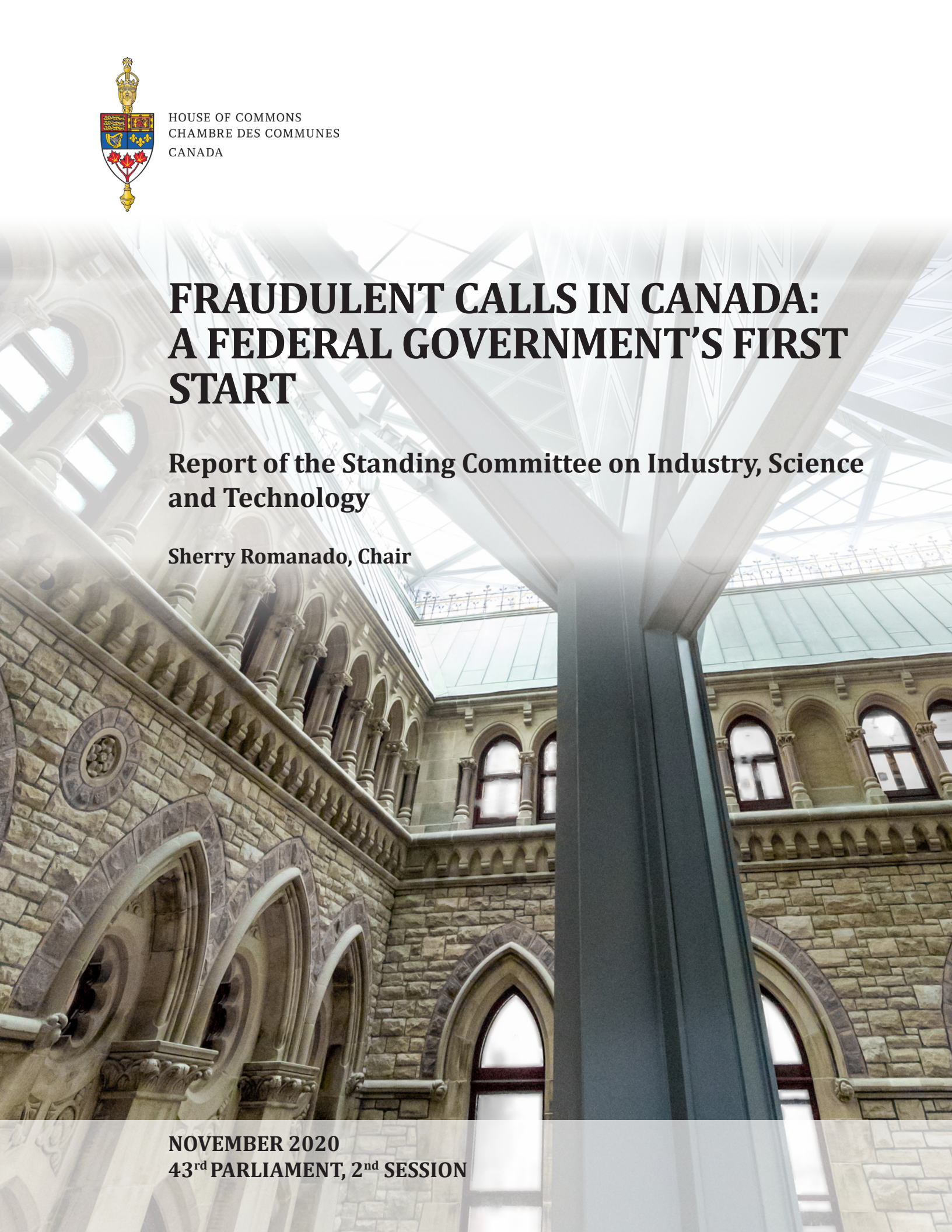

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

FRAUDULENT CALLS IN CANADA: A FEDERAL GOVERNMENT'S FIRST START

Report of the Standing Committee on Industry, Science and Technology

Sherry Romanado, Chair

NOVEMBER 2020
43rd PARLIAMENT, 2nd SESSION

FRAUDULENT CALLS IN CANADA: A FEDERAL GOVERNMENT'S FIRST START

Report of the Standing Committee on Industry, Science and Technology

Sherry Romanado
Chair

NOVEMBER 2020

43rd PARLIAMENT, 2nd SESSION

NOTICE TO READER

Reports from committee presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON INDUSTRY, SCIENCE AND TECHNOLOGY

43RD PARLIAMENT – 1ST SESSION

CHAIR

Sherry Romanado

VICE-CHAIRS

Hon. Michelle Rempel Garner

Sébastien Lemire

MEMBERS

Earl Dreeshen

Ali Ehsassi

Nathaniel Erskine-Smith

Tracy Gray

Helena Jaczek

Majid Jowhari

Emmanuelle Lambropoulos

Brian Masse

Jeremy Patzer

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Sean Casey

Julie Dabrusin

Marie-Hélène Gaudreau

Chris Lewis

Llyod Longfield

Paul Manly

Simon-Pierre Savard-Tremblay

Tako Van Popta

CLERK OF THE COMMITTEE

Michael MacPherson

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Francis Lord, Analyst

Sarah Lemelin-Bellerose, Analyst

STANDING COMMITTEE ON INDUSTRY, SCIENCE AND TECHNOLOGY

43RD PARLIAMENT – 2ND SESSION

CHAIR

Sherry Romanado

VICE-CHAIRS

James Cumming
Sébastien Lemire

MEMBERS

Earl Dreeshen
Ali Ehsassi
Nathaniel Erskine-Smith
Helena Jaczek
Majid Jowhari
Emmanuelle Lambropoulos
Brian Masse
John Nater
Derek Sloan

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Taylor Bachrach
Tony Baldinelli

CLERK OF THE COMMITTEE

Michael MacPherson

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Francis Lord, Analyst
Sarah Lemelin-Bellerose, Analyst

THE STANDING COMMITTEE ON INDUSTRY, SCIENCE AND TECHNOLOGY

has the honour to present its

FIRST REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied fraud calls in Canada and has agreed to report the following:

TABLE OF CONTENTS

SUMMARY

Fraud calls cause significant losses to Canadians. Supported by offshore fraud call centres and easily accessible technologies, such as robocalls and spoofing, fraudsters manage to deliver scams despite the best efforts of law enforcement agencies, the Canadian Radio-Television and Telecommunications Commission (CRTC), and telecommunications service providers (TSPs). To better protect the public, the federal government must support the adoption of new techniques and technology, such as a timely implementation of the STIR/SHAKEN framework that sufficiently addresses competition and privacy concerns. The federal government should also improve cooperation between relevant public authorities at home and abroad, data collection, public awareness and transparency, and criminal legislation and enforcement.

The federal government should pay further attention to allegations that fraudsters exploit federal wireless number portability rules to conduct harmful unauthorized-porting scams. While the CRTC and TSPs are developing measures against unauthorized porting, more should be done to protect Canadians. More specifically, the Committee invites the federal government to urge the CRTC to conduct a public inquiry into unauthorized porting, and to step in and regulate the matter directly should the CRTC fail to do so.

The COVID-19 pandemic led to an upsurge in fraud targeting Canadians. Indeed, between January 2020 and April 2020, the Royal Canadian Mounted Police observed that the number of fraud reports increased by 25% over the same period last year. The COVID-19 pandemic is putting lives and livelihoods at risk, and the Canadian economy in jeopardy. The federal government should prevent any further harm to Canadians. In the short term, increasing public awareness remains the most effective way to counter COVID-19–related fraud. The federal government should act now by launching a public awareness campaign in local and national media to warn Canadians against COVID-19–related fraud.

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

FRAUDULENT CALLS IN CANADA: A FEDERAL GOVERNMENT'S FIRST START

HELP PROTECT CANADIANS

If you have been a victim of fraud, report it to the Canadian Anti-Fraud Centre (CAFC) and the local police. Your actions will help protect all Canadians. For information on ongoing fraud schemes, consult the CAFC's webpage.

