related domain name registrations, and the specific terms that we're looking at are “COVID”, “coronavirus” and “pandemic”. To date, since January, we have seen 2,000 of these COVID-19-related domain names. We do a review every day, and it's 2,041 as of yesterday.

Out of these 2,000 domain names, we've identified only 20 that do not have a Canadian address. Under an autoprocess called the registrant information validation process, we email those individuals, those domain name holders, and ask them to confirm their identity and to confirm that they meet CIRA's Canadian presence requirements. In circumstances—

Mr. Majid Jowhari: So roughly 21 out of the 2,000 did not pass your test?

Mr. Albert Chang: That's correct.

Mr. Majid Jowhari: Once you identify that, what is the next step? How do you inform the registrant that they're not allowed to operate? Also, how is an individual who is now trying to access the .ca domain informed that it is a fraudulent domain?

Mr. Albert Chang: That's a great question.

We have an audit process, the registrant information validation process, or RIV for short. What we do in those instances is send an email to the domain name holder asking them to confirm that they meet CIRA's Canadian presence requirements and that they confirm their identity. In circumstances where they don't respond or they can't show they meet CIRA's Canadian presence requirements, we suspend the domain name, which means that the website will be taken down. Ultimately, we delete the domain name.

Mr. Majid Jowhari: That's the proactive part that CSE also mentioned, but before it even gets into the Canadian domain is it already stopped, so it's not going to impact?

Mr. Albert Chang: That's correct. I would also note that to date we have not received any complaints at all with respect to any COVID-19-related websites on a .ca domain name.

● (1550)

Mr. Majid Jowhari: Do you work with CSE to inform them that such an organization was attempting to create a domain? How often do you have that communication with CSE?

Mr. Albert Chang: We collaborate regularly with CCCS, but in terms of instances of one-offs, I don't believe we communicate each domain name to them individually.

Mr. Majid Jowhari: Where do you publish your results?

Mr. Albert Chang: In terms of the domain names that are not—

Mr. Majid Jowhari: Yes.

Mr. Albert Chang: Those are not made public.

Mr. Majid Jowhari: Those are not made public.

Mr. Albert Chang: That's correct.

Mr. Majid Jowhari: Okay. Let me move to CSE.

Mr. Jones, I was reviewing the Library of Parliament notes, which indicate that the “effectiveness of CIRA's technology relies on intelligence provided by the Communications Security Establishment's CCCS”. Can you shed some light on the technology you're referring to?

Mr. Scott Jones: From our perspective, we're one intelligence thread that is fed into CIRA. I'll let our colleagues at CIRA talk about the broader approaches, but our feed comes from our defence of the Government of Canada. As we see attacks or compromises happening, such as, for example, spam emails being sent to us or attempts to defraud the government, etc., we share those indicators regularly with our partners, including CIRA.

In CIRA's case, then, with Canadian Shield, they're able to take those and put those to block, so that even if a Canadian were to click on the link they wouldn't be able to get to the bad or malicious site. That's an advantage. We do that same level of defence on the Government of Canada as well, but that's where we get the information from. It's really from our defence of a coast to coast to coast and global network. We try to feed that into our partners at CIRA to make sure Canadians are protected.

Mr. Majid Jowhari: I believe my time is over. Thank you, Madam Chair.

The Chair: Thank you very much.

Our next round of questions goes to MP Lemire.

[*Translation*]

Mr. Lemire, you may go ahead for six minutes.

Mr. Sébastien Lemire: Thank you, Madam Chair.

I'd like to start by recognizing Mr. Masse's contribution; he's been making us more aware of the issue for quite some time. Thanks to him, it's on our radar and we are learning more about it. As a member of Parliament, I think it's incumbent upon us to act to better protect our constituents.

I'd like to follow up on Mr. Marchand's comments. One thing he mentioned was that, as people's socio-economic conditions worsen, external attacks become much more frequent. He referred to a 600% increase. What's more, he said information that's stolen isn't used immediately; that tends to happen down the road, within approximately 18 months.

Mr. Marchand, you said there was an accountability gap because the current state of affairs makes it easier to open fraudulent accounts and carry on criminal activity. Can you tell us, in concrete terms, how that's problematic and how companies could be held accountable?

Mr. Simon Marchand: Thank you, Mr. Lemire.

To start, I'll provide some clarity around the 600%. It refers to the increase in the number of attacks involving COVID-19 during this very specific period of time, not necessarily to the increase tied to economic factors. Naturally, during times of economic crisis, the number of scams goes up. The percentages vary.

That said, the lack of accountability in federally regulated companies is problematic in that all the current legislation—think of the Personal Information Protection and Electronic Documents Act, for example—forces companies to disclose that they were hacked and data was compromised. In Canada, however, we don't have an overall sense of how many people fall victim to identity theft once their information is stolen. Since banks and telecommunications carriers are federally regulated, they are making crimes involving one another easier to commit. In other words, much of the credibility for an identity is based on the fact that the individual has a cell phone account or bank account. These companies have tremendous amounts of sensitive information at their disposal, so once a hacker gets in, they can commit more and more fraud.

I have over a decade of experience in prevention, and I work with the fraud prevention teams in those companies. I can tell you that a bank's or telecommunications carrier's prevention team is under no obligation to disclose how many fraudulent accounts were opened daily or annually. They don't even have to contact or identify identity theft victims. That means you may have been the victim of identity theft, that your identity may have been used to open an account with a telecommunications carrier, for instance. The team in charge of fraud was able to detect the fraudulent use of a person's identity and reverse the transaction, but it doesn't have to notify the individual, in other words, the consumer. Consumers are completely clueless. No one has any idea when their identity has been used. The person can't take further steps to protect themselves in the future. That lack of accountability prevents the government from taking clear action to regulate the process of identifying or authenticating people who open bank or cell phone accounts.

● (1555)

Mr. Sébastien Lemire: Mr. Marchand, I gather that the Canadian Anti-Fraud Centre must be informed of this type of situation, for example.

For a company, what are the advantages and disadvantages of strong accountability when it comes to fraud? We know the advantages and disadvantages for individuals and for the public, but what about for companies?

Mr. Simon Marchand: The primary benefit of accountability is that it gives the government a clear picture of the situation. This makes it possible to determine the exact number of victims and to guide the steps needed to strengthen security measures in banks and telecommunications companies.

