Ms. Sherry Romanado, M.P.
Chair
Standing Committee on Industry, Science and Technology
House of Commons
Ottawa, Ontario K1A 0G6

Dear Colleague:

On behalf of the Government of Canada (the Government), we are pleased to respond to the first report of the Standing Committee on Industry, Science and Technology entitled *Fraudulent Calls in Canada: A Federal Government's First Start*, pursuant to Standing Order 109 of the House of Commons.

The Government extends its gratitude to the Committee for its work in studying fraudulent calls in Canada and for the Committee's efforts in developing this report and its recommendations. The report demonstrates the Committee's dedication to counter fraudulent calls. The Government has carefully considered the report and its recommendations, and agrees that these scams are a significant source of concern, in light of the considerable financial and emotional impacts that they can have on Canadians. The Government continues to take concrete actions to deliver on the report recommendations and to explore ways in which its frameworks, policies, programs, and international collaborative activities can be further improved to counter fraudulent calls for the benefit of all Canadians.

In its response, the Government first outlines the roles and responsibilities of key federal organizations in addressing the issue of fraudulent calls, including the Royal Canadian Mounted Police (RCMP), the Canadian Radio-television and Telecommunications Commission (CRTC), and the Competition Bureau, as well as the manner in which legislative frameworks and international collaboration enable them to effectively combat fraudulent calls. The Government then presents efforts under way to increase public awareness of fraudulent calls, to facilitate information exchanges between organizations fighting such scams, to inform and empower Canadians to prevent becoming victims of fraud, and to monitor and report progress achieved. Finally, the response describes the measures currently in place to combat fraudulent calls, along with the ongoing work to

…2

develop additional effective measures in a world where technology and scams are ever changing.

Introducing new legislation, and reviewing existing legislation and authorities (recommendations 3, 5, 10 and 11)

This first section describes the roles and responsibilities of the key federal organizations involved in tackling the issue of fraudulent calls, as well as the legislation and authorities that enable them to do so.

As noted in the report, in undertaking its duty to enforce Canada's laws, including those in the *Criminal Code*, the RCMP investigates fraud at the federal level when there is a connection to organized crime, and responds directly to individual fraud-related complaints when it has jurisdiction in an area through contract policing. The CRTC fights fraud calls less directly by advancing the objectives of the *Telecommunications Act* and enforcing orders under that Act against unsolicited telecommunications, which may or may not constitute fraudulent calls. In turn, the Competition Bureau also investigates fraudulent or deceptive telemarketing, as the *Competition Act* includes a specific provision related to these activities (section 52.1). This provision is broad and applies to traditional interactive calls and recorded calls, including robocalls.

The Government agrees that it is important to ensure that our criminal laws remain clear and contemporary, and to provide the necessary tools to respond to fraud in its various forms. The *Criminal Code* effectively prohibits the myriad of ways in which fraud can be committed, including fraud initiated by robocalls, through numerous offences contained in Part X, including the general fraud offence found under section 380. Further, sentencing courts are required to consider specifically enumerated aggravating factors relating to fraud, such as its complexity and magnitude, in determining a fit sentence. Fraud committed against seniors, who are often the victim of scam calls, will also constitute an aggravating factor where the offence had a significant impact on the victim based on their personal circumstances, such as their age, health, and financial situation. An offender may be sentenced up to a maximum term of 14 years imprisonment, may be required to pay a fine or restitution to the victim, and may also be prohibited from work that involves having control over the property of others.

The Government also recognizes the challenges associated with investigating fraud, as perpetrators hide behind technology, and often commit their crimes by crossing over multiple jurisdictions, often targeting Canadians from other countries. Given the transnational nature of many fraudulent calls, international cooperation is critical. Canada's laws provide a broad framework to facilitate international legal cooperation, including with respect to fraud, and Canada continues to work closely with its international partners to ensure that transnational offenders are held accountable.