INTRODUCTION

On 20 February 2020, the House of Commons Standing Committee on Industry, Science and Technology (the Committee) agreed to:

> Hold immediate hearings with the Canadian Radio-television and Telecommunications Commission (CRTC), Royal Canadian Mounted Police (RCMP), Canada's telecommunications companies and other telecom experts and advocacy groups, to better understand: (a) the influx of fraud calls to Canadians' home phones and cellular devices including robocalls, ghost calls, and spam calls; (b) to give an update on the successes and failures of the National Do-Not-Call List, and; (c) to outline the September 2020 STIR/SHAKEN measures and how this will benefit Canadian consumers.

The Committee held three meetings, heard from 21 witnesses, and received six briefs.

FRAUD AND OTHER NUISANCE CALLS

Understanding the Problem

The term "nuisance call" refers to undesirable, unsolicited vocal telecommunications. A "fraud call" is a nuisance call made with the intent of defrauding its recipient through deceit, falsehood, or other fraudulent means. As Kate Schroeder, from the Canada Network for the Prevention of Elder Abuse (CNPEA), put it, fraud constitutes "an attempt to deceive an individual to gain control over some aspect of that individual's life, whether it be financial, identity or other."[1] While receiving nuisance calls can annoy, infuriate, or in some cases compromise the enjoyment of a consumer's phone services,

1 House of Commons, Standing Committee on Industry, Science and Technology [INDU], *Evidence*, 43rd Parliament, 1st session, 12 March 2020, 1205 (Canada Network for the Prevention of Elder Abuse [CNPEA], Kate Schroeder). See also CNPEA, *Brief Submitted to INDU*, 28 April 2020.

fraud calls can have severe consequences for their victim, financial or otherwise, and amount to criminal behaviour.[2]

One type of ongoing fraud call is the so-called "CRA (or taxpayer) scam." The CAFC describes the CRA scam in the following manner:

> A scammer claims to be an employee of either the Canada Revenue Agency or Service Canada. They state you:
>
> - owe back taxes
> - have unpaid balances
> - committed a financial crime
>
> They insist that if you do not pay immediately, you'll be arrested, fined or even deported.
>
> The scammers may request payment via money service businesses, prepaid cards/gift cards (iTunes, Google Play or Steam cards) or Bitcoin.

Like many other fraud calls, the CRA scam is delivered through a "robocall:" a voice message delivered with a device capable of storing or producing phone numbers. The voice message usually urges its receiver to call a number. Calling the number leads the victim to communicate with a fraudster who attempts to defraud them through various means.[3] Between 2014 and 2019, the RCMP estimated that the CRA scam alone resulted in cumulative losses of over $16.8 million.[4]

The Canadian Electricity Association (CEA) – regrouping Canadian utilities and companies that generate, transmit, and distribute electricity – reported that fraudsters regularly target its members' customers. In such a fraud call, the fraudster impersonates a utility and intimidates the victim by threatening to cut off power to their business immediately before peak hours unless they pay "overdue charges." If the victim believes the fraudster, the latter requests payment in the form of pre-paid credit cards or Bitcoin. The CEA indicated that, in the last two years, one of its members received an average of 150 reports per month from its customers of fraudsters impersonating the utility.

---

2 INDU, *Evidence*, 43rd Parliament, 1st session, 10 March 2020, 1140 (Canadian Radio-television and Telecommunications Commission [CRTC], Ian Scott); Ibid., 1210, 1255 (Rogers Communications Inc., Howard Slawner & Deborah Evans). But see ibid., 1205 (Bell Canada, Jonathan Daniels).

3 See generally INDU, *Evidence*, 12 March 2020, 1110-1115 (Public Interest Advocacy Centre [PIAC], John Lawford).

4 INDU, *Evidence*, 10 March 2020, 1115 (Royal Canadian Mounted Police [RCMP], Eric Slinn).

Another CEA member estimated that, in 2018, its customers may have lost over $18,000 over a four-month period to such fraud calls, not to mention the reputational losses suffered by the utility itself.[5]

A disproportionate number of seniors, low-income households, and newer Canadians fall victim to fraudsters.[6] According to witnesses, seniors more easily trust strangers and tend to suffer from social isolation making them especially vulnerable to fraudsters using intimidation or pretenses of kindness to deceive their victim.[7] Other factors that further increase risk for seniors include economic insecurity, potential cognitive impairment, and lack of understanding of ongoing fraud schemes. Seniors may also encounter obstacles when trying to report fraud, for example fearing that victimization will make them appear incompetent or lacking knowledge in how to report the fraud. In response to an influx of fraud calls, some seniors may cancel telecommunications services, which increases social isolation. More Canadians could become vulnerable to fraud as the population ages.[8]

Easily accessible technology facilitates the automation and anonymization of fraud calls.[9] Internet telephony reduces the cost of delivering vast quantities of robocalls in a short time, making schemes such as the CRA scam cost-effective. Such cost effectiveness enables fraudsters to establish and maintain fraud-call centres that deliver fraud schemes on a large scale, most of which are located outside of Canada.[10] Fraudsters also hide or disguise their caller identification (caller ID) using a technique known as "spoofing."[11] While call spoofing is not illegal per se, fraudsters spoof calls to impersonate other individuals and organizations, and trick their victim into divulging valuable personal information to facilitate fraud. Because of call spoofing, caller-ID features are largely ineffective at countering nuisance and fraud calls.[12]

---

5 Canadian Electricity Association [CEA], *Brief Submitted to INDU*, 28 April 2020.

6 INDU, *Evidence*, 12 March 2020, 1110, 1140 (Lawford); Ibid., 1205 (Schroeder); CNPEA, *Brief Submitted to INDU*, 28 April 2020.

7 INDU, *Evidence*, 12 March 2020, 1125 (Lawford).

8 Ibid., 1205-1210, 1230, 1255 (Schroeder); CNPEA, *Brief Submitted to INDU*, 28 April 2020.

9 INDU, *Evidence*, 12 March 2020 1110-1115 (Lawford).

10 INDU, *Evidence*, 10 March 2020, 1100 (Scott).

11 According to the CRTC, spoofing "occurs when callers deliberately falsify the caller ID (e.g. telephone number) that is sent to called parties in order to disguise their true identity."

12 INDU, *Evidence*, 10 March 2020, 1135 (RCMP, Guy Paul Larocque); INDU, *Evidence*, 12 March 2020, 1105 (Internet Society Canada Chapter, Matthew Gamble); CEA, *Brief Submitted to INDU*, 28 April 2020.

Because of constantly evolving techniques and technology, authorities as well as telecommunications services providers (TSPs) and other stakeholders find it challenging to maintain up-to-date information on how fraudsters target victims and deliver fraud calls to Canadians – some witnesses evoking the image of an "arms race."[13] As a result, witnesses have emphasized the importance of keeping the public aware of ongoing fraud schemes and techniques.[14]

More specifically, the Public Interest Advocacy Centre (PIAC) and the CNPEA suggested that authorities and TSPs provide materials detailing ongoing fraud schemes through trusted channels and in a language vulnerable groups will understand. While more information must pressingly reach seniors, it should be directed to all ages. Authorities should also involve actors that can help protect Canadians from fraud, such as financial institutions, TSPs, and insurance companies. The CNPEA also proposed to pay attention to how awareness campaigns can effectively reach Canadians living in rural and remote areas.[15]

While Canadians regularly receive fraud calls, few witnesses could provide precise data on the magnitude of the problem. While citing CAFC's 2019 data, John Lawford, Executive Director and General Counsel of PIAC, stressed that there is no definitive or official source of data on fraud generally and fraud calls specifically.[16] Data is limited by the fact that as little as five percent of Canadians who fall victim to fraud report it.[17] The lack of reliable and accurate data increases the difficulty of intercepting fraud calls.[18] Mr. Lawford therefore stressed the need to improve the availability and quality of fraud-related statistics and regularly report them to the public.[19]

According to the CAFC, fraud calls account for $25 million of the $98 million lost to fraud in 2019.[20] The CNPEA estimated that victims who are senior citizens account for a

13 INDU, *Evidence*, 10 March 2020, 1125 (Slinn); Ibid., 1210, 1255 (Slawner & Evans); INDU, *Evidence*, 12 March 2020, 1135 (Gamble).