This certainly imposes a burden on the companies that must submit reports. However, I don't think that this burden is excessive, since the work has already been done. The data is already known. The data simply needs to be passed on to the legislator, to an organization overseen by the government. This organization could present the data on a broader and more anonymous basis so that the members of Parliament can access the information and know exactly what's happening in Canada.

Mr. Sébastien Lemire: I now have a question for Mr. Fortin from the Autorité des marchés financiers.

Mr. Fortin, what do you think of the potential requirement for companies to inform the anti-fraud centre of situations involving fraud?

Mr. Jean-François Fortin: Thank you for your question, Mr. Lemire.

This issue doesn't necessarily fall within our jurisdiction. We're a law enforcement agency. I would still say that it's a good idea. I don't know what would be legally feasible. I was listening to you speak earlier and I was thinking that the methods used to prevent fraud obviously include education and transparency. This is a key component.

In this type of situation, the question that you asked Mr. Marchand about informing people who have been victims of identity theft or whose information may be used by third parties could be a good way to prevent fraud.

Mr. Sébastien Lemire: My last question is for the representative of the Royal Canadian Mounted Police.

Would the requirement for companies to provide much stronger accountability help you with your work, if the legislation were amended, for example?

[*English*]

A/Commr Eric Slinn: It's a difficult question to answer. A lot of companies want to protect the integrity of their systems and all that kind of stuff, so they're apprehensive about coming forward sometimes.

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

Our next round of questions, for six-minutes, goes to MP Masse.

The floor is yours.

Mr. Brian Masse: Thank you, Madam Chair.

I want to thank the witnesses, and you, Madam Chair, and the other committee members, for continuing this work. I appreciate it very much.

One of the things that struck me in the testimony we had, which was excellent, is that we rely on social media, including Facebook, to investigate and promote how to protect ourselves against fraud. However, recently Facebook was found guilty and paid a $9-million fine for misleading Canadians. In fact, it was said that it made "false or misleading claims about the privacy of Canadians' personal information." Yet, we are spending tens of millions of dollars of government money to advertise on its platform.

I'll start with Mr. Marchand, because he may have a bit of perspective on the United States.

With regard to fraud from companies, Volkswagen had a U.S. settlement of $14.7 billion. In Canada, the Competition Bureau fined it $2.5 million. Equifax had a settlement of $600 million in the United States; Canada had a Competition Bureau fine of zero dollars. Most recently, Facebook had a $5-million fine in the United States, and in Canada, a $9.5-million fine.

I view the Competition Bureau, the Privacy Commissioner and the CRTC as important instruments in protecting Canadians from fraud. It seems that they might be a bit outdated with regard to their powers.

Can you comment as to whether there is a misalignment between our penalties in Canada and those in the United States that perhaps can create a problem for bringing accountability even with fraud by so-called corporate entities?

● (1600)

The Chair: Mr. Marchand.

[*Translation*]

Mr. Simon Marchand: Thank you for the question.

I think that the issue isn't so much the misalignment but the lack of any perceived real risk of a fee or a penalty. Fees are charged for the failure to disclose a leak of important information. However, there must also be a perceived real risk of a penalty. This is missing here.

In some cases, the risk of having to pay fees is considered the cost of doing business. In my opinion, this isn't a sound or even ethical approach to risk management. The regulatory bodies currently lack teeth. This may be the issue.

[*English*]

Mr. Brian Masse: You're correct. The cost of doing business is one of the reasons we fought to get rid of the use of environmental fines and penalties as tax deductions. Corporate fines and penalties used to be tax deductible in this country, which is something we worked on for a long period of time. Good companies were being penalized by bad ones using it as a loss leader.

I'm going to move on to Mr. Holland.

With regard to the good work you're doing at CIRA, the one thing I noted is that there seems to be no review. I was under the impression that with the sites you authorize, .ca would be a gold standard in many respects, and perhaps it still is. If they abuse it, does a review take place? If somebody has been registered with you and three months or six months or a year later we find they are doing illegitimate business with a domain name that may have gone through you in a legitimate way but later on was altered in terms of business practice—almost like a Trojan horse—what happens?

Mr. Byron Holland: That's a good question.

There's always a delicate balance for organizations like ours, because fundamentally we are a technical organization. We operate the infrastructure; we don't monitor what transpires on the infrastructure. That's certainly not our mandate.

In no way do I mean to skate out from under the responsibility, but we're a technical operator and not a content administrator. There are rules and regulations in terms of Canadian presence and behaviour; however, we are not proactively monitoring the content.

Mr. Brian Masse: I appreciate this, and I don't expect you to do something you're not supposed to do right now. I just assumed, perhaps naively and, I think, like many Canadians, that .ca is like a gold protected standard, especially since our government uses it. I use it for my site, and I would think that we would ban, fine or blacklist anybody misappropriating that at any point in history if we want to end fraud.

If there were proper resources, would that be something that your agency should do, or should it be another agency? I feel pretty strongly that if we're going to use the .ca brand, that's one where we could control fraud and also bring some accountability.

Would that be done using your organization's resources, or should it be done by somebody else, a third party?

Mr. Byron Holland: Given that we are a technical organization, my sense is that the oversight of content would be better placed in other organizations that are specifically set up to do that, whether law enforcement or even the CRTC. We are a gold standard in the global community that operates the technical functions of the Internet, and, to a great degree, that's because of some of our rules but also understanding the limits of our remit.

● (1605)

Mr. Brian Masse: Thank you, Madam Chair.

The Chair: Thank you very much.

Our next round of questions will go to MP Motz.

You have five minutes.

Mr. Glen Motz: Thank you, Madam Chair.

Mr. Masse, I appreciate that line of questioning. I think it's certainly an issue that we need to get some resolution on in the very near future.

I want to go back to Mr. Jones just for a quick minute before I connect with my friends from the RCMP.

I appreciate your comments that you were involved in this latest collaboration on the vaccine. I'm curious; are these the types of partnerships, the kinds of things we would be worried about in terms of stealing intellectual property and espionage?

Mr. Scott Jones: When we are working with any government department, it is primarily so that they are aware of the possible risks that come with any sort of activity online. The one truism is that no matter what technology you use, it always comes with risks.

We really do try to work proactively to figure out and understand what's happening, so that we can, first of all, understand the activity and make sure our defences are aimed toward that, but also give the advice that we would have so that they can take action to protect themselves.

Mr. Glen Motz: Thank you.

