Fintechs Canada

Innovation, Science and Economic Development Canada (ISED)
235 Queen St
Ottawa, ON K1A 0H5

September 26, 2024

RE: Consultation on a right to repair policy for home appliances and consumer electronics.

On behalf of Fintechs Canada, I would like to thank you for the opportunity to comment on the government's consultation on a right to repair for home appliances and consumer electronics that was launched on June 28, 2024.

Fintechs Canada serves as the collective voice for the most innovative financial technology companies. Serving millions of Canadians, our membership consists of market-leading Canadian fintechs, fintech-friendly financial institutions, the technology companies that power the credit union space, and global fintech companies, among others. Our mission is to assist Canadians in accessing a more competitive and inclusive financial sector, while also protecting its integrity, stability and security.

While we commend the government for taking steps to strengthen competition in Canada's repair sector, we urge the government to ensure that the implementation of any right to repair framework does not compromise the integrity of Canada's payment system. In particular, a broad scope of application of any right to repair framework may include payment devices and other payment technologies, such as electronic credential hardware. This could compromise the safety, security, and performance of these devices, which are designed to protect Canadians from malicious actors while enabling seamless commerce transactions.

In this letter, we explain why payment devices and related payment technologies must be exempt from the right to repair framework and provide recommendations on how this can be achieved.

Compromising security of payment devices

A broadly defined right to repair framework risks the over-inclusion of certain technology, including technology for facilitating payments, that require highly specialized devices and standards with complex repair or replacement requirements. This could undermine the security and integrity of such devices, making them more vulnerable to bad actors and risks undermining the confidence of Canadians in digital payments that are crucial to everyday life.

Payment devices are specifically designed to meet the highest data security standards. This ensures that Canadians can trust that their personal information and sensitive card details are kept safe and secure during their purchasing process. These devices include traditional 'point of sale' terminals, credit card machines and related technologies, such as electronic credential hardware that protects cryptographical keys and enables users to easily hold and upon choice, transmit personal digital payment credential data to enable the receiving or transferring of funds or assets. Some of these technologies, such as traditional 'point of sale' terminals, are widely adopted. Others are in the early stage of adoption, but they are expected to represent a significant part of the payment ecosystem in the future, and therefore should be considered as part of the policymaking process that will shape the consumer electronic landscape for years to come.

The data security and integrity standards associated with payment devices are designed to instil confidence that Canadians rely upon in their digital payment options, which represent almost 86% of all transactions in Canada.

These devices are meticulously designed to detect and respond to attempts to access internal elements,to prevent the removal of sensitive data, or the inclusion of additional tampering elements. Many of these devices have tamper-detection circuitry, which is designed to prevent them from being taken apart and manipulated by bad actors before they're used at the point of sale. This includes the use of tamper-evident seals on machines, which signal when a machine has been taken apart, as well as outfitting machines with tamper switches, which renders the machines inoperable when they're taken apart.

Tamper-proof devices are designed, in part, to counter "skimming," which is when scammers embed a piece of technology in a payment card-reading device to collect the sensitive financial information stored in a payment card's magnetic strip or microchip. There is no publicly available data on skimming in Canada, but it's clear that neither big banks nor large retailers are immune to it. Where there is data, it's clear that skimming is becoming a growing issue. For example, in the first half of 2023, the United States experienced a 20 percent

increase in skimming incidents compared to the same period in 2022. The United States also saw a 77 percent increase in the number of compromised payment cards compared to the same period in 2022.

If a right to repair framework were to encompass payment devices and related technologies, it could compromise the meticulous approach to security, safety, and integrity of these devices. This is crucial for protecting Canadians from financial crimes like fraud and for maintaining confidence in the payment system.

Conflicting with global standards, disrupting payments

Everyone suffers when there are weak links in any payment chain. That's why stakeholders within the industry joined forces long ago to create standards that protect people from various risks, including skimming. For example, the PCI Security Standards Council and EMVCo are organizations that were founded by large payment networks to make payments more secure and seamless. Compliance with these standards is critical to safeguard sensitive financial information and is required for any manufacturer and distributor of POS devices.

Under existing Payment Card Industry Data Security Standards ("PCI DSS"), devices must undergo stringent penetration testing as per the PCI PIN Transaction Security (PTS) and Point of Interaction (POI) Modular Security Requirements. Penetration testing ensures that bad actors can not tamper with the device in ways that could compromise payment data. As part of this testing, devices must have robust tamper-detection circuitry, and undergo regular audits to verify their integrity. If a payment device fails the checks, it is deemed unsafe and unusable. This can also trigger an investigation to assess whether there are any data breaches, which can result in fines for companies.

