Standing Committee on industry, science and technology

CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'industrie, des sciences et de la technologie

August 18, 2020

Hon. Navdeep Bains
Minister of Innovation, Science and Industry
Suite: 208, Wellington Building
House of Commons
Ottawa, Ontario K1A 0A6

Dear Minister Bains,

In the past months, the House of Commons Standing Committee on Industry, Science and Technology (the Committee) studied the influx of fraud calls to Canadians, Canada's Do-Not-Call List, the STIR/SHAKEN framework, and COVID-19−related fraud. While the Committee will report to the House of Commons on these matters, its members wanted to share some of their findings and observations with you at the earliest opportunity.

The evidence provided to the Committee shows that fraud calls continue to target Canadians. Supported by fraud call centres located overseas and easily accessible technologies, such as robocalls and spoofing, fraudsters have caused significant losses to their victims. Indeed, according to the Canadian Anti-Fraud Centre, fraud calls account for $25 million of the $98 million lost to fraud in 2019. While any Canadian can fall victim to fraud calls, seniors, low-income households, and newer Canadians remain especially vulnerable. Because of constantly evolving techniques and technology, authorities as well as telecommunications service providers (TSPs) and other stakeholders find it challenging to maintain up-to-date information on how fraudsters target and deliver fraud calls to Canadians. To fight fraud calls, witnesses highlighted the importance of supporting law enforcement through cooperation between international and national entities, raising public awareness, and implementing the STIR/SHAKEN framework as soon as possible – among other things.

Witnesses also drew the Committee's attention to unauthorized porting, or "SIM-swap" scams. The testimony suggests that fraudsters carry out SIM-swap scams by exploiting federal wireless number portability rules, which are meant to facilitate porting. Victims may have limited means to protect themselves once a TSP executes the porting. While the Canadian Radio-television and Telecommunications Commission (CRTC) and TSPs are developing measures against unauthorized porting, other witnesses argued that much remains to be done to protect Canadians. More specifically, they called for the CRTC to conduct a public inquiry into unauthorized porting.

Fraud targeting Canadians has increased during the COVID-19 pandemic. Between January 2020 and April 2020, the Royal Canadian Mounted Police (RCMP) observed that the number of fraud reports

increased by 25% over the same period last year. While fraudsters deliver scams through the usual channels – mainly texts and emails, but also phone calls and the Web – they now take advantage of uncertainties, anxieties, and misinformation surrounding the pandemic to fool their victims. The pandemic also puts Canadian cybersecurity at risk. For example, a representative of the Communications Security Establishment indicated that health and research organizations involved in the national pandemic response may attract the attention of malicious actors.

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 should act now by launching a public awareness campaign in Canadian local and national media to warn Canadians against COVID-19−related fraud. While the RCMP has redirected resources to respond to COVID-19−related fraud, witnesses reiterated that increasing public awareness remains the most effective way to prevent fraud and protect Canadians.

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.

To further increase public awareness and transparency, the federal government and Canadians should have visibility in the identification and authentication processes of federally regulated businesses. 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 refrain from giving these businesses the means to contact their victims.

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.
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 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 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 will urge 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 and by involving the public, including victims of SIM-swapping.

Thank you,

Sherry Romanado
Chair