Strengthening Canada's Cybersecurity Framework

Pre-Budget Submission to the House of Commons Finance Committee

August 3, 2018

List of Recommendations to Address Cybersecurity Challenges

- **Recommendation 1**: Tailor cybersecurity solutions to small and medium-sized businesses.

- **Recommendation 2**: Harmonize cybersecurity regulations using a baseline framework.

- **Recommendation 3**: Prioritize the development of next generation remote identity proofing and verification systems.

- **Recommendation 4**: Develop standards to improve interoperability and cyber threat detection and prevention while removing friction from commerce.

- **Recommendation 5**: Address the shortage of employees with cybersecurity skills.

- **Recommendation 6**: Consider a task force of industry, Government and law enforcement to focus cybersecurity efforts.

Introduction

Cybersecurity is one of the greatest challenges governments and businesses are facing at the present time, with serious implications for national security, financial stability and consumer protection.

It is also a top global priority for Mastercard because safety and security are foundational principles central to every part of our business and the innovative technology platforms and services we enable. We know that secure products and services are essential to the trust our customers, cardholders, merchants and other partners place in us.

To address directly the theme of the 2018 pre-budget consultation, cybersecurity is critical to Canada's economic growth and future competitiveness. A perceived weak defence system could negatively impact Canada's reputation as a place to do business. However, an unduly cumbersome regulatory framework could similarly drive investment elsewhere while diverting resources from actual defences to compliance.

The Federal Government should be praised for its cybersecurity efforts to date, including passing legislation to establish the National Centre for Cyber Security and releasing the National Cyber Security Strategy. Both are initiatives that Mastercard supports and a number of the issues raised in this submission align with priorities identified in the strategy. Our key message, however, is that time is of the essence in implementing the strategy.

About Mastercard

Mastercard is a technology company in the global payments industry. We operate the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard products and solutions make everyday commerce activities – such as shopping, traveling, running a business and managing finances – easier, more secure and more efficient for everyone.

Mastercard does not issue payment cards of any type, nor does it contract with merchants to accept those cards. In the Mastercard payment system, those functions are performed by financial institutions. Mastercard refers to the financial institutions that issue payment cards bearing Mastercard brands as "issuers", and the financial institutions that enter into contracts with merchants to accept Mastercard-branded payment cards as "acquirers".

Mastercard owns the Mastercard family of brands and licenses financial institutions to use those brands in conducting payment transactions. Mastercard also provides the networks through which its customer financial institutions can interact to complete payment transactions and sets certain rules regarding those interactions to allow the system to function efficiently.

When a cardholder presents a Mastercard-branded payment card to a merchant to purchase goods or services, the merchant sends the authorization request to its acquirer, the acquirer generally routes the request to Mastercard, and Mastercard routes the request to the issuer. The issuer either approves or declines the authorization request and routes its decision back to the merchant through the same channels. Mastercard's role is to facilitate the payment instructions between the parties to the transaction as well as to set the rules which allow the parties to interact effectively and efficiently.

The above is useful context for understanding why Mastercard has made cybersecurity a top global priority.

Mastercard and Cybersecurity

For Mastercard to provide value to the issuers, merchants and consumers that use our network, we must provide safety and security. We cannot afford to have any interruptions in the operations of our network. When an issuer issues a Mastercard card, when a consumer takes it out of his or her wallet, or when a merchant decides to accept Mastercard, each of those stakeholders needs to do so with the confidence that the network over which those payments will be made is reliable and resilient.

On that, we have a solid record. The Mastercard network has layers of cyber defences designed to mitigate risk and protect it from being hacked, and we are continually building resiliency to prevent a service interruption.

Over the last three years, Mastercard has invested over $1 billion reinforcing the cyber defences of our network and developing solutions to protect participants in the payments ecosystem, be they issuers, acquirers, merchants or cardholders. This has involved taking the lead in developing new payment and commerce ecosystem standards, which are constantly being revised with an eye to security.

Mastercard is also investing in innovation: enhancing our capability in house; acquiring cutting edge technology companies; and, nurturing our Start Path group of curated start-ups, connecting them with our issuing partners to grow their business.

Best Practices for Cybersecurity Risk Management

There are five widely accepted elements essential for cybersecurity risk management. How Mastercard is operationalizing elements of these best practices is detailed below.

Identify. The priority is to authenticate the identity of network users, and Mastercard is doing really interesting things here, including Mastercard Identity Check – informally known as Selfie Pay – which Canadian issuers were among the first to commercialize.

Protect. Device security is critical on this point. With a networked system, any device can be an entry point for a cyberattack. To this end, in 2017 Mastercard acquired NuData Security, an innovative Canadian technology company that helps businesses prevent online and mobile fraud using behavioural and biometric indicators. NuData enhances our capabilities, including preventing consumer device cyberattacks, account takeover and enabling intelligent friction.