Has there been any observable decline or increase in intrusions and attacks from certain countries as a result of the pandemic-related lockdown coming into effect, and if so, which countries?

Mr. Scott Jones: We really haven't seen a change in the cybersecurity environment. We have seen a shift in themes towards those related to COVID, but the level of activities has remained pretty constant around all aspects of cybersecurity.

Mr. Glen Motz: During this pandemic, have you invoked a request for proactive measures to stop or mitigate cyber-fraud in Canada?

Mr. Scott Jones: We work with partners around the world, including commercial partners. If we do see, for example, the Government of Canada's websites being impersonated, we ask for those to be taken down.

We'd also work with our law enforcement partners if we thought there was a criminality element to that, of course, and we collaborate closely with the cybercrime coordination unit under the RCMP.

Mr. Glen Motz: Thank you, Mr. Jones.

I want to move on to my friends from the RCMP before my time is up.

Specifically to the Canadian Anti-Fraud Centre, have you seen an increase in fraud? I think you said in your opening remarks that you have seen an increase related to the pandemic.

A/Commr Eric Slinn: We have.

Mr. Glen Motz: Is your team fully staffed and able to appropriately manage and respond to the increase you're seeing?

A/Commr Eric Slinn: Ironically, when the pandemic broke we, like many organizations, pushed our people home into a teleworking environment. Actually, it was quite seamless in that regard, in that they were able to get their computers and take complaints from complainants, so I don't think we've really been impacted greatly. We always welcome more resources for analytical work and proactive work, but our work has been pretty seamless in that respect.

Mr. Glen Motz: As you know, you guys at the Canadian Anti-Fraud Centre are kind of at the brunt end of the spear with respect to a lot of the major fraud investigation that occurs. Do you have vacancies in your group? Are you able to respond appropriately to all fraud, especially the larger fraud, that you are responsible for investigating?

A/Commr Eric Slinn: I think it's important to recognize that CAFC is really a collection area. It is not an active investigative group. It does some analytical work to see where trends are developing, to see new scams that are coming on the horizon, and it does an excellent job of that, but then it pushes out the relevant information to the policing jurisdiction, whether that be the RCMP or some other agency.

It is just facilitating, taking that initial complaint, doing some initial analysis and then pushing it out in an investigation.

Mr. Glen Motz: In your assessment, based on the information you guys are gathering and what you're seeing through this COVID, are doctors, nurses or front-line health care workers a top target of fraud or cyber-attacks during this pandemic?

A/Commr Eric Slinn: I don't know that I can say that.

Guy Paul, are you in a position to answer that?

● (1610)

Mr. Guy Paul Larocque (Acting Inspector, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police): I'm not sure if we know specifically at the Anti-Fraud Centre if a specific group of people in the population is being targeted. What we see is that fraud typically targets many people. Fraud doesn't have any discrimination. Everybody can be a potential victim at one point in time.

Mr. Glen Motz: We've seen it reported that a darknet hacker named Julius stole 1.4 million names.

I'm sorry, Madam Chair. I didn't see you waving your red flag at me.

The Chair: My apologies. I'm sorry to cut you off, MP Motz.

Our next round of questions goes to MP Lambropoulos.

You have five minutes.

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

I'd like to thank all the witnesses for being here today.

With regard to COVID-19, people are obviously taking advantage of the fear and the vulnerability of Canadians at the moment. They're doing whatever they can to take advantage of the situation, as they would under normal circumstances, but this is obviously a new angle that they can use.

Given the fact that we're going to be in this situation for at least several months to a year or a couple of years, what are some of the strategies that you think we can use moving forward in order to prevent such crimes from continuing to happen in the future?

That's a general question for whoever would like to answer it.

A/Commr Eric Slinn: On behalf of the RCMP, I touched on this in my opening statement. An ounce of prevention is worth a pound of cure. I don't think you can do enough prevention. Many of my colleagues who are witnesses here have talked about informing the public and letting them know what these scams are.

Because a lot of these threat actors are actually outside of Canada, it's very difficult for enforcement. From a prevention standpoint, I don't think you can message enough, and that is a key part of our strategy. It's to make the public aware of new scams, getting it out on our website and getting it out through partners.

As I said, it's a shared responsibility. We all have a piece to play, but prevention is huge.

Ms. Emmanuella Lambropoulos: Thank you. I—

[*Translation*]

Mr. Jean-François Fortin: Madam Chair, I'd like to make a comment.

The Chair: We're listening.

Mr. Jean-François Fortin: Thank you.

I completely agree with what Mr. Slinn just said. In my view, awareness and education are very important. We take action with regard to investors, but in this case, we're talking to all Canadians. We must watch out for situations that appear fraudulent. People can be tempted by the lure of gain in some circumstances.

Some schemes involve promoting a person who has invented a miracle vaccine or a miracle drug, for example. The Royal Canadian Mounted Police is an investigative team, and so are we. We must first encourage people to take care to avoid falling for this type of fraudulent scheme. We try to reach out to seniors, who can be contacted by telephone or on social media. That's one of the major issues. Governments probably have a role to play in raising public awareness about this issue.

[*English*]

Ms. Emmanuella Lambropoulos: Thank you.

With regard to medicine, vaccines or antibody testing that people are going to want to see happen in the coming months, people obviously will be taking advantage of this.

We've seen examples of it in Montreal already, where companies have put out ads for these types of tests, and we know that they weren't approved by Health Canada. What is done in circumstances like these in order to help protect Canadians once it's found out that people—a lab, let's say— are taking part in this type of criminal activity?

[*Translation*]

My question is for Mr. Fortin.

Mr. Jean-François Fortin: Could you repeat the question, please?

Ms. Emmanuella Lambropoulos: How are Canadians being protected from companies, such as laboratories that create fake drugs and that aren't necessarily approved by Health Canada, once we know that the laboratories are engaged in this type of activity?

● (1615)

Mr. Jean-François Fortin: Your question has two components. One component is outside our jurisdiction.

If we were dealing with pure fraud involving other criminal activities, we would then need to work with our police officer colleagues, such as the Royal Canadian Mounted Police or another agency.

If we see this type of promotion and the people involved intend to take money from investors, for example, in a situation where someone has invented or found a vaccine or a drug, we can take action in order to stop the activities and prevent them from continuing. We can even obtain cease and desist orders to ensure that investors don't lose money. We have ways of taking action very quickly and preventing the fraud from continuing any longer.

Ms. Emmanuella Lambropoulos: Thank you.