14 See for example INDU, *Evidence*, 10 March 2020, 1130, 1155 (Scott).

15 INDU, *Evidence*, 12 March 2020, 1120, 1135 (Lawford); Ibid., 1210, 1230, 1245 (Schroeder).

16 Ibid., 1110 (Lawford).

17 Canadian Anti-Fraud Centre, "Top 10 frauds of 2019" 20 February 2020. But see INDU, *Evidence*, 12 March 2020, 1205 (Schroeder); CNPEA, *Brief Submitted to INDU*, 28 April 2020.

18 INDU, *Evidence*, 12 March 2020, 1130 (Gamble).

19 Ibid., 1115 (Lawford).

20 INDU, *Evidence*, 10 March 2020, 1150 (Slinn).

quarter of these losses.[21] Matthew Gamble, Director of the Internet Society Canada Chapter (ISCC), cited a Truecaller study claiming that Canadians receive an average of 12 fraudulent or nuisance calls per month, with these numbers increasing as technology reduces the cost of robocalls and helps fraudsters evade enforcement.[22] The CRTC shared data from the United States, citing that in the month of February 2020 alone, Americans received over 2 billion fraudulent robocalls.[23]

Current Response

Witnesses stressed the importance of close collaboration between government bodies, TSPs, consumer groups, and other stakeholders both at home and abroad to effectively reduce and protect Canadians from fraud calls.[24]

Federal Authorities

The RCMP and the CRTC implement much of the federal response against fraud and nuisance calls. Both institutions collaborate with TSPs and other stakeholders to prevent or reduce nuisance and fraud calls and mitigate their impact. Being "arms-length" organizations, the RCMP and CRTC operate with a large degree of independence from the federal government. However, Mr. Lawford still proposed that both Parliament and the federal government take a more prominent role in reducing fraud calls: the former could provide continual oversight of measures taken while the latter more actively integrate countering phone and Internet fraud in digital policymaking.[25] To facilitate law enforcement efforts, Mr. Lawford also suggested criminalizing the use of robocalls, which attempt to defraud a person.[26]

The Royal Canadian Mounted Police

Assistant Commissioner Eric Slinn stressed that the RCMP makes financial crime, including fraud, a federal policing priority. As such, the law enforcement agency conducts investigations into fraud-call schemes that may lead to criminal prosecution.

---

21 INDU, *Evidence*, 12 March 2020, 1205 (Schroeder); CNPEA, *Brief Submitted to INDU*, 28 April 2020.

22 INDU, *Evidence*, 12 March 2020, 1105 (Gamble).

23 INDU, *Evidence*, 10 March 2020, 1150 (Scott).

24 See for example ibid., 1205, 1245 (Daniels); Ibid., 1210, 1255 (Slawner & Evans); INDU, *Evidence*, 12 March 2020, 1210 (Schroeder); CNPEA, *Brief Submitted to INDU*, 28 April 2020.

25 INDU, *Evidence*, 12 March 2020, 1115 (Lawford).

26 Ibid., 1145.

For example, in February 2020, as part of its "Project Octavia," the RCMP arrested and charged two individuals in connection with a CRA scam.

Assistant Commissioner Slinn highlighted the importance of public education to prevent fraud and described the RCMP's involvement in public awareness campaigns. For example, in response to reports of gift card scams in Alberta, the RCMP distributed fraud tip sheets to local businesses to prevent their customers from falling victim to these scams.[27] The CAFC is another important part of the RCMP's response to fraud. The RCMP operates the CAFC in partnership with the Competition Bureau and the Ontario Provincial Police. Acting as a central information repository, the CAFC plays an important preventive role by disseminating information on fraud to law enforcement agencies, private actors such as TSPs and financial institutions, and the Canadian public. The CAFC relies on information provided by Canadians to perform its activities, but Mr. Slinn warned that the increasing volume of fraud is overwhelming its staff.[28]

The RCMP's cooperation with other entities at home and abroad is a key component of their strategy against fraud. The law enforcement agency collaborates with multiple partners to protect Canadians, including the CRA, the Financial Transactions and Reports Analysis Centre of Canada, TSPs and financial institutions. Given that fraudsters carry out their activities on a global scale, the RCMP closely collaborates with foreign authorities and international law enforcement agencies, including the Five Eyes Law Enforcement Group.[29]

Assistant Commissioner Slinn emphasized the importance of international cooperation to counter fraud targeting Canadians, as the RCMP does not have jurisdiction to investigate and charge fraudsters operating overseas.[30] Mr. Slinn called on the federal government to urge foreign governments to shut down call centres abroad from which many, if not most, fraudulent robocalls originate, and to act against criminal behaviour committed against Canadians from inside their borders.[31]

The CEA expressed difficulty in obtaining the support of law enforcement agencies because law officers tend to lack the necessary time and resources:

---

27 INDU, *Evidence*, 10 March 2020, 1110-1115 (Slinn).

28 Ibid., 1115-1120, 1155.

29 Ibid., 1110, 1120.

30 Ibid., 1155.

31 Ibid. See also INDU, *Evidence*, 10 March 2020, 1215, 1245 (Slawner).

> One electricity company reported an attempt to share information in a timely fashion and in the required format with an interested law enforcement officer, only to later learn that the lack of response from law enforcement was due to the officer having been moved to a more pressing file. Electricity companies also noted that they had rarely heard of any continuing contact with victims after the initial complaint to local enforcement.[32]

Assistant Commissioner Slinn recognized that the Canadian law enforcement community still needs to do more to tackle fraud. The RCMP works to develop a more coordinated approach to policing response and increase its engagement effort to tackle fraud through the Canadian Association of Chiefs of Police.[33] He explained that police officers should investigate fraud calls and not simply refer victims to the CACF, which solely focuses on intelligence gathering as opposed to police investigation. Even though investigating fraud calls is difficult, most notably because they often originate from overseas, investigations remain important, if only, to gather intelligence.[34] The CNPEA echoed these comments, asking for the federal government to support Canadians reporting fraud and help prevent re-victimization.[35]

The Canadian Radio-television and Telecommunications Commission

Mandate and Key Activities

The CRTC fights fraud calls less directly than the RCMP. Ian Scott, Chairperson and Chief Executive Officer of CRTC and his colleagues, repeatedly emphasized that, unlike the RCMP, the CRTC does not police fraud. Instead, it focuses its enforcement activities on unsolicited telemarketing telecommunications.[36] However, the CRTC still plays a structural role in regulating and coordinating TSPs to reduce fraud calls and allow consumers to safely use telecommunications services. This role explains the involvement of the CRTC in the deployment of "STIR/SHAKEN" in Canada, as will be discussed further below.

Mr. Lawford would like the CRTC to take a more direct approach against fraud calls.[37] He recommended amending the *Telecommunications Act* or enacting "anti-phone fraud" legislation to give the CRTC more authority – and responsibility – to tackle fraud calls.

