Cyber Security and Cyber Fraud

Remarks by Andrew Ross

Director, Payments and Cyber Security

Canadian Bankers Association

for

Senate Standing Committee on Banking, Trade, and Commerce

October 26, 2017

Ottawa

CHECK AGAINST DELIVERY

ASSOCIATION DES BANQUIERS CANADIENS | CANADIAN BANKERS ASSOCIATION

EXPERTISE CANADA BANKS ON
LA RÉFÉRENCE BANCAIRE AU CANADA

Good morning. I would like to thank the Committee for the opportunity to speak with you today about cyber security and cyber fraud. As coincidence may have it, October is Cyber Security Awareness Month and so the Committee's hearings are timely. My name is Andrew Ross, and I am the Director of Payments and Cyber Security for the Canadian Bankers Association (CBA). Joining me are my colleagues Darren Hannah, the CBA's Vice President for Finance, Risk and Prudential Policy and Sandy Stephens, Assistant General Counsel.

The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

Banks in Canada are leaders in cyber security and have invested heavily to protect the financial system and the personal information of their customers from cyber threats. Despite the growing number of attempts, banks have an excellent record of protecting their systems from cyber threats. Banks take seriously the trust that has been placed in them by Canadians to keep their money safe and to protect their personal and financial information.

Canadians have come to expect greater convenience when using and accessing financial services, and banks have invested heavily to provide Canadians faster and more convenient ways to do their banking. Now consumers can bank anytime from virtually anywhere in the world through online banking and mobile apps, providing real-time access to their financial information. Today, 72 per cent of Canadians primarily do their banking online or on their mobile device. That's up from 52 per cent just 4 years ago.

As more banking and other transactions are done electronically, networks and systems are becoming increasingly interconnected. This requires banks, government, and other sectors to work together to ensure Canada's cyber security framework is strong and able to adapt to the digital economy.

As the Committee is well aware, the Department of Public Safety is currently leading a review of Canada's cyber security strategy. The CBA has been an active participant in those consultations and we would like to outline for the Committee many of the recommendations we have already submitted to the government.

Lead Federal Agency

The Canadian cyber security framework would benefit from having one lead agency within the federal government to deal with cyber threats. Within the current cyber security landscape there are many federal government departments and agencies that have oversight of different critical infrastructure sectors. An opportunity exists to integrate all of these government cyber activities across critical infrastructure sectors into one single government agency. This would improve Canada's resilience by developing common standards, enhancing coordination for intelligence sharing across sectors and with law enforcement, and providing a single point of interaction for consumers and businesses to report cyber-related incidents and cyber crimes.

Consistent Standards for Critical Infrastructure Sectors

The delivery of financial services relies on other sectors, such as telecommunications and electricity. Canadians need to be assured that all critical infrastructure sectors are protecting them from cyber threats. Therefore, we encourage the Government to create a consistent set of standards and rules for all critical infrastructure sectors. Consistent standards will provide stronger oversight and greater comfort to those using, and relying on, these services.

Block and Share Malicious Data Communications

The telecommunications sector is the conduit through which electronic data flows. Identifying and blocking malicious traffic, and sharing that information across sectors, would benefit consumers and businesses, including banks. Once a cyber threat is identified, allowing telecommunications providers to block known malicious traffic can help stop further transmission of bad data. Blocking bad data would significantly reduce the volume of malicious emails that target those most vulnerable such as consumers and small businesses. This would also limit the spread of viruses, botnets, and other forms of malicious software that target corporations and governments. It is our understanding that legislative changes are needed to allow telecommunications providers to proactively block bad traffic and we encourage the government to study legislative options for making this possible.

Canadian banks and other businesses are also customers of telecommunications companies. Enabling telecommunications companies to share threat information with relevant customers would help improve cyber resiliency. The converse is also true. The financial sector has invested heavily in

robust cyber resilience capabilities to identify malicious data on its systems. Sharing this information with telecommunications companies, and allowing them to block malicious end-points, would stop traffic from spreading to other businesses and consumers. Accordingly, any legislative changes should enable this two-way sharing of information.

Information Sharing to Build Cyber Resilience

The benefits from sharing threat information extend beyond the financial and telecommunications sectors to other sectors, government, and law enforcement. Rapid intelligence sharing of threats is a highly effective means of minimizing the impact of cyber attacks. In order to achieve timely sharing between the private sector and government agencies, improved sharing protocols and control integration is required. We support initiatives such as the Canadian Cyber Threat Exchange, which promotes the exchange of cyber security information and best practices between government and businesses.

While we support greater information sharing, we recognize that security and privacy go hand in hand. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) balances the privacy rights of individuals with the need of organizations to collect, use and disclose personal information in the course of carrying out their business. However, recent amendments to PIPEDA impede the ability of organizations to share personal information to detect, prevent and suppress cyber crime. Banks fully support and adhere to PIPEDA; however, a mechanism to share information about cyber criminals will be necessary to improve Canada's cyber resilience.

Cyber Awareness and Education

Similar to initiatives to improve financial literacy, we recommend the development of a national cyber literacy program. Cyber criminals often target ordinary citizens; thus greater cyber awareness is needed to reduce the number of victims. A national cyber literacy program, that educates and helps protect consumers, would help to deal with current and future threats.

Today, there is a global shortage of cyber security personnel. A talent pool to address the demand is required, both now and for the future. Building Canada's talent pool requires improved educational options for careers in cyber security, re-training options for the existing workforce, mature career-

development management practices, and creative cross-pollination with high-demand disciplines that are closely tied to cyber security. We believe Canada has an enormous opportunity to leverage our strong education system and to re-train our highly educated work force to fill that gap.

The Future Framework for Financial Services

As the financial sector undergoes tremendous change driven by technology, new entrants are able to deliver financial services digitally, fueling competition. Of course, increased competition has a positive impact in the marketplace, accelerating innovation and increasing choice for Canadians. Throughout this change, protecting consumers' security and privacy, while ensuring the safety, soundness and stability of the overall financial system in Canada, remains paramount.

Most new technology-based financial services firms are less regulated than established financial institutions, and many are largely unregulated. This makes it difficult to assess the cyber resilience of these firms. Some may have the same risk controls as banks; however, most will not possess the same depth of experience in defending and protecting data in the rapidly evolving digital threat environment. Further, the connected nature of financial services means that this growing list of market participants has the ability to spread cyber contagion throughout the sector. As a result, cyber resilience needs to be a central consideration for policy makers when defining the future framework for financial services.

Conclusion

In conclusion, I want to reiterate that cyber security is a priority for Canada's banks. They continue to collaborate and invest to protect Canadians' personal and financial information. And banks support the government's work to protect Canadians while promoting innovation and competition. However, the industry recognizes that threats and challenges are constantly evolving. We want to work more collaboratively with the government and with other sectors. In order to achieve that objective, we encourage the federal government to finalize and implement its renewed cyber security strategy to protect Canadians and improve Canada's cyber resilience.

Thank you very much for your time and I look forward to your questions.