funded by:
Women and Gender Equality Canada | Femmes et Égalité des genres Canada
Government of Canada | Gouvernement du Canada
Canada

CANADIAN CENTER FOR WOMEN'S EMPOWERMENT | CENTRE CANADIEN POUR L'AUTONOMISATION DES FEMMES

Written Submission for the Consultation on the Consumer-Driven Banking Regulations

By: Canadian Center for Women's Empowerment (CCFWE)

[Reviewed and endorsed by the Canadian Network on the Prevention of Elder Abuse (CNPEA)]

August 24, 2026

To: Department of Finance Canada
90 Elgin Street
Ottawa ON
K1A 0G5

From:
Canadian Center for Women's Empowerment (CCFWE)
Ottawa, ON
K2J 5C6
https://ccfwe.org/

ABOUT CCFWE

The Canadian Center for Women's Empowerment (CCFWE) is the only non-profit organization in Canada solely dedicated to addressing economic abuse and economic injustice in the context of gender-based violence (GBV).

Through research, education, policy change, and financial empowerment, CCFWE works to prevent economic harm, strengthen survivor safety, and advance systemic solutions that support women's economic security and independence.

Learn more: https://ccfwe.org/

WHAT IS ECONOMIC ABUSE?

Economic Abuse is a range of behaviours that allow someone to control someone else's economic resources or freedoms. It refers to various tactics that limit an individual's financial autonomy, including but not limited to: denying them access to their money, exerting control over their resources, or leveraging intimidation and threats to constrain their economic freedom.

Technology-Faciliated Economic Abuse: Technology-facilitated economic abuse is a form of abuse where digital tools are used to control or sabotage a person's finances. Abusers may monitor or restrict financial activity, steal information, or manipulate online accounts to prevent financial independence. Examples include: unauthorized access to banking apps, altering passwords, using e-transfers to threaten, or destroying devices needed for work and financial management.

There are generally three different forms of economic abuse:

- **Economic Control:** This occurs when someone limits or completely controls a survivor's access to financial resources and decision-making. This includes monitoring or restricting all of the survivor's financial activity, denying the survivor access to bank accounts, credit cards, or cash, forcing the survivor to ask for money or live on a strict "allowance" or limiting the survivor's access to basic needs such as food, housing, transportation, or healthcare

- **Economic Exploitation**: This occurs when someone actively damages the survivor's financial standing or credit. This can include asset deprivation such as withholding or stealing income, savings, or jointly owned property, coerced debt (forcing the survivor into debt, often without their knowledge or consent), or identity fraud and theft (using the survivor's identity to commit financial fraud or open credit accounts)

- **Employment and Education Sabotage:** this occurs when someone controls or inhibits the survivor's ability to gain or maintain employment and education. This form of abuse can be exacerbated when the survivor works with the abuser (e.g., co-owning a business).

Prevalence of economic abuse:

- **93%** of their abusers didn't allow them to have their own money and have taken away paychecks and/or financial aid.
- **90%** of victim-survivors had decision-making power taken away from them while their abuser made all financial decisions.
- **90%** of their abusers demanded participating victim-survivors information on how money was spent and asked for receipts.
- **90%** of victim-survivors couldn't access bank accounts or access to financial information.
- **90%** of abusers threatened with physical harm if victim-survivors paid rent or other bills that were needed.
- **84%** of abusers had debt built up under the victim-survivors name.
- **78%** of Economic Abuse survivors have faced physical abuse at some time with their partner.

ON THE ISSUE

The Canadian Center for Women's Empowerment (CCFWE) generally supports the objectives of secure, consumer-driven banking. We support a framework that centres transparency over consumer data and financial services, and that focuses on customer consent. However, this must include strict guidelines and requirements for any third-party providers offering services. Safeguards are essential to avoid the harms and risks that come with easier access and greater interconnectedness of services.

As already noted during the consultation session on Friday, August 21, 2026, CCFWE urges the Department to avoid focusing solely on risks posed by outside hackers, and to ensure that risks by partners and family members causing harm are also considered and addressed.

Consistent with similar studies in the United States, the United Kingdom, and Australia CCFWE's own research shows that approximately 96% of domestic abuse survivors report experiencing economic abuse. The same research found that 90% of participating survivors reported not having access to bank accounts or financial information, and that decision-making power had been taken away from them while their partner made all financial decisions.