The Chair: Thank you.

[*English*]

Our next round of questions goes to MP Van Popta.

You have five minutes.

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

My first question will be for Mr. Marchand.

Thank you for your testimony. Thank you for educating us on some of these important statistics.

You told us about increased identity theft associated with so many Canadians who are teleworking, as we are today. I think you mentioned a 600% increase in phishing. Again, thank you for that information. What do we, as legislators, do with that? Do you have any specific advice for what we as legislators can do to help you help Canadians better protect themselves?

[*Translation*]

Mr. Simon Marchand: Thank you for the question.

Perhaps we could look at two tools in the short term. The goal is to provide tools to companies that face these risks. Now that the fraudsters have access to the information, how can we equip banks and telecommunications companies with tools to prevent the fraudsters from successfully attacking them?

The STIR/SHAKEN standards are included in these tools. Of course, in my view, because the Americans will implement these standards quickly, we can expect fraudsters to come north of the border and to take advantage of a gap in Canada's legislation and regulations.

In my opinion, the STIR/SHAKEN standards are an essential tool because fraudsters use scooping to carry out certain types of identity fraud. This isn't just a matter of robocalls, but also a matter of identity theft.

As for the other tool, I think that the rules for identifying customers should be strengthened. Right now, a social insurance number, a driver's licence or a health insurance card is enough to open a bank account or a telephone account. These pieces of identification are outdated. We must start looking at the issue of digital identity and biometric identity.

Several countries have already transitioned to these higher levels of identification. To protect Canadians, we must consider whether some form of more advanced biometric identification should be required to open accounts.

[*English*]

Mr. Tako Van Popta: Thank you very much for that.

You mentioned STIR/SHAKEN. I know the CRTC has described STIR/SHAKEN as “the only viable authentication/verification solution that can provide consumers with a measure of additional trust in caller ID.”

Do you agree with that? Is that an accurate assessment?

Mr. Simon Marchand: I don't know if it's the only one, but it's a useful one, for sure.

I don't think we can afford not to have this additional layer of security and validation. We do not want to let fraudsters have that tool in their tool box when we can—not without difficulty—technically deploy that for ourselves to try to fight fraud. It's not the only one, but it's a tool that we should consider.

Mr. Tako Van Popta: Good. Thank you for that.

I believe the CRTC said this will be mandated for carriers later this year, September 2020, I think. Is that realistic?

[*Translation*]

Mr. Simon Marchand: Unfortunately, the issue with the STIR/SHAKEN standards is that the carriers don't believe that this deadline will be met. If I'm not mistaken, representatives of Rogers, Bell and Telus appeared before a House committee to request an extension of the deadline. I think that it's necessary to be firm and to require implementation as quickly as possible.

Canada's telecommunications networks are outdated. They won't make it possible to fully implement the STIR/SHAKEN standards. However, I don't think that this constitutes a reason to not begin implementation in the fall. It's just necessary to make sure that the pressure from the telecommunications lobby doesn't push the government to extend the deadline to 2021, which I think would be a mistake.

● (1620)

[*English*]

Mr. Tako Van Popta: Thank you.

Perhaps you could tell us a bit about the limitations associated with STIR/SHAKEN. For example, if spoof calls come from outside of Canada or outside of a STIR/SHAKEN protocol area, apparently the filter doesn't work.

[*Translation*]

Mr. Simon Marchand: Yes, absolutely.

That's the biggest limitation. This technology will apply only to calls from Canada and possibly the United States. All participating countries will benefit. However, not everything that comes from outside will be covered. However, when we know that a call doesn't have the STIR/SHAKEN certification, we know that it's a higher risk call and that we must pay attention to it.

[*English*]

The Chair: Thank you very much.

Our next round of questions goes to MP Ehsassi.

You have five minutes.

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

Thank you to the witnesses for appearing before our committee. I found the testimony very helpful.

My first question is for you, Mr. Jones. During your testimony, you were suggesting that one sector that should be highlighted for attention is the health care sector, given that there are many more cyber-attacks. However, approximately a month ago, the top authorities in the United Kingdom and the U.S. warned that universities are also incredibly vulnerable. Have you seen an uptick on cyber-attacks on universities? Would you agree with their assessment?

Mr. Scott Jones: Thank you for the question.

While I emphasized the health care sector, given the pandemic, we are actually working with and reaching out to every sector of critical infrastructure in the economy, including universities and the broader education sector as well. We rely on the reports of any sort of malicious cyber-activities. We try to proactively communicate anything that we're seeing from our defence of the government.

One of the things is that we don't watch Canadians. We don't watch what's happening on Canadian networks. We defend the government, and we rely on reporting.

We have certainly reached out to universities. We're providing proactive and tailored advice and guidance so they can take some measures to secure themselves, and we are also hoping to build a partnership where they will call us when they see an event or an incident so that we can work together.

Mr. Ali Ehsassi: Absolutely, but the reason I'm highlighting universities is that approximately three weeks ago there was a pretty elaborate cyber-attack on York University. Is that a trend? Are we going to see more of that?

Mr. Scott Jones: Whether it's a trend or not—we don't have enough information to determine that—we certainly do see that universities, due to their open nature and the rapid influx and departure of students, do have unique vulnerabilities. They are also emphasizing the open, collaborative nature of their network, which makes it harder to protect.

In trying to work with them to better defend, one of the things we have pointed them to is some of the work that CIRA is doing. It immediately offers a quick benefit for defence if you use the CIRA Canadian Shield, but there are the broader enterprise-grade services as well. While every Canadian can benefit, it's also something for universities. I think my colleague mentioned that at the beginning as well.

Mr. Ali Ehsassi: On the term you used when an organization actually contacts you, you said you "intervene". I presume that's a term of art, but what does that entail? What does intervention entail? Do you help them beef up their system? Do you trace where those attacks came from? What actions does your organization undertake?

Mr. Scott Jones: "Intervene" was probably a bit of a loose term. What we do depends upon what the organization is comfortable with and the type of cyber-incident. If it's traditional ransomware, we'll provide advice and guidance. We'll try to help them recover, best practices, etc. If it's a more advanced actor who is clearly hurting them, we might provide more tailored assistance, if it's a system of importance, for example. We'd certainly try to work with a commercial provider or a commercial partner who would be helping them rebuild their defences.