…3

The RCMP has been steadfast in its commitment to combat fraud. For example, in October 2018, the RCMP commenced Project OCTAVIA. As part of this investigation, the RCMP and other Canadian law enforcement bodies successfully worked with law enforcement agencies in the United Kingdom, the United States, and India to target fraudsters who impersonated Canada Revenue Agency (CRA) employees, as well as other interrelated frauds involving criminals operating overseas. As of December 2020, the investigation had resulted in the closing of at least 39 call centres in India and the RCMP charging at least 10 individuals. Effective RCMP international enforcement work is ongoing.

With respect to legislative frameworks and policy guidance for telecommunications, the CRTC is empowered to take a wide range of actions to help combat unsolicited and fraudulent calls, protect consumers, and to embed these considerations in its ongoing work. Actions include the ongoing administration of the Do Not Call List (DNCL), the Unsolicited Telecommunications Rules, measures to block calls at the network level including a trial using artificial intelligence, the implementation of STIR/SHAKEN to authenticate calls, a call-trace regime to help aid in enforcement, cooperation with international partners, and improved information for consumers on call features available to better manage unwanted calls. The CRTC also has different codes of conduct and other regulatory frameworks to protect consumers. The CRTC plans to review these again as part of its future work. Further information on the implementation of these initiatives is outlined in the section below.

The CRTC is guided by the objectives of the *Telecommunications Act*, as well as section 41 and related provisions that give the CRTC specific powers to prohibit or regulate unsolicited calls, which may or may not constitute fraudulent calls. The CRTC is also guided by binding policy directions. In particular, in 2019 the Government issued a direction to the CRTC to promote competition, affordability, consumer interests and innovation.[1] This direction is a binding order that directs the CRTC to consider certain factors when making decisions and provides guidance on the means to achieving the policy objectives and the measures to use when relying on regulation.

The Government appreciates the need to review frameworks periodically. This is reflected in recent work by the Broadcasting and Telecommunications Legislative Review (BTLR) Panel and its broad review of existing communications legislation in Canada. Among other areas of its review, the BTLR Panel was directed to examine whether further improvements pertaining to consumer protection were warranted.

…4

[1] *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives to Promote Competition, Affordability, Consumer Interests and Innovation*; available at: https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11524.html.

Furthermore, the Government recognizes the need for various government departments and agencies to share data and confidential information while fighting fraudulent and unsolicited telecommunications. The Government agrees with the Committee on the importance of privacy rights being respected when information is shared. There are information sharing provisions within various pieces of legislation to enable the sharing of confidential information, and the Government is actively reviewing several pieces of legislation and examining whether to expand these provisions, while balancing privacy considerations.

For example, the Committee's recommendations on data sharing with respect to the CRTC will be considered in the context of the Government's review of the recommendations made by the BTLR Panel. We note that under the *Consumer Privacy Protection Act*, a Government bill currently being considered by Parliament, there are provisions which allow for information sharing agreements between the Office of the Privacy Commissioner (OPC) and regulatory bodies, such as the Competition Bureau and the CRTC.

The Government also recognizes the importance of transparency around the breadth and frequency of data breaches and the resulting fraud from such activities within Canada. On November 1, 2018, all businesses, including banks and telecommunications carriers, became subject to new mandatory breach reporting regulations under Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Organizations are required to inform the OPC of any breach of security safeguards involving personal information that may pose a real risk of significant harm to individuals. In addition, they must notify the affected individuals about these breaches and keep records of all data breaches within the organization, which the OPC may review. Furthermore, in December 2018, Parliament passed over 60 new or enhanced measures to protect bank customers, including a requirement for banks to make the number and nature of consumer complaints, including those related to fraud, available on their website on an annual basis. Banks must include a description of the consultations undertaken in respect to complaints received in their Public Accountability Statement, and the Financial Consumer Agency of Canada includes a summary of these complaints in its Annual Report to Parliament.