Detect. This is focused on stopping an attack before it begins, by using data analytics for increased security protection. Mastercard is making major investments in artificial intelligence, including the recent acquisition of Brighterion, a global artificial intelligence (AI) leader, which enhances the ability to detect sophisticated attacks. Brighteron's AI solutions help Mastercard to find the proverbial needle in a haystack when it comes to sifting through massive quantities of data.

Respond. In order to respond effectively to threats, information sharing and collaboration among government and law enforcement, industry partners and financial institutions, both in Canada and abroad, are critical.

Recover. Like other industry leaders, Mastercard is continually building and improving resiliency plans to ensure our back up plans work if they are needed. This includes real time machine-to-machine automated means of responding to an attack. In addition, leveraging solutions developed by Vocalink, we are able to track money mules and assist issuers in recovering funds.

Recommendations

The following recommendations should be considered as Canada further refines and implements its National Cyber Security Strategy.

First, in a networked, interconnected digital world, **cybersecurity solutions need to be tailored to small and medium-sized businesses** (SMEs). Cyber criminals will seek out the weak points in the system to launch an attack. Therefore, we need to provide a framework for small businesses to protect their operations. To that end, Mastercard is playing a leading role in defending SMEs through the Cyber Readiness Institute (CRI), which emphasizes the practical application of tools for SMEs.

For example, on July 1 the CRI launched the Cyber Readiness Program, a pilot project designed to collect the cybersecurity best practices from Fortune 500 companies and translate those into recommendations for businesses without the resources to hire their own security staff. As Mastercard CEO Ajay Banga stated about the launch, "Even if you're a big company you're only as strong as the weakest link you come into contact with because all our reputations are tied up in this together."

The CRI is also urging Fortune 500 companies to include the principles from this program throughout their supply chain. The CRI pilot wraps up on September 30, at which point it will assess strengths and opportunities for improvement before scaling it for a wider audience.

Second, **cybersecurity regulations need to be harmonized using a baseline framework**. Global companies like Mastercard frequently confront an expanding and overlapping set of cybersecurity regulations in different jurisdictions. That results in huge expenditures of time and resources on compliance – which is a very different concept than defence from a cyberattack. In other words, compliance shows adherence to a set of regulations at a specific time, whereas defence requires a constant focus and evolution.

Third, evidence from recent breaches suggests that adversaries have caught up to current standards used for remote identity proofing and verification. Identity proofing is used to establish the uniqueness and validity of an individual's identity to facilitate the provision of an entitlement or service. Previous solutions, like knowledge-based verification questions are no longer as useful, as breaches have allowed attackers to gather sufficient data to answer questions once thought to be secret.

The government should **prioritize the development of next generation remote identity proofing and verification systems.** Greater investment in R&D and standards work on identity, promoting innovation around identity, and government leadership in offering new digital services to validate attributes – shifting away from a paper based approach – would help governments and the private sector stay a step ahead of hackers and accelerate the emergence of better identity proofing solutions.

Fourth, with the Internet of Things, there will soon be 30 billion connected devices. This creates enormous opportunities for the digital economy, but it also increases cyber risk. Therefore, governments and the private sector should **develop standards to improve interoperability and cyber threat detection and prevention while removing friction from commerce**. Data analytics should be used for increased security protection.

Fifth, as the cyber threat grows, governments and the private sector **need to address the shortage of employees with cybersecurity skills**. The world needs to start training the next generation of cyber experts, and Canada's strategy rightly notes this. This is also an area where the CRI has put focus and it should be a critical consideration for Canada given a recent Deloitte report that found demand for workers in this area is growing by 7% annually and Canada will need 8,000 new cyber workers by 2022.

Finally, and more generally, collaboration, information sharing and bringing all stakeholders to the table are required to fight cyber crime, and we hope the new National Centre for Cyber Security will provide this forum. Within that structure, Canada **should consider a task force of industry, Government and law enforcement to focus cybersecurity efforts**. This is an issue so fundamental to the future of our economy and society that it needs attention and leadership at the highest levels, and Mastercard is ready to lend its expertise in any way possible. For example, in the U.S., President Obama commissioned an expert Task Force on Cybersecurity, on which Mastercard's CEO sat. It issued a series of recommendations, with the CRI a direct offshoot of its emphasis on securing SMEs.

Conclusion

Canada is doing solid work on cybersecurity, but we do not have the luxury of time when it comes to cyber threats. This issue is critical to Canada's future economic growth and competitiveness, both as a threat and an opportunity.

On the threat side, as is so often stated, those engaged in cyber defence need to get it right 100% of the time, whereas cyber criminals only need to be right once to cause potentially huge turmoil.

On the opportunity side, companies like Mastercard are investing billions in cybersecurity. If Canada can develop the skilled workforce required in this area, which would stimulate the creation of innovative cybersecurity firms like NuData, Canada can be a leader in this area, which opens up enormous economic opportunity.

We strongly encourage the Government to operationalize the national strategy quickly, and we hope our recommendations are helpful in that regard. In particular, we encourage consideration of the model that already exists with the Cyber Readiness Institute and the executive leadership shown by President Obama with his Task Force on Cybersecurity. We remain available to discuss our findings in greater detail at the Committee's convenience.