---

32 CEA, *Brief Submitted to INDU*, 28 April 2020.

33 INDU, *Evidence*, 10 March 2020, 1145 (Slinn).

34 Ibid., 1150.

35 INDU, *Evidence*, 12 March 2020, 1210, 1245 (Schroeder).

36 INDU, *Evidence*, 10 March 2020, 1100 (Scott).

37 See also ibid., 1215 (Slawner).

Mr. Lawford pointed to the US *Telemarketing Consumer Fraud and Abuse Prevention Act* as a potential source of inspiration. Such legislative changes would directly extend the mandate of the CRTC from telemarketing to fraud.[38] Rogers Communications Inc. (Rogers) also suggested that the CRTC draw inspiration from measures taken by US agencies to stop international robocalls from entering domestic networks.[39]

Like the RCMP, the CRTC closely cooperates with multiple entities to meet its mandate. These entities include TSPs, other federal departments and organizations, law enforcement agencies, its foreign counterparts, and international organizations.[40] Such collaboration helps with sharing knowledge, harmonizing practices, and coordinating action against fraud and other threats to telecommunications networks, and thus strengthen the international response to address fraud globally.[41]

To support these initiatives, the CRTC exchanges information with other organizations. For example, it signed memoranda of understanding with its foreign counterparts in the United States, Japan, the United Kingdom, Australia, and New Zealand to share information. However, the CRTC does not have the same flexibility to share information with Canadian organizations. The CRTC proposed that Parliament amend its enabling legislation to allow it to share information it collects with Canadian law enforcement agencies and government bodies.[42]

National Do Not Call List

The CRTC created the National Do Not Call List (DNCL) in 2008 to reduce unsolicited telemarketing calls, thanks to a legislative framework provided by the *Telecommunications Act*. The DNCL is a registry of personal phone numbers that cannot be called for solicitation purposes. The CRTC formulates and enforces the rules applicable to the DNCL while a National Operator – currently Raymond Chabot Grant Thornton Consulting – manages the DNCL by collecting applicable fees from subscribed telemarketers.

Under the DNCL rules, telemarketers cannot initiate a telemarketing call unless they or their client is a registered subscriber to the DNCL. The DNCL rules prohibit telemarketers from initiating a telemarketing telecommunication to a consumer's personal phone

38 INDU, *Evidence*, 12 March 2020, 1115, 1135, 1145 (Lawford).

39 INDU, *Evidence*, 10 March 2020, 1215 (Slawner).

40 Ibid., 1005-1110, 1135 (Scott).

41 Ibid. See for example ibid., 1210 (Slawner).

42 Ibid., 1110, 1140 (Scott).

number registered on the DNCL, unless the consumer expressly consented to be contacted by the telemarketer or their client. The DNCL rules also exempt some organizations, such as charities and political parties. The CRTC explained that while registration is free, telemarketers have to pay a subscription fee to obtain an up-to-date copy of the DNCL.[43]

Consumers can complain to the CRTC about telemarketing telecommunications they receive in contravention to the DNCL rules. Canadians have subscribed to the DNCL since its creation, with an average of 858 of them subscribing each day last year. All in all, Canadians have registered more than 14 million numbers with the CRTC. The CRTC interprets these figures as evidence that Canadians are confident in the effectiveness of the DNCL.[44] However, as Bell Canada (Bell) and Rogers argued, the DNCL can only stop calls made by telemarketers operating in Canada, while the majority of nuisance calls originate from overseas by actors that have no intention of complying with DNCL rules.[45]

While the CRTC received around 84,000 complaints related to the DNCL in the 2018-2019 period, it has only pursued enforcement actions in about 500 cases. The CRTC defended its enforcement record, explaining that, on its own, the total number of complaints can be misleading as it contains non-validated complaints and complaints that may relate to the same telemarketing campaign. Moreover, the CRTC sees its enforcement actions, especially administrative monetary penalties (AMPs), not as punishment for breaking the rules, but as incentives to comply with them. This approach explains why the CRTC shows restraint in enforcing the DNCL rules. While every case may not warrant AMPs or other formal enforcement actions, the CRTC strives to educate telemarketers on their obligations, notably with compliance programs and audits.[46]

Telecommunications Services Providers

TSPs play an important role in preventing and reducing fraud calls delivered through their services. The CRTC formulates regulations TSPs must comply with, notably to implement measures that may help consumers protect themselves against fraud attempts. Some measures are applied throughout the industry, such as the universal blocking of evidently illegitimate calls and the upcoming STIR/SHAKEN framework. TSPs may also offer measures of their own to their customers. TSPs may implement

43 Ibid., 1125 (CRTC, Alain Garneau).

44 Ibid., 1100 (Scott).

45 Ibid., 1205 (Daniels); Ibid., 1210, 1250 (Slawner).

46 Ibid., 1100, 1120, 1140-1145 (CRTC, Scott, Garneau, and Steven Harroun).

sector-wide and individual measures through different techniques while sharing the overall goal of protecting their customers from fraud calls.[47]

The STIR/SHAKEN Framework

STIR/SHAKEN is a framework of interconnected standards that enable TSPs to validate caller-ID information on Internet protocol-based (IP) calls. The STIR/SHAKEN framework does not filter nor block calls, but counters spoofing by providing information on the legitimacy of a phone call and would help its receiver decide whether or not they should answer it.[48] The CRTC has described it as "the only viable authentication/verification solution that can provide consumers with a measure of additional trust in caller ID."[49] The CRTC was considering requiring TSPs that provide voice telecommunications services to implement STIR/SHAKEN by 30 September 2020.[50]

According to COMsolve Inc., a technology services provider, the eventual deployment of the STIR/SHAKEN framework could increase pressure to implement analytics-based call blocking solutions. While COMsolve argued that while "STIR/SHAKEN in combination with analytics-based call blocking is the best way to deal with unwanted spoofed calls," callers should have visibility in how TSPS and their partners authenticate and treat their calls, as well as being able to demonstrate they use authorized numbers.[51]

Many witnesses supported the implementation of STIR/SHAKEN as one of many means to protect Canadians against fraud calls, including Bell, Rogers, and TELUS Communications Inc. (TELUS). These TSPs have thus made meaningful progress towards

47 Ibid., 1245-1250 (Daniels); Ibid., 1250 (Slawner).

48 Ibid., 1105 (Scott); INDU, *Evidence*, 12 March 2020, 1105, 1125 (Gamble). But see INDU, *Evidence*, 10 March 2020, 1225 (TELUS Communications Inc. [TELUS], Jérôme Birot); TELUS, *Brief Submitted to INDU*, 9 March 2020; COMsolve, *Brief Submitted to INDU*, 29 April 2020.

49 *Compliance and Enforcement and Telecom Decision CRTC 2019-402*, para. 22, 9 December 2019.

50 INDU, *Evidence*, 10 March 2020, 1105 (Scott). See also *Compliance and Enforcement and Telecom Notice of Consultation CRTC 2019-404*, 9 December 2019. But see *Compliance and Enforcement and Telecom Decision CRTC 2019-402-2*, para. 17, 15 September 2020 (since it appeared before the Committee, the CRTC extended this deadline to 30 June 2021).

51 COMsolve, *Brief Submitted to INDU*, 29 April 2020.

its implementation.[52] However, they also warned that they could not fully implement the STIR/SHAKEN framework by September 2020 despite their best efforts.[53]

Some witnesses pointed to multiple issues that the CRTC and TSPs must address before launching the STIR/SHAKEN framework. Many of them are technical in nature such as adapting phone networks and devices to properly operate the STIR/SHAKEN framework. According to the testimony of TSPs, these challenges must be addressed before consumers can enjoy the full benefit of the framework.

To operate, STIR/SHAKEN requires all TSPs carrying a call to interconnect through IP-based technology. A call will not be verified if, at any point along a network, it proceeds through non-IP technology. While the ISCC observed that most of smaller TSPs provide IP-based telephony technology,[54] some of the large TSPs' networks still rely on non-IP, circuit-switch equipment. These TSPs must therefore upgrade their network to fully implement STIR/SHAKEN, a process they described as time consuming.[55]

TSPs also stressed that most phones today, including landline telephones and most cellphones, cannot display to their owner the information the STIR/SHAKEN framework would provide. Phone manufacturers, such as Apple and Samsung, must therefore design devices that can effectively display such information. Evidently, Canadian TSPs cannot dictate the speed at which these manufacturers will deliver these devices.[56] Other witnesses also noted that the CRTC and the industry have yet to formulate display standards: what and how information about the legitimacy of a phone call will be communicated to consumers.[57]

---

52 INDU, *Evidence*, 10 March 2020, 1205 (Daniels); Ibid., 1210 (Slawner); Ibid., 1225 (Birot); TELUS, *Brief Submitted to INDU*, 9 March 2020. See also INDU, *Evidence*, 12 March 2020, 1115 (Lawford); Ibid., 1125 (Gamble).