The Government will continue to monitor the effectiveness of its legislation and other authorities in addressing and reporting the issue of fraudulent calls, and pursue updates as necessary, in general and as part of legislative review efforts under way.

…5

Increasing international collaboration to close fraud call centres, prosecute fraudsters, and include fraud prevention considerations in trade agreements (recommendation 4)

As noted above, as fraudulent calls can originate from other countries, effective international collaboration is essential to deter and prevent fraudulent activities. In addition to collaborating from a legal perspective, the Government will continue to engage and foster collaboration internationally in enforcement and fraud prevention activities.

The RCMP's International Network has offices in 30 cities, located in 26 countries. Canadian police investigators and other law enforcement personnel seek assistance from RCMP officers abroad to pursue investigations that go beyond Canada's borders. Canadian law enforcement officials continue to collaborate with foreign counterparts to make arrests and close fraud call centres. Project OCTAVIA, addressed earlier, is a recent example of effective RCMP international enforcement work in this area.

Further, the Competition Bureau meets regularly with domestic and international partners to address cross border problematic conduct and to develop common approaches to similar issues. The Government is supportive of exploring options for including fraud prevention considerations in future trade agreements and other cooperation instruments. This could include provisions on increased cooperation and collaboration, information sharing, and joint public awareness initiatives on fraudulent and deceptive marketing practices.

Improving the availability and accessibility of information concerning fraudulent calls and progress on countermeasures, as well as increasing the awareness of Canadians of such scams (recommendations1, 2, 14 and 15)

In addition to a strong legislative framework and effective international collaboration, the best tool in combatting fraudulent calls may be increasing consumer awareness by sharing information concerning current threats. Organizations that are mandated to counter fraud must also have effective information sharing measures to advance a cohesive approach to prevent, mitigate, deter, and respond to current and emerging scams.

As set out in the Committee's report, the RCMP, the Competition Bureau, and the Ontario Provincial Police operate the Canadian Anti-Fraud Centre (CAFC). The CAFC is the central repository for mass marketing fraudulent complaints, including those related to telemarketing. Canadian police services share information on fraudulent incidents with the CAFC for analysis and operational purposes.

…6

The CAFC is a key organization when it comes to increasing the availability and accessibility of fraud data. This organization works closely with national and international partners to proactively identify emerging domestic and international scams and threats. When it receives information on a fraud case, the CAFC analyzes the associated data and disseminates relevant information to numerous partners, including law enforcement organizations, telephone companies, email service providers, financial institutions, and credit card companies. In so doing, it could hinder communications between fraudsters and potential victims, and, at times, it successfully contributed to blocking the receipt and laundering of victims' funds. To further the availability of fraud prevention information and data, the CAFC began co-chairing the Fraud Prevention Forum with the Competition Bureau. The Fraud Prevention Forum is an information sharing body for a multitude of fraud prevention stakeholders across Canada.

The Government also recognizes the importance of information as a front-line tool for Canadians to prevent fraud. That is the reason why the CAFC publishes data on the number of fraudulent activities reported, the number of victims, and the associated cost of fraud each year. Furthermore, CAFC's website includes an up-to-date list of scams, including by type of medium, such as telephone, as well as information for Canadians about how to protect themselves from fraud and what to do if they are a victim of fraud.

Moreover, through the Uniform Crime Reporting Survey, Statistics Canada collects data on all crime reported to the police, including attempted crimes. The information includes police-reported fraud and attempted fraud via telephone calls. Statistics Canada will continue to work with law enforcement agencies and other partners to advance the public release of statistics on fraudulent calls.