Then, finally, if it were something that required the intervention of the state, we would look to leverage some of the new authorities that were granted to CSE in terms of it going out and actually defending the organization, but that is something that we really do reserve for when it's unreasonable to expect the commercial sector to defend. In reality, what we really want is a vibrant commercial sector that is able to work and defend Canadian industry, so we really emphasize partnerships and the ability to work together.

● (1625)

Mr. Ali Ehsassi: Thank you.

Given all the advisory work you do and the counsel you provide to various organizations on a general basis, would it be fair to say that the guidance you are providing essentially establishes the standard of care from a legal standpoint as to whether organizations are actually adhering to best practices and insulating themselves from losses?

Mr. Scott Jones: Well, I'm an engineer and not a lawyer, so I'm not sure that I'm qualified to demonstrate the standard of care.

One of the things we have worked on with our colleagues in Innovation, Science and Economic Development is the cybersecure Canada program to provide baseline cybersecurity controls to help small and medium-sized organizations do things that are actually within reach. I think one of the failings of the commercial cybersecurity industry is that we talk about things that a multi-million dollar or a billion-dollar company can afford. We need things that Canadian small businesses can afford, and that's what this is really trying to achieve.

[*Translation*]

The Chair: Thank you.

[*English*]

Mr. Ali Ehsassi: I think I have about 20 seconds remaining.

The witness from—

The Chair: Actually, no. Unfortunately, you have no more time remaining. You went over.

[*Translation*]

I'll now give the floor to Ms. Gaudreau.

Ms. Gaudreau, you have the floor for two and a half minutes.

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Good afternoon. Thank you, Madam Chair.

I've heard many things that help me understand why people are concerned. The Privacy Commissioner has been telling us for some time now that we're seeing a crisis of confidence. There has been a great deal of talk about education as a form of prevention. He says that 90% of Canadians have lost confidence with regard to the misuse of their data. Moreover, 38% of Canadians believe that companies more or less respect their privacy rights.

That said, some potential measures were brought up earlier. Mr. Marchand pointed out that other countries had laws to crack down on companies. For example, a company that doesn't use the necessary tools to protect personal information is liable to a penalty equivalent to 4% of its sales.

Mr. Marchand, what do you think?

Mr. Simon Marchand: Thank you for the question.

Ultimately, I think that education is a good thing. People need to learn about the risks that they face when they're online and when they answer calls. In my opinion, the legislation is inadequate. However, the legislation does partly touch on the protection of data entrusted to a company with which people do business. However, an entire segment of the legislation is completely missing. In this case, the segment concerns the verification of what happens to the identity of the individual once they've made the mistake of providing their personal information or once this information has been stolen from them without their knowledge.

When this identity is used to obtain a credit card, open a bank account, engage in money laundering or anything of that nature, we shouldn't only look at the crime. We should also look at the fact that the crime facilitates global criminal activity on a larger scale, including human trafficking, drug trafficking or terrorist activities. I think that companies must be held accountable for this other aspect. Much stronger legislation must be implemented to protect people once their identity has fallen into the wrong hands.

Ms. Marie-Hélène Gaudreau: Okay.

The Chair: I'm sorry, your time is up.

Mr. Masse now has the floor.

[*English*]

You have two and a half minutes.

Mr. Brian Masse: Thank you, Madam Chair.

My question is for Mr. Slinn from the RCMP.

We have had cases in the past in which someone has paid out a ransom for a cyber-attack and loss of privacy. A good example is the University of Calgary. Under Canadian law, is there any obligation for a company or an institution to even acknowledge that they've paid out a ransom for a cyber-attack, or is that something that doesn't have to be disclosed?

● (1630)

A/Commr Eric Slinn: That's a good question. I'm not 100% sure on that. I do know that a lot of private companies are reticent to report a cyber-attack on their business, for obvious reasons. It may affect people's confidence in that business and the data that they hold. I don't know, to be candid, if there is a legal obligation for them to report that they paid a ransom. My initial thought is no, but I'm happy to see if I can find that answer for you.

Mr. Brian Masse: Maybe you can work with our researchers on it as well. They do some really good work for us.

I'd be interested to know that. That eventually did go public. It goes to what Mr. Marchand was saying with regard to not even having to report certain breaches.

Then you have cybercrime. With regard to ransom, do you know if there has been an increase? Is there a database created? I've found over the years that I only hear about these cases. I wonder if the RCMP has a log of those who have complied or voluntarily said they paid a ransom, and whether any of that—Mr. Jones might have a comment on this too—comes from state governments that are involved in some type of cyber-attack and attempts at ransom.

A/Commr Eric Slinn: We keep information on everything that's reported, but it's more like fraud against individuals. We know there's massive under-reporting, and the same is likely happening at the company level as well.

Mr. Brian Masse: Mr. Jones, do you have any comment with regard to other states, especially non-democratic governments, that might have been using some attempts to leverage...? Is that ever quantified or made public?

Mr. Scott Jones: Certainly the one thing about ransomware is that it is massively under-reported. We know that. When people do come forward, it tends to be on the cybercrime side of things. That is what we've seen.

We have reported and looked for other types of links, but it's predominantly cybercrime-focused, and it is absolutely under-reported.

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

The Chair: Thank you.

We now move to the third round. Our first question goes to MP Dreeshen.

You have five minutes.

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

Certainly it's interesting testimony that we've had here today.

Of course, on fraud being investigated, we have certain comments, even from the government, about whether or not they even want to investigate fraud at this particular point in time. I think that probably gives the criminal element an opportunity to jump in here as well, which is kind of frustrating.

I want to go back to something. At the end of March, the Communications Security Establishment noted that it had taken down a number of fraudulent websites that had spoofed the Public Health Agency of Canada, the Canada Revenue Agency and, most recently, the Canada Border Services Agency. We recently heard from General Vance, the country's chief of the defence staff, that he's seen indications that Canada's adversaries intend to exploit the mounting anxiety about the global pandemic.

To the RCMP, I'm wondering what form you believe these attacks will take. Which countries are we talking about, and are we taking steps now to deal with this?

A/Commr Eric Slinn: When it comes to the threat actors, they generally are in countries we've dealt with in the past. It doesn't have to be the COVID-19 pandemic. It can be a romance scam; it can be phishing.

There are certain individuals, certain countries, where this continues to plague us, if you will. We do our utmost to work with international partners, whether it be Five Eyes partners or other partners, to help disrupt some of those networks.