53 INDU, *Evidence*, 10 March 2020, 1210, 1245 (Slawner); Ibid., 1245 (Birot). But see *Compliance and Enforcement and Telecom Decision CRTC 2019-402-2*, para. 17, 15 September 2020 (since it appeared before the Committee, the CRTC extended this deadline to 30 June 2021).

54 INDU, *Evidence*, 12 March 2020, 1105 (Gamble).

55 INDU, *Evidence*, 10 March 2020, 1210-1215 (Slawner); Ibid., 1225, 1235 (Birot); Ibid., 1245 (Daniels); TELUS, *Brief Submitted to INDU*, 9 March 2020. See also COMsolve, *Brief Submitted to INDU*, 29 April 2020. But see INDU, *Evidence*, 12 March 2020, 1105 (Gamble).

56 INDU, *Evidence*, 10 March 2020, 1205, 1230 (Daniels); Ibid., 1225, 1235 (Birot); TELUS, *Brief Submitted to INDU*, 9 March 2020.

57 INDU, *Evidence*, 10 March 2020, 1130 (Scott); Ibid., 1210 (Slawner); COMsolve, *Brief Submitted to INDU*, 29 April 2020.

For these reasons, some witnesses argued that the CRTC should postpone imposing the implementation of STIR/SHAKEN.[58] According to Jonathan Daniels, Vice-President at Bell, June 2022 would offer a more realistic deadline for full implementation of the framework on Canadian networks.[59] Mr. Gamble, from the ISCC, added that the timeframe for full implementation of STIR/SHAKEN will remain unknown until consumers are willing and able to adopt it.[60] The CRTC had assured the Committee that while it expected TSPs to be able to implement STIR/SHAKEN by September 2020, it would provide them more time to do so upon request.[61]

Beyond technical challenges, the ISCC drew the attention of the Committee to policy issues raised by the current implementation of the STIR/SHAKEN framework. As per its proposal, the CRTC would require all TSPs offering voice communication services to implement STIR/SHAKEN, including smaller carriers. Rogers predicted that smaller carriers will benefit from the experience large TSPs will gain from implementing STIR/SHAKEN.[62] However, the ISCC argued that early policy and design decisions benefit large TSPs over smaller ones.[63]

For example, under the STIR/SHAKEN framework, only a TSP owning a phone number can authenticate it, leaving the over 1,200 resellers of telecommunications services that do not own their phone numbers without the ability to authenticate them. According to the ISCC, the current STIR/SHAKEN framework puts these smaller carriers at risk of losing customers to larger TSPs who can authenticate their phone numbers. This outcome would in turn reduce competition in Canada's telecommunications sector.[64]

To explain disadvantages imposed on smaller carriers, the ISCC points to their underrepresentation on the CRTC's working group charged with formulating STIR/SHAKEN standards. Indeed, few small carriers have enough resources to participate on such forums.[65] Mr. Gamble added that the Alliance for Telecommunications Industry Solutions (ATIS), who took part in developing the STIR/SHAKEN framework, is currently

58 INDU, *Evidence*, 10 March 2020, 1245 (Slawner); Ibid., 1245 (Daniels); Ibid., 1245 (TELUS, John Mackenzie).

59 Ibid., 1205 (Daniels).

60 INDU, *Evidence*, 12 March 2020, 1150 (Gamble).

61 INDU, *Evidence*, 10 March 2020, 1130 (Scott). But see *Compliance and Enforcement and Telecom Decision CRTC 2019-402-2*, para. 17, 15 September 2020 (since it appeared before the Committee, the CRTC extended this deadline to 30 June 2021).

62 INDU, *Evidence*, 10 March 2020, 1240 (Slawner).

63 INDU, *Evidence*, 12 March 2020, 1105 (Gamble).

64 Ibid., 1105, 1150.

65 Ibid., 1125, 1135.

studying proposals to better account for smaller carriers, but that the CRTC-imposed deadline of September 2020 would pass before ATIS can release its conclusions.[66] When questioned on this subject, the CRTC responded that its consultation process extends to small carriers that provide vocal communication services, and that these carriers could mitigate the costs associated with implementing STIR/SHAKEN by regrouping among themselves or by partnering with larger TSPs.[67]

Finally, the STIR/SHAKEN framework could raise privacy issues. As authenticated calls proceed through networks, TSPs will obtain data on their source and destination. TSPs may share this data with third parties at home or abroad, for example to conduct analysis in order to improve spam filtering techniques or to build customer profiles.[68] Both ISCC and PIAC proposed requesting that the Privacy Commissioner examine risks associated with STIR/SHAKEN.[69]

Other Measures

Implementing the STIR/SHAKEN framework is one of many measures TSPs have taken to reduce fraud calls, either on their own or in compliance with CRTC's decisions. Since December 2019, the CRTC mandates the universal blocking of evidently illegitimate calls, such as international calls using local numbers or non-standard calls, such as from phone numbers that do not conform to a ten-digit structure.[70] Bell reportedly blocks 220 million calls per month under universal call blocking.[71] One of the CRTC's working groups is also working on a call traceback process to better identify the origins of nuisance calls.[72]

Individual TSPs also offer their customers different services to reduce nuisance and fraud calls. In addition to common features such as caller-ID and call-filtering systems,[73] TELUS offers its customers a "call control" feature that prompts (or "challenges") unverified

66 Ibid., 1150. But see *Compliance and Enforcement and Telecom Decision CRTC 2019-402-2*, para. 17, 15 September 2020 (since it appeared before the Committee, the CRTC extended the deadline for implementing the STIR/SHAKEN framework to 30 June 2021).

67 INDU, *Evidence*, 10 March 2020, 1135 (Scott).

68 INDU, *Evidence*, 12 March 2020, 1105, 1150 (Gamble).

69 Ibid., 1140; Ibid., 1140 (Lawford).

70 INDU, *Evidence*, 10 March 2020, 1105, 1150 (Scott); Ibid., 1220 (Birot); Ibid., 1210 (Slawner).

71 Ibid., 1205 (Daniels).

72 Ibid., 1150 (Scott).

73 Ibid., 1220 (Birot).

callers to press a randomly selected number before they can reach the intended recipient. TELUS maintains records of calls that initiate and pass this gateway feature to optimize call control and to prevent a legitimate caller from being challenged multiple times. Its Vice-President Jerome Birot claimed that robocalls cannot pass the call-control challenge and therefore fail to go through. Thanks to this feature, TELUS blocks up to 40% of calls intended for its customers.[74]

Mr. Daniels explained that Bell developed algorithmic technology that identifies fraudulent callers. Bell anticipates this technology will block 120 million illegitimate calls per month. As per the *Telecommunications Act*, Bell requested the CRTC's approval to undergo a three-month trial during which the company will block illegitimate calls.[75]

Mr. Howard Slawner, Vice-President at Rogers, also explained that every stakeholder can help raise awareness about fraud calls.[76] In addition to making information available on its website to help its customers protect themselves, Rogers also engages in targeted awareness campaigns. For example, when it notices that a scam targets a particular community, Rogers puts ads in local newspapers in that community's language of choice.[77] Rogers also claimed to collaborate with other major carriers to develop industry-wide filtering solutions.[78]

TSPs provided different responses when asked if they charge their customers for these screening features. The Committee heard that TSPs may charge customers for at least some of the features that reduce nuisance calls delivered through their networks.[79] Representatives from TELUS explained that it offers its call-filtering features, including call control, free of charge to most of it residential customers.[80] Bell charges customers for its caller-ID features, but does not plan do so for its new call-blocking technology.[81]

74 Ibid., 1225-1230. TELUS, *Brief Submitted to INDU*, 9 March 2020. But see INDU, *Evidence*, 12 March 2020, 1130 (Lawford).

