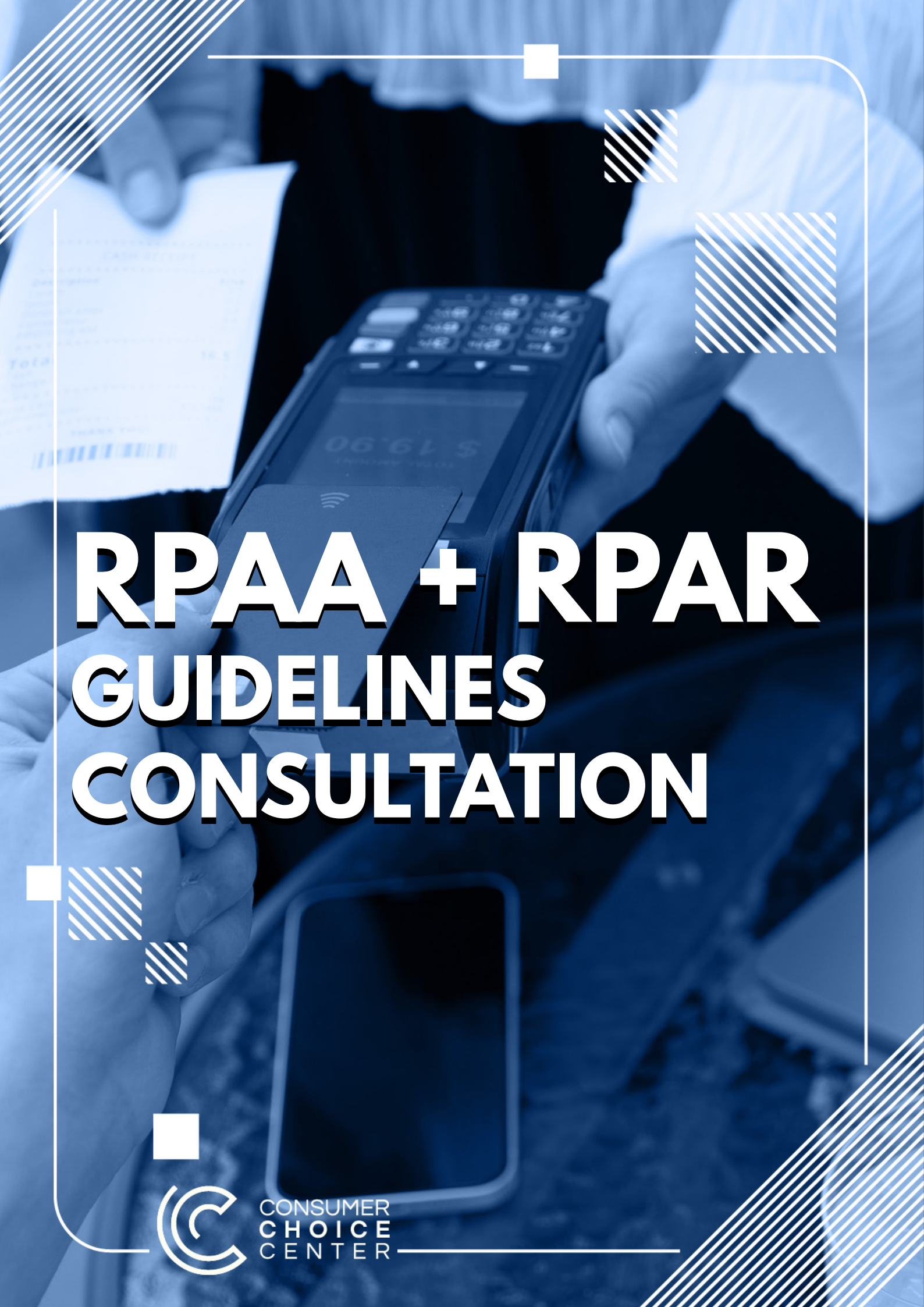

RPAA + RPAR GUIDELINES CONSULTATION

CONSUMER CHOICE CENTER

The Consumer Choice Center is an independent, nonpartisan consumer advocacy group that champions the benefits of freedom of choice, innovation, and abundance in everyday life.