Mr. Earl Dreeshen: In August 2019, the RCMP told the media it had turned an investigation into CRA fraud calls to Canadians into a national priority, and that 39 so-called call centres in countries like India had been taken down, while 45 people overseas had been arrested. In February of this year, two Canadians connected with this fraud were also arrested.

What RCMP resources are currently being invested into this type of overseas fraud investigation? Are many of these COVID-19 fraud scams coming from overseas?

● (1635)

A/Commr Eric Slinn: On specific resources, I can't give you an exact amount of resources. However, I can tell you that, as the person responsible for federal policing criminal operations, I've issued a directive to all divisional CROPS to pivot—to use a pandemic term here—financial crime resources to COVID-19 frauds, which means greater intel collection and greater enforcement capacity. We recognize our obligation there, and we are trying to up our game. We will continue to work with those international partners.

I think the project you alluded to involving India was Project Octavia, in February. Those scams continue.

Mr. Earl Dreeshen: Thank you very much.

Madam Chair, could I give the remaining two minutes to Ms. Gray, please?

The Chair: Yes, absolutely.

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

My question is for Assistant Commissioner Slinn and Inspector Larocque. We know that COVID-19-related fraud calls and texts have become pervasive over the last few months in trying to defraud vulnerable Canadians, including seniors and new Canadians. We heard that from you today. At what point in this process would these calls be considered illegal?

A/Commr Eric Slinn: Because I'd probably talk too much, I'm going to pass the buck to Guy Paul.

Mr. Guy Paul Larocque: Thank you, sir.

Typically, once an attempt is made to reach out to a potential victim, the line has been crossed. It's virtually impossible to investigate every single case that comes in because of the massive amounts. As we explained earlier, we have many reports of fraud, but it's about being able to look at the totality. That's the benefit of people reporting an incident to that call centre. We're then able to see an overview and disseminate information to the proper law enforcement body or the proper partners to assist us in moving forward.

Mrs. Tracy Gray: Thank you.

You've already mentioned today that fraud is up, so what's being reported to the RCMP and the Canadian Anti-Fraud Centre? Would you have an estimate as to how many of these related calls might be from spoofed numbers? Do you have any estimation of that?

Mr. Guy Paul Larocque: No, not on the spoof numbers specifically. I have numbers on COVID-related fraud, which we starting saving since the beginning of March, and they say that the vast majority of the complaints we got were linked to text messages. Calls were third in terms of being reported.

Mrs. Tracy Gray: Okay. I understand—

The Chair: Unfortunately, MP Gray, that is all the time for that round.

Our next round of questions goes to MP Erskine-Smith.

You have the floor for five minutes.

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

I want to start with the Communications Security Establishment. Last week, U.S. intelligence suggested that organizations conducting research into COVID-19 may be targeted by computer hackers linked to the Chinese government. Do we have any evidence in Canada of that warning being a reality?

Mr. Scott Jones: We issued a joint statement with our colleagues at the Canadian Security Intelligence Service warning that Canadian organizations can expect to be targeted not only...but by different foreign actors as well. One of the things we really emphasize is the need to take proactive measures against any actor who could go after this type of activity or be interested in this type of information. I think it was actually the first time that we issued a joint statement with CSIS, and in that case, it was to bring attention to that.

Mr. Nathaniel Erskine-Smith: The warning there is about potential threats. Have any of those potential threats already been realized?

Mr. Scott Jones: Our goal is to really make sure we're getting information out so that people can protect themselves before it becomes an actual incident—

Mr. Nathaniel Erskine-Smith: Have we not had an incident yet?

Mr. Scott Jones: We've seen some compromises in research organizations, which we've been helping to mitigate. We're still continuing to look through what the root cause of those is.

Mr. Nathaniel Erskine-Smith: Do we have any evidence that any foreign actor has attempted a hack for COVID research?

Mr. Scott Jones: That's something that we'd have to look into and get back to you on. We really look to see how to block the activity before it becomes a compromise, regardless of who the actor is. We put our attention to anybody who is targeting these types of organizations, be they criminals, states or individual hackers from around the world.

Mr. Nathaniel Erskine-Smith: We have a warning from CSE and CSIS about the potential, it may have taken place and you're just not certain as of today.

● (1640)

Mr. Scott Jones: We continue to work with organizations, but one of the things that we don't do.... There's not a giant magnifying glass looking at Canada and the Internet activity. We don't direct our activities at Canadians, so we really do rely on a partnership and an engagement with colleagues in the private sector, in research and in other levels of government to really try to report this and put the picture together.

Mr. Nathaniel Erskine-Smith: Have any of those private sector or public sector actors come to you and said they've had an incident and they'd like your help looking into it?

Mr. Scott Jones: We have worked with some private sector actors. Whether or not it's related to COVID or the research and development type of activity remains to be seen, but we've been working with private sector actors ongoing. It increases as more people become aware of what we can provide and what work we can do together. Certainly, as we get more information out there about what's—

Mr. Nathaniel Erskine-Smith: On COVID specifically, though, have institutions or organizations come to you and told you they've been subject to an incident related to COVID research?

Mr. Scott Jones: Yes, we've seen activity coming from organizations that have seen malicious, or at least suspicious, activity. We're working with them to determine whether or not it was malicious, where it came from and if it was successful.

Mr. Nathaniel Erskine-Smith: Have there been any instances where you have been able to make a determination about the source of the hacking?

Mr. Scott Jones: We've turned that over to the intelligence side of the business to look at where it's coming from.

Mr. Nathaniel Erskine-Smith: I understand.

This question is for CSE and the RCMP.

We hear from constituents all the time about scams. The RCMP has tallied up that it costs individuals about $100 million a year overall for these scams, at least those that are reported. I would say they are under-reported, because people are embarrassed when they are taken advantage of. We hear about this all the time, and it's not just from seniors, although I've heard predominantly from seniors.

We've made significant investments in cybersecurity over the last number of years. You are the experts. Are there measures that other countries take that we do not? Are there measures, in your experience and estimation, the government could take to better strengthen our society against such fraud?

Mr. Scott Jones: I'll start and then turn it over to my colleagues in the RCMP.

The first thing we've done is we've really tried to give practical things that every Canadian can do that are within reach. That's something all countries are doing. We've tried to make this as accessible as possible through, say, Get Cyber Safe.