75 INDU, *Evidence*, 10 March 2020, 1210, 1240, 1255 (Daniels).

76 Ibid., 1210-1215 (Slawner). See also CEA, *Brief Submitted to INDU*, 28 April 2020.

77 INDU, *Evidence*, 10 March 2020, 1235 (Evans). But see INDU, *Evidence*, 12 March 2020, 1245 (Schroeder).

78 INDU, *Evidence*, 10 March 2020, 1210 (Slawner).

79 INDU, *Evidence*, 12 March 2020, 1140 (Gamble).

80 INDU, *Evidence*, 10 March 2020, 1220, 1240-1245 (Birot).

81 Ibid., 1240, 1250 (Daniels).

Mr. Slawner could not confirm whether or not Rogers charges its customers for call ID or blocking features.[82]

Mr. Lawford suspected that TSPs will attempt to pass on the cost of implementing STIR/SHAKEN and other new features to their customers. He argued that customers should be given these features free of charge given that reducing and preventing nuisance calls is in the interest of the telecommunications sector as a whole. If TSPs charge their customers for these features, Mr. Lawford calls for the CRTC to regulate and monitor their prices.[83]

UNAUTHORIZED PORTING

Witnesses drew the Committee's attention to unauthorized porting, also known as "SIM-swapping." "Porting" refers to the transfer of a phone number between service providers.[84] "Unauthorized porting" occurs when a person's phone number is transferred or "swapped" from one SIM card to another without the person's authorization. Unauthorized porting locks its victim out of their phone as any calls and texts sent to that number are directed to the fraudster's device. Redirecting these telecommunications enables a fraudster to commit further wrongdoings, such as theft, account takeover, and impersonation. A fraudster may for example use text-based authentication to reset a password associated to an account in order to access information therein. Unauthorized porting can therefore have disastrous, long-lasting consequences for their victim.[85]

According to Mr. Randall Baran-Chong, Co-Founder of Canadian SIM-swap Victims United, fraudsters carry out SIM-swap scams by exploiting federal wireless number portability (WNP) rules. Meant to increase competition in the telecommunications market, WNP rules enable consumers to easily transfer their phone number form one TSP to another.[86] A fraudster may execute a SIM-swap scam by impersonating their intended victim by using very little information – the intended victim's phone number and either their account number, their device's identification, or a PIN – and contacting a

82 Ibid., 1245 (Slawner).

83 INDU, *Evidence*, 12 March 2020, 1115, 1140, 1150 (Lawford).

84 INDU, *Evidence*, 10 March 2020, 1230 (Evans); INDU, *Evidence*, 12 March 2020, 1215 (Randall Baran-Chong, as an individual).

85 INDU, *Evidence*, 12 March 2020, 1220 (Baran-Chong); Randall Baran-Chong, *Brief Submitted to INDU*, 12 March 2020.

86 Baran-Chong, *Brief Submitted to INDU*, 12 March 2020. See *Telecom Decision CRTC 2005-72*, 20 December 2005.

TSP's customer service to port their phone number from one SIM card to another. The TSP will oblige and, in compliance with WNP rules, execute the porting with little obstacle and in as fast as two hours and a half.[87]

According to Mr. Baran-Chong, victims have limited means to protect themselves once a TSP executes the porting. The fraudster may keep watch on their intended victim through social media and wait for a moment where they might have limited access to their phone to carry out the scam. Once they understand what happened, the victim may not be able to retrieve control of their phone number quickly given that TSPs generally do not offer round-the-clock customer service. Fraudsters can commit damaging wrongdoings in a short period of time. Little to no compensation is offered to victims of unauthorized porting.[88]

While the CRTC and TSPs are developing measures against unauthorized porting,[89] Mr. Baran-Chong claimed that much remains to be done to protect Canadians. Mr. Baran-Chong called for raising public awareness of SIM-swap scams and increased coordination between law enforcement agencies. He also argued for stricter and consistent regulations requiring mandatory pre-porting notifications and verifications. He argued that Canadian governments, TSPs, financial institutions, and other businesses should move away from text-based, two-factor authentication towards more secure authentication systems. He suggested drawing inspiration from other jurisdictions that have been proactive in their response against unauthorized porting, such as Australia, South Africa, and the United States.[90]

Both PIAC and ISCC supported Mr. Baran-Chong's call for the CRTC to conduct a public inquiry into unauthorized porting.[91] Mr. Lawford and Mr. Baran-Chong criticized the CRTC and TSPs for having only limited discussions on the matter behind closed doors, without sufficiently involving victims of SIM-swapping and the larger public. While they acknowledge that some information must be kept from fraudsters, such informal

87 INDU, *Evidence*, 12 March 2020, 1215 (Baran-Chong); Baran-Chong, *Brief Submitted to INDU*, 12 March 2020. See also INDU, *Evidence*, 12 March 2020, 1230 (Evans); Canadian Wireless Technology Association (CWTA), *Brief Submitted to INDU*, 28 April 2020.

88 INDU, *Evidence*, 12 March 2020, 1240, 1255 (Baran-Chong).

89 See for example INDU, *Evidence*, 10 March 2020, 1230 (Evans).

90 INDU, *Evidence*, 12 March 2020, 1220-1225, 1235-1240, 1250 (Baran-Chong). Baran-Chong, *Brief Submitted to INDU*, 12 March 2020.

91 INDU, *Evidence*, 12 March 2020, 1130 (Gamble); Ibid., 1135 (Lawford).

discussions would not enable the transparent development of an effective response against unauthorized porting.[92]

The Canadian Wireless Telecommunications Association (CWTA) defended Canadian TSPs' response to unauthorized porting. TSPs – including Bell, Rogers, and TELUS – are part of the WNP Council, which develops and maintains porting processes and specifications. The CWTA claimed that the WNP Council is formulating industry-level safeguards against unauthorized porting. The WNP Council cooperated with the CRTC on this matter by providing information the latter requested. According to the CWTA, a "public consultation will not add any value to this ongoing work, but will instead divert resources from the implementation of the additional safeguards being developed."[93] The CWTA also expressed concern that a public inquiry into unauthorized porting would only reveal to fraudsters the substance of these safeguards and how to circumvent them.[94]

COVID-19–RELATED FRAUD

Fraud targeting Canadians has increased during the COVID-19 pandemic. Between January and April 2020, the RCMP observed that the number of fraud reports increased by 25% over the same period last year.[95] While fraudsters deliver scams through the usual channels – mainly texts and emails, but also phone calls and the Web – they take advantage of uncertainties, anxieties, and misinformation surrounding the pandemic to fool their victims:

> 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.[96]

Assistant Commissioner Slinn insisted that while some groups are more vulnerable than others, everyone is at risk. Indeed, organized crime organizations are using fraudulent

92 Ibid., 1120, 1135 (Lawford); Ibid., 1235 (Baran-Chong); Baran-Chong, *Brief Submitted to INDU*, 12 March 2020.

93 CWTA, *Brief Submitted to INDU*, 28 April 2020.

94 Ibid.

95 INDU, *Evidence*, 43rd Parliament, 1st session, 20 May 2020, 1525, 1640 (Slinn & Larocque).

96 Ibid., 1525 (Slinn). See also ibid., 1635, 1650 (Larocque).

means to misappropriate public funds Canadian governments have allocated to relief measures.[97]