As an organization, we are extremely concerned by the current draft version of the Retail Payment Activities Act (RPAA) and the Retail Payment Activities Regulations (RPAR) guidelines. In particular, the 'Operational risk and incident response' and 'Safeguarding end-user funds' documents often lack conceptual clarity and raise implementation challenges for payment service providers (PSPs).

Comments on the 'Operational Risk and Incident Response' guideline

Proportionality is directly defined in Annex A on page 47 of the text as "The balance of risk management rigor with the impact that a reduction, deterioration or breakdown of the PSP's retail payment activities could have on end users and other PSPs".

Nevertheless, this invocation of proportionality is limited to the number and value of end-user funds held, the number and value of electronic fund transfers concerning a retail payment activity, and the number and value of end-users (see page 48). The same cannot be said of the scope of the risk management and incident response framework, whose requirements are prescriptive for all payment service providers. Though technically "not limited to the PSP's ubiquity and interconnectedness", limits in resources or personnel merely influence the scale rather than the scope of the measures to be taken (see paragraphs 4.4 on objectives, 5.4 on identifying operational risks, and 8.6-8.7 for incident response plans as examples).

Thus, the Consumer Choice Center would like to echo the general concerns voiced in the comments on the first edition of the Canadian Gazette regarding the negative impact of these requirements on small businesses and startups in the fintech sector. According to the Bank of Canada's own comments, around 2,500 companies (a varied group including "payment processors, digital wallets, currency transfer services, and other payment technology companies"), many of them small or medium-sized, would fall under the guidelines. That being the case, the regulations raise undue operational burdens (in the form of high compliance and monitoring costs) which the guidelines do not justify,

especially given the lower level of risks posed by the transactions of smaller firms.

Despite this objection, as the retail payments supervision FAQs confirm, there is no streamlining option for SMEs, which are presently required to introduce the same list of reliability targets and indicators, identification of operational risks, protection of assets, detection and monitoring capabilities, incidence response plans, internal reviews, and testing. Such PSPs must also submit annual reports, significant change reports, incident reports, information requests, and notices of change in information.

The rigid application of the RPAA and RPAR stifles the Canadian fintech sector's dynamism, security, and competitiveness. On the one hand, the demands constitute a high barrier to entry into the market that many current and future firms will not be able to meet, creating an advantage for large incumbents (many of whom are not subject to the RPAA or the RPAR as account providers under paragraph 13 or guarantors under paragraph 14 of the RPAR) over newer startups. On the other hand, many firms will need to reallocate resources and personnel from research and development or fraud prevention to meet guideline conditions, compromising the industry's flexibility and safety. Ultimately, these hidden costs will be passed down to consumers as end users, who will be left with fewer, more expensive, and more vulnerable options.

Another worry revolves around liability rules, which are currently ill-defined and excessively broad. For instance, paragraph 12.2 of the guideline states liability "applies regardless of the geographic location of the third-party service provider or the geographic location of the technologies that the third-party service provider uses to provide services to the PSP. " At the same time, paragraph 12.7 claims, "A PSP must meet regulatory requirements, including when relying on third parties providing services related to its retail payment activities. Under section 87 of the RPAA, a PSP is liable for a violation committed by any of its third-party service providers acting in the course of its contract". Materiality condition aside (paragraphs 12.10-12.12), PSPs cannot realistically be expected to know and monitor the relevant activity of outside parties, let alone ones that the Bank of Canada and external authorities are expected yet find difficult to document (paragraph 12.36.3)!

Even more so, though the Bank intends to harmonize the RPAA, RPAR, and its guidelines with those of the United Kingdom and the European Union, its proposals go well beyond the two existing jurisdictions. While the guideline recommends that all registered PSPs

provide information on their ubiquity and interconnectedness, reporting in the EU's Payment Service Directive 2 and the UK demands only information on fraud prevention and security risks (see article 19, paragraph 1 of the PSD2 and the Financial Services and Markets Act 2023, article 72). It is not hard to see how such sweeping decisions add extra bureaucratic hurdles that would disincentivize international firms from entering the Canadian market and cooperating with Canadian counterparts.