To increase consumer awareness of frauds, the Competition Bureau and the CAFC have conducted a public awareness campaign to promote the Fraud Prevention Month in March for the past 16 years. This year, the theme for Fraud Prevention Month will be the digital economy of scams and frauds, with COVID-19 related fraud as a strategic consideration. Further, as the pandemic presents uncertain and anxious times for Canadians, the CAFC, along with federal organizations—including the CRA, Competition Bureau, and the RCMP—have produced a number of information products concerning COVID-19 related fraud. These are accessible on their respective websites, as well as through various social media platforms. Notably, the CRA invested $4 million last year to raise awareness of COVID-19 related fraud through their "Slam the Scam" campaign using various tools, such as search engine marketing.

The Government is also taking steps to enhance the quality of information on fraud in Canada by improving the processes by which Canadians can report fraud. For example, the National Cybercrime Coordination Unit (NC3) and the CAFC are developing a new

…7

National Cybercrime and Fraud Reporting System to improve the processes used to report fraud and cybercrime incidents to law enforcement. It is expected to be operational in 2022 and will help to improve the quality of data on fraud in Canada.

In addition, the Government will continue to monitor the progress of solutions combatting fraud and advance more transparent progress reporting. As the telecommunications industry continues to develop and implement solutions to combat these scams, the CRTC has required industry to file multiple status update reports to ensure transparency in their work.

The Government will continue to work closely with public and private stakeholders to promote fraud awareness for Canadians, and to explore the best options to inform Canadians of COVID-19 related fraud and the progress of countermeasures under way.

Implementing measures to combat fraudulent calls and illegal activities, while maintaining consumer privacy, competition, and affordability (recommendations 6, 7, 8, 9, 12 and 13)

The Government recognizes the importance of protecting Canadians from fraudulent and unsolicited telecommunications and the need to develop measures that combat these activities. As the volume and sophistication of scams and fraudulent activities increases, new measures must be developed to strengthen Canadian's trust in their telecommunications services. Provisions of the *Telecommunications Act* gives the Government broad powers to regulate and prohibit unsolicited telecommunications. The CRTC has leveraged this authority to set new requirements for industry to combat fraudulent telecommunications, as well as to establish a regime of requirements regarding unsolicited telecommunications, such as telemarketing.

A variety of measures have been introduced to combat fraudulent and unsolicited telecommunications in recent years. For example, the DNCL allows consumers to place their telephone and fax numbers on a registry to help reduce the number of telemarketing calls that they receive. The DNCL has been in operation for 12 years and includes over 14 million registered phone numbers. The CRTC has the power to issue monetary penalties against telemarketers who do not comply with the DNCL rules and in the 2019–2020 fiscal year, over $700,000 of financial penalties were issued against telemarketers who violated the DNCL rules, including a single penalty of over $100,000 against a non-compliant company.

Furthermore, in 2019, new CRTC requirements came into force which mandated that all telecommunication companies that did not offer their customers call filtering must block telephone numbers that are blatantly illegitimate, i.e., numbers that do not correspond to

XXX-XXX-XXXX, from reaching their destinations. The CRTC also imposed a requirement that industry develop call traceback solutions, which assist law enforcement in identifying callers who commit fraud. In addition, in 2020, the CRTC approved Bell's request to implement a trial call blocking solution that leveraged artificial intelligence. From March to September 2020, the trial prevented over 200 million nuisance calls from reaching Canadians. The CRTC is currently considering a subsequent request from Bell to make this solution permanent.

The CRTC has also required telecommunications service providers to implement the STIR/SHAKEN framework, which will notify Canadians if a call that they are receiving is from a trustworthy and verified number. This framework will directly combat scams where fraudsters "spoof" the Caller ID of organizations in an attempt to defraud their victims. In 2019, the CRTC established the Canadian Secure Token Governance Authority (CSTGA), which was a key step in the implementation of the STIR/SHAKEN framework. Through various industry-CRTC working groups, the CRTC is collaborating with telecommunications service providers to efficiently implement the new requirements that they have imposed, and leverage existing industry expertise to develop new solutions. By requiring the implementation of leading-edge technical solutions to fight fraudulent calls while collaboratively working with industry to ensure their successful implementation, the CRTC is contributing to a safer and stronger telecommunications sector in Canada.