Other witnesses also observed a surge in fraud targeting Canadians during the pandemic. Jean-François Fortin, Executive Director of Enforcement at the Autorité des Marchés Financiers (AMF), reported financial scams tricking victims into investing in fake treatments and vaccines, as well as an increased risk of insider trading due to delays in the release of financial reports.[98] Scott Jones, head of Communications Security Establishment's (CSE) Canadian Centre for Cyber Security (CCCS), also reported on COVID-19–related fraud, such as phishing campaigns and malware scams in which fraudsters impersonate public health organizations to defraud Canadians of their money and private information.[99] Simon Marchand, chief fraud prevention officer at Nuance Communications, reported a significant increase of COVID-19–themed phishing scams in recent weeks that could threaten their victims with identity theft for months, if not years. Mr. Marchand also argued that unsupervised teleworking may give ill-intentioned employees more opportunities to misappropriate private, sensitive information.[100]

CSE warned that the pandemic puts Canadian cybersecurity at risk. Considering reports of recent cyberattacks targeting Canadian intellectual property, Mr. Jones indicated that malicious actors will see health and research organizations involved in the national pandemic response as tempting targets. CSE is working with organizations that have reported suspicious activities related to COVID-19–research to determine their nature, their origin, and whether they were successful.[101] Like fraud, most cyberattacks appear to originate from overseas.[102]

In reaction to the increase in fraud reports, the RCMP redirected financial resources and dedicated a specific program to coordinate its response. The CAFC leads intelligence gathering and analysis as well as public outreach efforts while the RCMP collaborates with local police organizations as well as its national and international partners to exchange intelligence and coordinate law enforcement.[103] Assistant Commissioner Slinn assured the Committee that, while the RCMP always welcome more resources to fight

97 Ibid., 1525, 1610 (Slinn).

98 Ibid., 1500, 1610, 1615 (Autorité des marchés financiers, Jean-François Fortin).

99 Ibid., 1515, 1605, (Communications Security Establishment, Scott Jones).

100 Ibid., 1520 (Nuance Communications, Simon Marchand).

101 Ibid., 1515, 1540, 1635-1640 (Jones).

102 Ibid., 1505 (Canadian Internet Registration Authority [CIRA], Byron Holland).

103 Ibid., 1525, 1635 (Slinn).

fraud and despite transitioning to teleworking, the CAFC is sufficiently staffed to fulfill its functions.[104]

Law enforcement, however, has limits. Given the vast number of fraud reports, it is not possible for the RCMP and other police organizations to pursue every case. The fact that most fraudsters operate overseas further complicates enforcement and increases reliance on the activities of international partners. The RCMP nonetheless encourages local police organizations to pursue fraud cases through its engagement with the Canadian Association of Police Chiefs, and by sharing of intelligence through the CAFC and Criminal Intelligence Service Canada. Feeling they could still do more, RCMP representatives argued that police organizations could dedicate more resources and efforts to combatting fraud.[105]

Given the limitations of law enforcement, the RCMP and other witnesses emphasized that public awareness remains the most effective way to prevent fraud.[106] The AMF responded to the COVID-19–related fraud by warning and offering its assistance to consumer and senior protection associations, and communicating information through its partners. The AMF also ran a public awareness campaign on television, the Web, and social media from 6 April and 5 May 2020, with efforts to specifically reach seniors and other vulnerable groups.[107] As for the RCMP, the police organization distributed and posted bulletins on its website and social media to warn against COVID-19−related fraud.[108]

The Canadian Internet Registration Authority (CIRA), the operator of the ".ca" registry, also leads public awareness initiatives to increase cybersecurity and reduce vulnerability to online fraud. CIRA's Cybersecurity Awareness Training is a training platform helping users identify fraud, fake news, misinformation, and scams. CIRA also offers a free cybersecurity course to help Canadians working from home protect themselves and their organizations against cyber threats.[109]

In April 2020, CIRA launched the "CIRA Canadian Shield" to further help prevent online fraud and cyber attacks. The Canadian Shield is a free firewall service that prevents its users from accessing known malicious websites, based on intelligence provided by CSE.

104 Ibid., 1605.

105 Ibid., 1610, 1630-1635, 1645-1650 (Slinn & Larocque).

106 Ibid., 1525, 1610, 1645-1650; Ibid., 1610 (Fortin).

107 Ibid., 1500-1505 (Fortin).

108 Ibid., 1650 (Larocque).

109 Ibid., 1530-1535 (Holland).

Byron Holland, President and Chief Executor of CIRA, testified that 50,000 Canadians are currently using its Canadian Shield. CIRA also provides enterprise cybersecurity services to Canadian hospitals, schools, universities, and municipalities.[110] More generally, CIRA ensures that individuals and organizations do not use the .ca domain name for fraudulent purposes, notably through its registration and auditing processes. Mr. Holland assured the Committee that the .ca websites remain safe for Canadians to use despite the increase of COVID-19–related fraud.[111]

Through the work of its CCCS, CSE plays an important role to maintain cybersecurity in Canada. Its activities include raising public awareness of cyber threats, especially with vulnerable entities such as Canadian health and research organizations, and contributing to the removal of fraudulent websites. CSE also monitors and protects important federal programs against cyber threats, including the Canadian Emergency Response Benefit web application. CSE works proactively to help public and private organizations protect themselves against cyber threats, for example by providing information and early warnings to potential targets as well as assistance to victims of cyberattacks.[112]

Mr. Marchand recommended other measures to further protect Canadians against fraud and improve cybersecurity. He supported transitioning from current means of identification, such as social insurance numbers, driver licences, and health insurance cards, to more advanced and secure ones, specifically biometrics.[113] He also recommended that the federal government should require companies in federally regulated industries, such as banks and telecommunications carriers, to disclose to an individual when their information was used in an attempt to open a fraudulent account. Such early warning would help victims of identity theft better protect themselves. Mr. Marchand also argued that these companies should enhance visibility in their identification and authentication processes by disclosing, on a yearly basis, how many accounts they opened on the basis of fraudulently obtained information.[114] While Assistant Commissioner Slinn suspects organizations will avoid disclosing such information to maintain consumer confidence and the integrity of their processes,[115]

110 Ibid., 1505; Ibid., 1550 (Jones).

111 Ibid., 1505, 1530, 1545 (CIRA, Holland & Albert Chang).

112 Ibid., 1520-1525, 1605, 1620 (Jones).

113 Ibid., 1655 (Marchand).

114 Ibid., 1550, 1600, 1625.

115 Ibid., 1555, 1630 (Slinn).

Mr. Fortin believed that Mr. Marchand's proposal would increased transparency and public awareness.[116]

Finally, Mr. Marchand recommended deploying the STIR/SHAKEN framework as soon as possible. While he acknowledged STIR/SHAKEN's limitations, the biggest of which being that it will only apply to calls originating from Canada and the United States, the framework will still help consumers and businesses identify potentially fraudulent calls. Mr. Marchand also finds it crucial to implement STIR/SHAKEN promptly to prevent fraudsters from increasing their activities in Canada after the framework is implemented in the United States.[117]

COMMITTEE OBSERVATIONS AND RECOMMENDATIONS

In making recommendations, the Committee keeps in mind that, given the current legislative framework, the federal government has limited direct power over the activities and decisions of arms-length organizations such as the RCMP and the CRTC. Nonetheless, the federal government can encourage and support these organizations in addition to assuming responsibilities of its own.

Federal and provincial authorities cannot protect Canadians against fraud if they do not have sufficient data to inform policing and policymaking. Raising public awareness about fraud is crucial to help Canadians protect themselves. Authorities and other stakeholders should adapt information materials to their intended audience and the circumstances. This could include disseminating materials in a language other than French or English, when appropriate. The Committee therefore recommends:

Recommendation 1

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

Recommendation 2

That the Government of Canada work with the Canadian Radio-television and Telecommunications Commission, telecommunications service providers, and police

116 Ibid., 1555 (Fortin).

117 Ibid., 1615-1620, 1655 (Marchand).

enforcement agencies to increase and improve information available to Canadians about fraud calls.