Non-compliance with PCI DSS requirements can prevent payment devices from entering the market and may result in serious penalties, loss of trust, and financial repercussions for merchants and consumers alike. If a right to repair framework were to be so broad that it applies to payment devices, it could make it difficult for these devices to continue to align with existing standards. Requiring repairability in PCI DSS-compliant devices could make it challenging to ensure tamper-proof and other anti-penetration features remain uncompromised.

Undermining performance of payment devices

Getting the right to repair framework right is crucial to guaranteeing the performance of payment devices, which businesses rely on to serve customers, take payments, and grow their operations everyday.

Payment devices are designed to be used in everyday business settings, and are often combined into single devices to provide a range of business operations. For example, a restaurant may use a payment device to not only take payment from a customer, but also to manage the full customer experience, from order management through to order operations. As such, these devices are designed to produce high performance and seamless continuity of service in many different settings - from wet environments like bars, restaurants, and outside venues, to high intensity environments such as shops, markets, and service businesses. These features are essential to ensuring businesses and customers are able to buy and sell goods and services in the easiest way possible.

To achieve such performance, payment devices often contain lithium-ion batteries, commonly used in such payment devices due to their high-performance standard and longer life than other battery forms. However, they have some inherent safety risks such as overheating, sparking, and fire when mishandled or punctured. Furthermore, to ensure robust performance in a range of business settings, payment devices are designed to be non-porous and are well-sealed, which whilst reducing replaceability, reduces overall product turnover and enhances consistent performance.

An inappropriately designed right to repair framework may inadvertently lead to hazardous conditions for batteries, such as mishandling scenarios where a battery is exposed to high temperatures or physical damage. In turn, it may also result in re-designed devices that are more susceptible to wet environments, or less able to manage the everyday bumps and hits of a business environment. This could see increased costs for merchants as they have to turn over more devices, potentially risking the safety of individuals attempting to repair devices themselves, and have a material impact on electronic waste.

Our recommendation

While we support giving consumers greater choice over the repair options for the products they buy, it is necessary that the scope of any right to repair framework does not encompass payment devices or related facilitators.

Most payment devices can't be captured by a right to repair framework because most payment devices are owned by financial institutions or payment companies, who provide the devices to merchants as part of a contractual agreement for payment services.

However, some payment devices aren't owned by financial institutions or payment companies because they're purchased by Canadians acting in a

commercial capacity, such as corporations and sole proprietors. When this is the case, the payment devices still need to be designed to be tamper proof, and show no signs of being tampered with, lest the devices be in violation of the required global standards and rendered inoperable.

Other related payment devices, such as electronic credential hardware devices are designed principally for consumers. However,their unique nature - in protecting and transmitting sensitive personal data or credentials such as cryptographic keys - means they are not a standard consumer device, and should not be treated as such.

For this reason, the federal government should make sure that the right to repair framework does not capture payment devices or related facilitators. The government could do this through the following options.

Option 1: Explicitly exclude payment devices from the legislation.

The government can include language in Canada's right to repair framework that specifically excludes certain products from its scope. We recommend that this includes specific payment devices, as well as associated payment technologies like specialised electronic credential hardware. An exclusion approach has been adopted in states such as New York and California, noting that some technologies have specialised functions that could be undermined otherwise.

Option 2: Exempt items that could be impaired by right to repair requirements.

The government could also include language in the legislation that exempts a broader category of items, such as payment devices, from right to repair regulations if the repair process would require disabling security or privacy features, or otherwise impair the functionality of the item. This approach has already been implemented in right to repair legislation, including in California, to reflect the need to protect the safety and security integrity of devices.

Option 3: Exempt items that are not currently offered for repair.

Finally, the government should consider whether current devices should be eligible for repair. Many companies offer warranty-based replacements rather than repair services. For payment devices, this reflects the complexity associated with repair and the need to guarantee the integrity of such devices to secure personal and sensitive data and protect against bad actors.

Right to repair is designed to bring transparency to the wider repair ecosystem, and protect against monopolisation of existing resources. Where a product is not currently offered for repair, any policy should not in turn require a repair function to be set up, which would create significant and unpredictable upheaval for a range of products, including payment devices.

***

Fintechs Canada thanks you for considering our perspective on right to repair for home appliances and consumer electronics. We look forward to working with you and continue to support the government's efforts.

Sincerely,

Alex Vronces
Executive Director, Fintechs Canada
1 Richmond Street West, Suite 300
Toronto, Ontario M5H 3W4