Proposals for improving the 'Operational Risk and Incident Response' guideline

The Consumer Choice Center proposes the following revisions to the document:

- Shift to a principles-based procedure in which regulators trust PSPs to define what matters regarding proportionality

- Simplify the requirements for SMEs through a gradual approach to operational risk and incidence response based on the existing criteria of interconnectedness and ubiquity complemented by a clearly specified cutoff point (as a de minimis threshold to exclude minor payments from the full criteria).

- To clarify liability and remove the possibility of moral hazard from principal-agent problems, refer only to the technologies and services with an actual presence in Canada along the payment chain (paragraph 12.2) and assign primary liability to the regulators themselves.

- Harmonize the RPAA rules with international regulations by recognizing the latter in practice as a sufficient condition for third parties (relaxing the demand for strictly equivalent criteria in the guideline).

Comments on the 'Safeguarding end-users' guideline

Section 2, entitled "Means of safeguarding end-user funds," presents PSPs with two options: either hold end-user funds in a trust account wholly dedicated to them or create a dedicated account with insurance/guarantee in place that is equal to or greater than the initial sum. The presentation of two options and combinations thereof embedded in

subsection 20 (1) of the RPAA and 2.1 of the guideline is an improvement over previous versions, which mandated a single solution.

Nonetheless, the condition of mandatory safeguarding fails to acknowledge the variety of services in the fintech sector. Holding money in trust or collateral may be unnecessary - the nature of the PSP is such that it only holds funds for a short time. Alternatively, it may prove unfeasible because it creates an undue fiscal burden on many smaller businesses for whom holding collateral below 1:1 may prove sufficient. Opening a bank account could prove difficult since it involves a PSP's direct and indirect competitors, once again advantaging the status quo at the expense of innovation.

Paragraph 1.5 of the regulations acknowledges the dilemma and raises the possibility that "There could be instances when a PSP only holds funds for a short period before they are withdrawn or transferred by the end user (e.g., intraday)". Yet it insists on safeguarding regardless, only modifying the required timeline - "The Bank, therefore, expects a PSP to segregate all end-user funds it holds as soon as practical on receipt and no later than the end of the business day following the receipt. However, funds must be recorded by the PSP as end-user funds held on its ledger and treated as part of its framework."

Additionally, there is lingering uncertainty about what qualifies as a suitable account provider, especially when that account provider is a foreign financial institution. Paragraph 2.13 refers to a possible account provider as "a foreign financial institution that is regulated by a regulatory regime that imposes standards in respect of capital, liquidity, governance, supervision, and risk management that are comparable to those that apply to those entities". It is not clear what "comparative" mean in this paragraph. This ambiguity is concerning, given paragraph 2.16 makes it incumbent on PSPs to determine whether the foreign financial institutions it wants to engage with are adequate or not: "The Bank expects a PSP to analyze, using publicly available information, whether the regulatory regime the foreign financial institution is subject to imposes prudential standards that are comparable to those that apply to entities regulated in Canada." The brief mention of the Basel Committee on Banking Supervision in the same paragraph is unsatisfactory (are the Basel rules merely necessary but insufficient?).

Proposals for improving the 'Safeguarding end-users' guideline

The Consumer Choice Center proposes the following revisions to the document:

- Similar to the previous section, introduce a tiered safeguarding evaluation requiring lower collateral below 1:1 or no collateral at all, subject to the firm's ubiquity and interconnectedness.

- Extend the exemption from paragraph 1.6 (which absolves instantaneous receipt and transfer of end-user funds from safeguarding) to other PSPs on a class basis (e.g., intraday PSPs).

- Clarify the meaning of "comparative" in paragraph 2.13 by giving more concrete examples of compatible foreign financial institutions.