The second thing we've tried to do is to find partners who can give capability. CIRA is a great example of that. That's something every Canadian can look into that immediately raises the cybersecurity bar. The one thing with cybercriminals especially is that they go after the lowest bar. If it's not economically feasible, they're going to move on to the next target, so by doing—

Mr. Nathaniel Erskine-Smith: I appreciate all that—and I know I'm running out of time—but there would be nothing, in your estimation, that we could do as a government to improve your work.

Mr. Scott Jones: We're trying to leverage the mandate we have today. I think anything else would be a policy question that should probably be debated by you and the ministry.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you very much.

Our next round of questions will go to MP Gray.

You have the floor for five minutes.

Mrs. Tracy Gray: Thank you very much, Madam Chair.

This question will go to the assistant commissioner.

We've talked a bit about anti-fraud and spoofing. I'm wondering if there are some provisions in place for those who spoof their phone number, like, for example, telemarketers. Would you be able to confirm that caller-ID spoofing is still legal in Canada, even for those who might use it for malicious intent?

A/Commr Eric Slinn: I'm going to pass this off to Guy Paul because I think he deals with it more often, but spoofing does become difficult. Proving where a call was spoofed and the software that's available make it even more challenging.

Guy Paul, maybe you can add more to that.

Mr. Guy Paul Larocque: Thank you, sir.

As far as the method of solicitation goes, last year direct calls were the number one overall way Canadians were reached for frauds that were reported to us. It's reasonable to assume that most of those calls were spoofed.

The challenge with spoofing a number is that it's not illegal in the sense that there are applications out there for people to do it just to play pranks on people. The issue is when people use it to commit crimes like fraud. Then, of course, it's not the spoofing itself that's illegal. It's the actions taken by the scammers, like representing a government agency to extort money from Canadians.

● (1645)

Mrs. Tracy Gray: Would you say there are sufficient lines of communication right now during this time of the pandemic between the CRTC and the RCMP when it comes to tackling telephone fraud?

Mr. Guy Paul Larocque: We have frequent conference call meetings to discuss the issue. We've been in touch with our main partners pretty much on a weekly basis to discuss current trends and how the situation has evolved. I can say that we've been in contact very often with our close partners.

Mrs. Tracy Gray: Let's say, for example, a complaint comes in about a fraudulent call and it's received by the CRTC. You said you have weekly communication. Is there a quicker process that happens when something seems to be emerging or seems quite serious? Is there a more expedited protocol?

Mr. Guy Paul Larocque: Yes, there is. Those calls are mainly to discuss trends in intelligence that we can share with each other, but when there's something urgent or emerging we have protocols in place where we can share the information more rapidly. It's done within the same day or the day after when the information is what we call “hot”.

Mrs. Tracy Gray: Out of the number of reports that the Canadian Anti-Fraud Centre receives, what percentage would you say is investigated and what percentage would lead to actual enforcement? Do you have those numbers?

Mr. Guy Paul Larocque: Unfortunately not, because it's a very difficult metric. You'd have to turn to Statistics Canada to have a better picture of what has been investigated, or where charges were laid, because of how it's being reported through the protocols in place or policies that police agencies across the country have to adhere to.

Mrs. Tracy Gray: Would you say that there's an adequate level of enforcement when it comes to fraudulent calls, based on your assessment?

Mr. Guy Paul Larocque: That's a very tough question to answer, because we always think that more could be done. There are always better things that we can do as law enforcement as well.

Fraud is a collective problem. We need to be able to educate the public. We think public education is the key issue in being able to mitigate fraud. One thing we'll never be able to stop is the solicitation of fraud, but a successful measure is to help the public recognize what the risks behind fraud are. In that way, they'll be able to reject the fraud attempts when they see them.

Mrs. Tracy Gray: Okay.

A/Commr Eric Slinn: Guy Paul is being nice there too. I think I said in my previous testimony in March that we need to do a better job, and not just the RCMP but all of law enforcement. It's not a sexy crime like many of the drug crimes are and those sorts of things. As a community, we need to do better. We've engaged the Canadian Association of Chiefs of Police as well to up our game with these frauds.

Mrs. Tracy Gray: Thank you.

Typically, the CSE would use the common criteria for information technology security evaluation to evaluate the security claims of information technology products. Obviously, our committee has focused on this a lot. We've seized on this topic of improving network access for Canadians, and of course—

The Chair: MP Gray, unfortunately, you're over time. I'm sorry about that.

Mrs. Tracy Gray: Okay. Thank you.

The Chair: Our next round of questions goes to MP Longfield.

You have five minutes.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you.

MP Gray, you were heading down a path that I was thinking of heading down as well, so maybe I can build on some of your questioning.

To continue with the RCMP, we're fortunate in Guelph to have a former RCMP officer, Gord Cobey, as our chief of police. We work quite closely together. We also have the OPP around Guelph, so we have multijurisdictional police forces who are working together and keeping ties between each other.

My question is in terms of the previous meeting when you were with us, Mr. Slinn, and were mentioning public education and how important it is to exchange information quickly. If you're allowed to share that publicly, how does that actually happen between forces? Is there a way we can improve or help you to improve quick responses, as we've needed to do in other areas in COVID?

● (1650)

A/Commr Eric Slinn: Thanks for that question.

I think the Canadian Anti-Fraud Centre is a great hub for collecting a lot of that intelligence. They do a great job of pushing that intelligence out either in close to real time or as a trend analysis, bulletins or postings to various law enforcement agencies across the country. The other thing they do well is informing Criminal Intelligence Service Canada, which does a lot of the intelligence tracking.

To answer your question, I think the framework is in place where intelligence on fraud is passed expeditiously to various law enforcement agencies across the country. It's just a matter of putting more resources or effort into these fraud investigations. I don't want to characterize them as being easy investigations. These international ones can be very complicated, and securing international evidence in a country can be challenging as well.

Mr. Lloyd Longfield: One thing we've seen through COVID is that public health has been sharing information very openly with the public, which is helping the public to be on alert for behaviours that are helping and behaviours that are not helping when fighting the pandemic. Is that an opportunity in terms of a more open sharing of where we are getting attacked or is that tipping our hats to the bad guys?

A/Commr Eric Slinn: No, I don't think so. I think we strive to do that through the Canadian Anti-Fraud Centre. Maybe your question is this: Should we be more broad in our sharing, having local law enforcement agencies putting that up on their websites? I think that's a great observation, and it's something we can certainly build on.

Mr. Lloyd Longfield: Thank you.

