

March 28, 2024

MP Joël Lightbound,  
Chair, Standing Committee on Industry and Technology  
Sixth Floor, 131 Queen Street  
House of Commons  
Ottawa, Ontario  
K1A 0A6

*Transmitted as via email to [joel.lightbound@parl.gc.ca](mailto:joel.lightbound@parl.gc.ca), and [INDU@parl.gc.ca](mailto:INDU@parl.gc.ca)*

**Retail Council of Canada requests amendments to C-27 to protect retail workers and our communities.**

Dear Committee Chair Lightbound,

Over the past two years, retailers in Canada have seen a sharp increase in retail crime and violence in our stores. Historically, the perception of retail crime conjured images of shoplifting – discreetly taking a product from a store without paying. This is no longer the case.

Retail crime is violent, it is organized, and it is dangerous. Across Canada, perpetrators of retail crime are increasingly using weapons to threaten employees and customers, destroying property, and are increasingly agents of highly coordinated organized crime.

The rapidly changing nature of retail crime is outpacing the ability of Canadian retailers' staff, police, and our justice system, to respond to this more violent face of retail crime. This changing face of retail crime is making our workplaces unsafe for staff and customers. Statistics on workplace injury are challenging to aggregate; however, some of our members have shared with us that, for them:

- Aggravated assault against their employees and/or customers is up over 61% year-over-year, and up over 1,300% when compared to two years ago.
- Documented workplace violence involving weapons (including guns) are up 82% year-over-year.
- The instances of in-store battery are similarly shocking – up over 47% year-over-year, and up over 2,200% when compared to two years ago.

Further, members have shared with RCC some direct anecdotes on employee safety:

- One member shared that 130 guards were injured last year. Another retail member has shared how they currently have 18 staff members on long-term disability as a direct result of retail crime.
- As a more statistical representation, a member shared how nearly 25% of their worker compensation claims last year were directly linked to retail crime.

With justice and police resources stretched thin across the country, retailers have found that retail crimes are treated as one off, isolated incidents and therefore deprioritized. While some retail crimes may indeed be of minor public concern, e.g. the proverbial teenager stealing low value

apparel, there are serious retail crimes occurring that pose a genuine danger to staff and to customers.

We believe Bill C-27 should modernize privacy and data protections and allow for effective innovation and business operations, with harmonization and interoperability being top priorities across Canada and internationally. We strongly support the importance of consumer consent and positive consumer experiences. We also believe that physical safety in stores is crucial for shoppers and employees. Without a more reasonable, risk-based approach to data-sharing with police and other retailers, we fear that the trend of violent and other serious retail crime will only increase. We need the Canadian government to support retailers in protecting those who work and shop in retail stores from more serious, violent and organized crimes.

As Canada considers Bill C-27, we would therefore like the committee to consider amendments Bill C-27's CPPA to responsibly allow for the prevention, detection, or suppression of violent crimes, repeat theft and organized criminal activity. We would like the opportunity to present to your committee, or to discuss the proposed amendments below with the members of the committee to share how they support retailers in protecting our staff and customers against workplace violence.

Sincerely,



Matt Poirier  
Vice-President, Federal Government Relations  
Retail Council of Canada

### ---Proposed Amendments to Bill C-27---

Suggested amendments to C-27's proposed new privacy law, the *Consumer Privacy Protection Act (CPPA)*, with exact text beneath:

1. Amend Section 27(1) of the CPPA to expand the ability for an organization to disclose PI to another organization for the purposes of detection, prevention or suppression of violent or organized crime or repeat theft as well as fraud.
2. Amend 40(3) to allow disclosure to other organizations for detection, prevention or suppression as well as investigation of a contravention of a law.
3. Amend Sections 44 and 45 to allow organizations to proactively share data with law enforcement where circumstances give rise to a reasonable expectation of fraud, violent or organized crime or repeat theft.

We note that any disclosure under these amendments would still need to demonstrate due diligence that it:

- is for an appropriate purpose;

- is reasonable and proportionate for the intended purpose;
- if made on notice to or with the consent of the affected individual, would compromise the ability to detect, suppress or prevent the crime;
- is sufficiently detailed so as to identify the suspect(s) with appropriate accuracy, taking into account the purpose of the disclosure and potential impact on the individual; and
- is bound by the principles of limited disclosure as to both quantity of information and recipients on a need-to-know basis; and
- is made with appropriate safeguards, including some or all of the following where appropriate: secured channels of communication; password authentication; limited retention periods, followed by auto-deletion; written policies/SOPs for teams involved in information-sharing with mandatory annual training and periodic internal compliance audits; documented logging of disclosures; and transparent disclosure of practices in privacy notices.

**Proposed Consumer Privacy Protection Act (CPPA) amendment text:**

**Prevention, detection or suppression of ~~fraud and~~ serious crime**

**27(1)** An organization may disclose an individual’s personal information to another organization without the individual’s knowledge or consent if the disclosure is reasonable for the purposes of detecting or suppressing fraud, **violent or organized crime or repeat theft**, or of preventing fraud, **violent or organized crime or repeat theft if there is a reasonable expectation that these ~~have been~~ or might be ~~is likely to be~~ committed** and it is reasonable to expect that the disclosure with the individual’s knowledge or consent would compromise the ability to prevent, detect or suppress **these crimes**.

**Breach of agreement or contravention**

**Disclosure**

**40(3)** An organization may disclose an individual’s personal information without their knowledge or consent if the disclosure is made to another organization and is reasonable for the purposes of **detecting, suppressing, preventing or** investigating a breach of an agreement or a contravention of federal or provincial law that has been, is being or is **reasonably expected to be ~~about to be~~ committed** and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation

**Law enforcement — request of government institution**

**44** An organization may disclose an individual’s personal information without their knowledge or consent to a government institution or part of a government institution,

- (a)** That has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing federal or provincial law or law of a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

(b) For the purposes of detecting, suppressing or preventing fraud or relating to a contravention of a federal or provincial law or law of a foreign jurisdiction that has been, is being or is reasonably expected to be committed.

#### **Contravention of law — initiative of organization**

**45** An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution or a part of a government institution if the organization has reasonable grounds to believe that the information relates to a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is reasonably expected to be ~~about to be~~ committed.