To further increase public awareness and transparency, the federal government and Canadians should have some visibility into the manner and the number of times that federally regulated businesses notify victims of identity theft as soon as possible after fraud is detected. While the Committee acknowledges that these businesses should notify victims of identity theft as soon as possible, any legal obligation to do so should account for the fact that fraudsters will avoid giving these businesses the means to contact their victims.

Recommendation 3

That the Government of Canada introduce legislation requiring businesses in federally regulated industries, such as banks and telecommunications carriers, to publicly disclose each year how many accounts they discovered had been opened using fraudulent information and how many individuals they contacted to notify them that their information was used for fraudulent purposes.

As underlined by the RCMP, the CRTC, and other witnesses, collaborating with domestic and foreign partners is a crucial component of an effective response against fraud calls targeting Canadians. The federal government should facilitate such collaborations, both at home and abroad. The Committee therefore recommends:

Recommendation 4

That the Government of Canada increase its collaboration with foreign governments and international organizations to close overseas fraud call centres and prosecute fraudsters targeting Canadians, and include fraud prevention considerations in any current and future trade agreements.

Recommendation 5

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

Despite the technical challenges it raises, the Committee supports the implementation of the STIR/SHAKEN framework and acknowledges the CRTC’s determination to see it

deployed as soon as possible and in close collaboration with TSPs. The Committee encourages the CRTC to re-examine the involvement of small carriers in order to maintain competition in the telecommunications market. The federal government can and should lend support to these small carriers. The Privacy Commissioner of Canada should also examine privacy issues raised by STIR/SHAKEN. The Committee therefore recommends:

Recommendation 6

That the Government of Canada support the involvement of smaller carriers in the implementation of the STIR/SHAKEN framework in order to maintain competition in the telecommunications market.

Recommendation 7

That the Government of Canada request the Privacy Commissioner of Canada to examine potential privacy issues raised by the implementation of the STIR/SHAKEN framework.

The federal government or the CRTC could require that TSPs charge Canadians little to nothing for features that help reduce or prevent fraud calls delivered through their networks. On the other hand, the Committee observed that the telecommunications industry largely drives the development of these features. Given that combatting fraud is an "arms race," TSPs must have incentives to invest in the development of countermeasures. The federal government and the CRTC must therefore find the right balance between making these features as widely available as possible while encouraging innovation. The Committee therefore recommends:

Recommendation 8

That the Government of Canada support the development of industry-based solutions against fraud calls at a reasonable cost for consumers.

Recommendation 9

That the Government of Canada encourage the Canadian Radio-television and Telecommunications Commission to monitor and consider the cost of industry-based solutions against fraud calls when making decisions that affect the affordability of telecommunications services.

The federal government should examine whether current criminal provisions can effectively protect Canadians against fraud calls, including those initiated via robocalls. While this review could lead to introducing legislation that specifically prohibits

defrauding or attempting to defraud a person through vocal telecommunications, the Committee does not endorse the proposition to mandate the CRTC to enforce criminal legislation. Beyond the practical challenges associated with building capacity to lead criminal investigations, it may distract the CRTC from what should be its main focus: enabling Canadians to safely use their phones by coordinating TSPs, notably through regulations. The Committee therefore recommends:

Recommendation 10

That the Government of Canada review legislation pertaining to fraud to ensure that it adequately and explicitly prohibits fraud calls, including fraud calls initiated by robocalls, and further review criminal fines, penalties, and enforcement with regards to Canadian and international laws.

Recommendation 11

That the Government of Canada review directives and authorities issued to the Canadian Radio-television and Telecommunications Commission to ensure that protection against fraud delivered through vocal telecommunications is sufficiently integrated in Canadian telecommunications policy in order to best protect the public.

The Committee joins Mr. Randall-Chong, ISCC, and PIAC in urging the CRTC to conduct a formal public inquiry into unauthorized porting. Federal authorities as well as TSPs, financial authorities, and other stakeholders must tackle this emerging threat and quickly formulate countermeasures. Testimony presented to the Committee shows that a new balance between competition and security must be found relative to porting. As much as possible, regulations and other countermeasures should be developed in a transparent manner by involving the public, including victims of SIM-swapping.

Recommendation 12

That the Government of Canada support efforts by the Canadian Radio-television and Telecommunications Commission to conduct a public inquiry into unauthorized porting.

Recommendation 13

Should the Canadian Radio-television and Telecommunications Commission fail to launch a public inquiry into unauthorized porting within six months, that the Government of Canada introduce legislation to protect Canadians against unauthorized porting.

The COVID-19 pandemic is putting lives and livelihoods at risk, and the Canadian economy in jeopardy. The federal government must prevent any further harm to Canadians. In the short term, increasing public awareness remains the most effective way to counter COVID-19−related fraud. Time being of the essence, the federal government must act now.

Recommendation 14

That the Government of Canada launch a month-long, public awareness campaign in Canadian local and national media, to warn Canadians against COVID-19–related fraud.

Recommendation 15

That the Government of Canada work toward becoming an international leader in the prevention of fraud by reviewing progress on these recommendations one year from now with a report from all relevant ministers to the House of Commons, and then refer it to the appropriate Committee.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Bell Canada	2020/03/10	7
Jonathan Daniels, Vice-President Regulatory Law		
Canadian Radio-television and Telecommunications Commission	2020/03/10	7
Ian Scott, Chairperson and Chief Executive Officer		
Steven Harroun, Chief Compliance and Enforcement Officer		
Alain Garneau, Director Telecommunications Enforcement, Compliance and Enforcement Sector		
Rogers Communications Inc.	2020/03/10	7
Howard Slawner, Vice-President Regulatory Telecommunications		
Deborah Evans, Chief Privacy Officer		
Royal Canadian Mounted Police	2020/03/10	7
Eric Slinn, Assistant Commissioner Federal Policing Criminal Operations		
Guy Paul Larocque, Acting Inspector Canadian Anti-Fraud Centre		
Telus Communications Inc.	2020/03/10	7
John MacKenzie, Director Regulatory Affairs		
Jérôme Birot, Vice-President Voice and Services Development Operations		

Organizations and Individuals	Date	Meeting
As an individual	2020/03/12	8
Randall Baran-Chong, Co-Founder Canadian SIM-swap Victims United		
Canadian Network for the Prevention of Elder Abuse	2020/03/12	8
Kate Schroeder, Board Member		
Internet Society Canada Chapter	2020/03/12	8
Matthew Gamble, Director		
Public Interest Advocacy Centre	2020/03/12	8
John Lawford, Executive Director and General Counsel		
Autorité des marchés financiers	2020/05/20	16
Jean-François Fortin, Executive Director, Enforcement		
Christian Desjardins, Director of Assessment and Inquiry		
Canadian Internet Registration Authority	2020/05/20	16
Albert Chang, Corporate Counsel		
Dave Chiswell, Vice-President, Product development		
Byron Holland, President and Chief Executive Officer		
Communications Security Establishment	2020/05/20	16
Scott Jones, Head, Canadian Centre for Cyber Security		
Nuance Communications	2020/05/20	16
Simon Marchand, Certified Fraud Examiner and Certified Administrator, Biometrics and Security		
Royal Canadian Mounted Police	2020/05/20	16
Guy Paul Larocque, Acting Inspector, Canadian Anti-Fraud Centre		
Eric Slinn, Assistant Commissioner, Federal Policing Criminal Operations		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Baran-Chong, Randall

Canadian Electricity Association

Canadian Network for the Prevention of Elder Abuse

Canadian Wireless Telecommunications Association

COMsolve Inc.

Telus Communications Inc.

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 7, 8, 16, 27 and 29) from the 43rd Parliament, First Session and (Meeting No. 2) from the 43rd Parliament, Second Session is tabled.

Respectfully submitted,

Sherry Romanado
Chair