Not many Canadians know about the Canadian Anti-Fraud Centre and the work that's being done there. I have a report in front of me that shows that 188 Canadians have been victims to COVID-inspired scams and have lost a total of $1.2 million between the months of March and May of 2020.

Maybe this question is for Mr. Larocque. How does that compare? I think that in previous parts of this meeting I was hearing that there isn't much of a spike, but are we up from the same period last year?

Mr. Guy Paul Larocque: Yes, we are. The number of reports that we received at the Canadian Anti-Fraud Centre was up about 25% for the same period, for the first four months of the year.

Obviously, in April, we had an uptick in extortion email campaigns, which really put the numbers up. In just April alone, we received about 5,000 more complaints on that. As far as notifying the public, the Canadian Anti-Fraud Centre has produced bulletins. Twice we've provided a bulletin on scams around the pandemic, which was posted on our website, posted through social media and distributed to many of our partners. We try to leverage our network to be able to create as much publicity as we can around those scams, so that the public is very equipped to respond to those attacks.

Mr. Lloyd Longfield: Thank you.

With less than a minute left, maybe I can stay with you. This is with regard to MPs who might contribute to giving paths in for phishing. In the last week, I've had a Webex meeting with the mayor and the MPP, which we have regularly, Microsoft Teams meetings with some students at a high school, and this Zoom meeting. Are we contributing to the problem by opening ourselves up through networks such as these, or is there something that we need to be more aware of?

Mr. Guy Paul Larocque: I'm not sure if I properly understand the question, but every effort to educate one another will certainly contribute to better protecting ourselves. One initiative that we've started picking up from the U.K. is Tell2. If everyone tells two other people, in no time we would cover the country.

Mr. Lloyd Longfield: Great. Thank you very much.

Mr. Guy Paul Larocque: You're welcome.

The Chair: Thank you very much.

[*Translation*]

Mr. Savard-Tremblay, you have the floor for two and a half minutes.

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Thank you, Madam Chair.

My question concerns borders. Since American fraudsters can easily cross the border, do the Canadian laws make us particularly vulnerable, especially given the delay in implementing the STIR/SHAKEN standards?

I'm not sure to whom I should direct my question, perhaps to the representative of the Royal Canadian Mounted Police.

● (1655)

Mr. Simon Marchand: I can respond quickly, with your permission.

Mr. Simon-Pierre Savard-Tremblay: We're listening, Mr. Marchand.

Mr. Simon Marchand: Without commenting specifically on the STIR/SHAKEN standards, I can tell you that this issue was observed when EMV smart card technology was introduced in Canada. In the months following the implementation of the technology and once the critical mass had been reached, we saw fraudsters moving south of the border quickly enough to continue cloning cards, whereas here the trend was fading.

For fraudsters, the border isn't an issue. They'll go where they encounter the least resistance and the fewest obstacles to commit their crimes. We can reasonably believe that, if the STIR/SHAKEN standards are implemented in the United States and not in Canada, the fraudsters will come here and spoof telephone numbers.

Mr. Simon-Pierre Savard-Tremblay: This would lead to a competition of sorts between the two systems, where Canada would stand out for its laxity in terms of actually applying a standard. Is that a good summary of your comments?

Mr. Simon Marchand: Yes. In all cases of fraud, the fraudsters go where the laws are the easiest to circumvent and where there are fewer regulations. If the standard isn't implemented here and is implemented south of the border, the fraudsters will come to Canada.

Mr. Simon-Pierre Savard-Tremblay: Is it urgent to act and to legislate on this issue?

Mr. Simon Marchand: As I said earlier, it's essential to take action with regard to the STIR/SHAKEN standards. In terms of information security and consumer protection, Canada lags behind Europe and some of the American states. It's becoming urgent to act. If we don't act, we'll become the target of criminal organizations, which will come and attack Canadians.

Mr. Simon-Pierre Savard-Tremblay: Madam Chair, do I have time to ask another question?

The Chair: You have 20 seconds left.

Mr. Simon-Pierre Savard-Tremblay: Okay. I don't think that's enough time.

I want to thank Mr. Marchand and all my colleagues.

The Chair: Thank you.

[*English*]

Our next round is for MP Masse.

You have two and a half minutes.

Mr. Brian Masse: Thank you, Madam Chair.

One of the things that really got me irritated about the Facebook situation was that they used third party applicants too. In the United States, they settled for $5 billion, and over here, $9 million. That doesn't even cover the Government of Canada's advertising costs. We're actually going to try to do that by having advertisements on fraud, this by a party that really has misled Canadians. I think that's inappropriate messaging. I suppose we have very few tools for that.

I'm going to follow with Mr. Marchand. With regard to STIR/SHAKEN, I understand the testimony from the companies, but it wasn't very compelling that we shouldn't do it anyway because there will be some net benefits even if not everybody has STIR/SHAKEN right away. Also, you could screen your phone calls coming in that way. You could have choices as a consumer and be empowered. You could choose to not even take a call if it wasn't being screened through STIR/SHAKEN. You'd have more control.

Are there other things we can do? I don't mind if you shoot these ideas down. It won't hurt my feelings. Should we be doing something more robust with a Crime Stoppers approach? Should we be doing something with direct mail, because we can control the messaging directly to Canadians through the postal system? Should we be looking at a royal commission?

The more we spend on preventing fraud, the more money we also take away from other crime. We seem to be missing a link in this country to take it to the next level.

Mr. Simon Marchand: That's a very broad question. It would require probably its own two-hour session.

We could use direct by mail—why not?—but fraudsters have been observed intercepting mail sent to customers. If they really want to target someone, they will intercept the mail. I think it brings us back to a new step in identification, which means digital identity, talking about biometrics, something that fraudsters are not able to breach. They are not able to impersonate a voice print or a biometric factor, and I think that's the next step.

Biometrics is sensitive, and that would definitely require a public consultation of some sort to make sure that we understand what the parameters are that we're setting and how it's going to be managed and handled.

Mr. Brian Masse: Thank you.

Thank you, Madam Chair.

I want to thank all the groups for working on this. I know they've done a lot of good work over the years. I've seen it and I appreciate that.

The Chair: Thank you so much.

With that, we are at the end of the third round of questions.

I'd like to thank everyone for being here today. Thank you so much for your testimony.

[*Translation*]

Thank you for your patience with the technology.

● (1700)

[*English*]

Thank you to our IT team, translators, clerk and our analysts.

Our next meeting will be tomorrow. Stay tuned.

The meeting is adjourned.