The Government understands that the STIR/SHAKEN framework must support competition in the telecommunications market, which includes taking the needs of small carriers into consideration. The CRTC is currently looking into how small carriers will adopt the STIR/SHAKEN framework, and the CSTGA is also actively engaging with small carriers on their requirements. Furthermore, while the STIR/SHAKEN framework will be a key element to combat fraud and unsolicited telecommunications to protect consumers, the Government understands the need to consider any impact that the STIR/SHAKEN framework could have on the affordability of telecommunications services. That is why the Government issued the 2019 Policy Direction, which instructs the CRTC to consider, among others, the impact of its decisions on competition and affordability.

While the STIR/SHAKEN framework will be an important tool in the fight against fraudulent calls, it should be noted that the international standards and equipment needed to implement it are still under development. As a result, the CRTC has recently agreed to a request from the telecommunications industry to extend the deadline for the implementation of the STIR/SHAKEN framework until June 2021. This new deadline matches the implementation deadline in the United States, and will give the CRTC time to ensure that the framework is implemented in a way that maximizes benefits for

Canadians and reflects the range of telecommunications service providers involved. For example, the CRTC recently began proceedings to consider expanding the membership of the CSTGA and the role of smaller service providers.

In addition to considering affordability and competition, the Government must also consider privacy considerations. Privacy has long been considered a fundamental right in Canada. The Government recognizes that strong privacy protections are instrumental to the prosperity and security of Canadians. In the *Telecommunications Act*, the protection of the personal privacy of Canadians is listed as one of the objectives of Canada's telecommunications policy.

Canada's privacy framework situates consent as a key pillar to ensure that Canadians understand what they are consenting to, in particular, the nature, purpose, and consequences of the collection, use, or disclosure of their personal information. As noted above, the OPC has oversight responsibilities of PIPEDA and is mandated to protect and promote the privacy rights of Canadians. The OPC regularly participates in the regulatory proceedings at the CRTC and is welcome to provide input into the development of measures to combat fraudulent and unsolicited telecommunications, including the STIR/SHAKEN framework. The CRTC also understands the importance of maintaining consumer privacy in the telecommunications market and is currently conducting a regulatory proceeding on how telecommunications companies handle confidential customer information, what information should qualify as confidential customer information, and any resulting measures that should apply to the collection, use, and disclosure of that information.

The Government agrees that fraudulent activity involving unauthorized porting of mobile phone numbers is a serious issue of a global nature. In Canada, rules regarding the customer transfer process are intended to help consumers switch providers if they choose to do so, reducing barriers to benefit from competition in the wireless market. However, fraudsters have leveraged these processes and the vulnerability of Canadians for nefarious purposes. While deeply concerning, these fraudulent activities are already a violation of the *Criminal Code* and do not warrant the creation of further legislation. The Government supports the independence of the CRTC and its ongoing efforts to combat porting fraud by working with industry to protect consumers. Since the beginning of 2020, the CRTC has been engaging regularly with the Canadian Wireless Telecommunications Association and members of the Wireless Number Portability Council on this issue. Activities include assessing interim measures, the implementation of a new enhanced verification industry-wide process to allow consumers to safely port their mobile phone number, as well as regularly collecting data from carriers on number transfers and SIM swapping, to allow the CRTC to continue to monitor this issue moving forward.

…10

Conclusion

The Government would like to reiterate its gratitude to the members of the Committee for their work and dedication to the completion of this study and combatting fraudulent calls for all Canadians. The Government will continue to work with key stakeholders and civil society to advance and examine ways in which to combat such fraud.

Sincerely,

The Honourable François-Philippe Champagne, P.C., M.P.
Minister of Innovation, Science and Industry

The Honourable Bill Blair, P.C., M.P.
Minister of Public Safety and Emergency Preparedness