Special consultations and public hearing on the issue of personal data breach at Desjardins

2019/11/21

Remarks by Éric Prudhomme,
Director (Quebec)

Delivered to the National Assembly of Quebec's Commission of Public Finance

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Good Afternoon. I would like to thank the Committee for the opportunity to speak with you today.

My name is Eric Prud'homme, and I am Director, Quebec Region for the Canadian Bankers Association. I am joined today by Angelina Mason, the CBA's General Counsel and Vice President. The CBA is the voice of more than 70 domestic banks, foreign bank subsidiaries and foreign bank branches operating in Canada. Banks employ 275,000 people in Canada, and nearly 45,000 people in Quebec, who 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.

For clarity, we would like to point out that the Mouvement des caisses Desjardins is not a member of the CBA which represents federally regulated banks subject to the Bank Act.

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. Banks employ teams of highly-skilled professionals in cybersecurity and data protection, and the banking sector invests heavily in technology and security measures. From 2007 to 2017, Canada's six largest banks spent more than $84 billion on technology, with a significant portion of those resources being focused on digital security measures. Canadian banks have an excellent record of protecting their systems and customers from ever-evolving cyber threats.

As federally regulated financial institutions, the CBA's members are subject to robust cyber security and privacy requirements established under legislation, regulation and through regulatory supervision. Privacy has always been a cornerstone of banking and strong measures to protect personal information have long been a part of banks' policies and practices.

The banking industry was the first to go beyond a statement of principles and develop a comprehensive privacy code of conduct in 1986. The values in this code are now reflected in the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which governs how organizations collect, disclose and provide access to personal information. The banks were among the first businesses subject to PIPEDA beginning in January 2001 and have an excellent record of compliance with the law.

All banks have comprehensive privacy policies in place and privacy officers that ensure that the policies are being followed and customer information is being protected, kept accurate and up-to-date as required by PIPEDA. We believe that PIPEDA has worked well to date to balance the protection of individuals' personal information with the legitimate use of personal information by organizations. PIPEDA is principles based and technologically neutral, providing the necessary framework for innovation as well as new technologies and business models. It is well positioned to continue that mandate going forward.

In the extremely rare instance of an occurrence, banks are required to report certain breaches of security safeguards involving personal information to the Office of the Privacy Commissioner of Canada (OPC), notify individuals affected by the incidents and notify organizations that can help to mitigate the harm from the incidents. In notifying affected individuals, banks must provide sufficient information to allow the individual to understand the significance to them of the breach and to take steps to reduce the risk of harm that could result or to mitigate that harm. In instances where a breach could result in significant harm, banks can, and do, monitor account activity in cases of suspected or actual breaches of personal information and, if there is unauthorized activity, help to stop any misuse. Moreover, banks may provide indemnification in certain circumstances for a loss of funds due to unauthorized transactions. Banks also can, and do, engage credit bureaus to assist in reducing the risk of harm.

Banks are also subject to the Office of the Superintendent of Financial Institutions' (OSFI) Technology and Cyber Security Incident Reporting requirements. If a federally regulated financial institution has a technology or cyber security incident that materially impacts the normal operations of that institution, that institution must report that incident to OSFI within 72 hours. Banks are also expected to update OSFI with information as it becomes available, including short-term and long-term remediation plans, and to provide a lessons-learned report. Additionally, banks' senior management teams are expected to review their institutions' cyber risk management policies and practices to ensure they remain appropriate and effective in light of changing circumstances and risks.

Cyber security and resiliency are collaborative priorities for banks in Canada. There is no competitive advantage to going it alone. As more banking and other transactions are done

electronically, and networks and systems become increasingly interconnected, collaboration between banks, governments, law enforcement and other sectors will only grow. Today, 72 per cent of Canadians primarily do their banking online or on their mobile device. That is up from 52 per cent just four years ago.

Canadian banks were active participants in the consultation to develop the National Cyber Security Strategy and are strongly supportive of an integrated public-private sector approach to cyber security and resiliency in Canada. Banks continuously work with government agencies, including the new Canadian Centre for Cyber Security, to share the latest knowledge and actively engage with other organizations such as the Canadian Cyber Threat Exchange. This goes a long way to fostering private and public sector collaboration and protecting Canadians and, ultimately, creating a more resilient, safer cyber environment for our society.

A key priority for the new Canadian Centre for Cyber Security will be to ensure cyber resiliency across key industry sectors in Canada. Encouraging a collaborative environment with the Centre providing a focus where the public and private sector can turn for expertise and guidance, will enhance Canada's cyber resiliency.

The CBA also believes that raising awareness about cyber security among Canadians is imperative. Educating Canadian citizens is a shared responsibility between the government and the private sector. General knowledge of the issues and an understanding of personal accountability to maintain a safe cyber environment are required to help ensure comprehensive cyber security extends to the individual user level. The banking industry looks forward to further collaboration with governments on common public awareness initiatives such as incorporating online cyber security safety into efforts to promote financial literacy.

In conclusion, I want to reiterate that the protection and privacy of Canadians' data is of the utmost importance to Canada's banks. Indeed, as technology continues to evolve rapidly and more Canadians bank in digital environments, we continue to explore technology solutions that enhance data privacy and security for our customers, for example through digital identification and authentication solutions. Canada's banking industry will continue to collaborate and invest

to protect Canadians' personal and financial information and banks will support the work of governments to protect Quebecers and all Canadians.

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