According to currently available data, approximately 44% of Canadian women report experiencing some form of domestic violence. Applying the above prevalence rate, this suggests that roughly 40% of all women in Canada have experienced economic abuse, and by extension some form of financial control and coercion.

Given the increased interconnectedness of the framework, and the number of parties that will rely on one another for authentication and consent checks, the federal government must work closely with organizations such as CCFWE, and others working on economic abuse, gender-based violence, and elder abuse, to understand the risks posed by trusted persons causing harm, and to build preventative measures into the regulation that mitigate the risk of consumers experiencing increased fraud and financial coercive control, compounded by new technology and AI.

Below are more specific positive and negative impacts that CCFWE foresees for people with lived experience of economic abuse.

Potential positive impacts for people with experiences of economic abuse

- **Transparency**: Personal data on transactions, open credit cards, and accounts, available through a consumer dashboard, can give victim-survivors greater visibility into potential economic abuse by a partner causing harm.

- **Documentation**: If designed with the potential for misuse and economic abuse in mind, data on transactions initiated by a partner causing harm, such as the opening or modification of joint financial products, would be easier to detect, providing documentation and proof of coerced debt or economic abuse. This includes irregularities and unusual spending patterns that may signal economic abuse or fraud.

- **Easier to change banks**: Partners causing harm often compromise victim-survivors' bank accounts or other financial products. By making it easier for consumers to switch banks, consumer-driven banking could benefit victim-survivors by streamlining the process of opening personal accounts at financial institutions that have not been compromised.

- **Easier access to loans**: Entrepreneurs with experiences of economic abuse face structural and compounding barriers within Canada's financial and entrepreneurial systems. Coerced debt, damaged credit, interrupted work histories, and safety risks are not well recognized or accommodated by conventional lending and business-support systems, and traditional lending criteria exclude many survivors who are still rebuilding financial autonomy after violence. Consumer-driven banking could enable lenders to look beyond credit scores and coerced debt to assess actual repayment capacity based on broader spending patterns and repayment habits thereby increasing survivor entrepreneurs' access to capital and funding.

Potential negative impacts for people with experiences of economic abuse:

While there are potential opportunities for people with experience of economic abuse to benefit from consumer-driven banking, CCFWE is also aware of and concerned about risks that this could entail. Similar to CCFWE's concerns and recommendations for the federal Code of Conduct on the Prevention of Economic Abuse, the federal government must ensure that the Consumer-Driven Banking Act ("the Act") foresees potential dangers and risks related to economic abuse to mitigate the misuse of financial services by partners causing harm.

- **Increase in coercive control and technology-facilitated economic abuse:** Economic abuse as a form of coercive control often includes financial surveillance and control, where victim-survivors are required to justify what they spent and how, often under threat or force. While a consolidated overview of personal data and transactions can be a significant benefit for some consumers, for people with experiences of economic abuse this same feature could increase coercive control by making it easier and more effective for a partner or family member causing harm to monitor and surveil their financial activity.

  With Bill C-16, the Protecting Victims Act, the federal government has explicitly criminalized coercive control in intimate partner relationships, including financial control.

Yet the proposed Regulations would make it dramatically easier for a partner causing harm to exert this same financial control and surveillance by giving them a single, complete view of a victim-survivor's financial data and transactions.

Coercive control and economic abuse also do not end after separation. CCFWE has heard from numerous survivors that banks have shared updated information, such as addresses or phone numbers, with an ex-partner causing harm after separation as the ex-partner still appeared as a joint account holder on a financial product. With no additional safeguards in place for joint financial products under consumer-driven banking, this same pattern could become even easier to replicate, giving ex-partners easier access to updated information about victim-survivors and putting both their financial and physical safety at risk (see also *Joint accounts and authorized users*).

- **Authentication and KYC:** Because the framework relies heavily on APIs and low-barrier identity verification, a partner or family member causing harm may be able to open financial products in a victim-survivor's name without ever triggering a fraud flag. The proposed Regulations describe consumer profile data as including information provided at account opening, identification, and verification such as name, address, date of birth, and employment information, all details a family member or romantic partner would typically already know. This risk is heightened when the victim-survivor lacks access to their own account information or dashboard and therefore has no way to notice the new product being opened. As multiple participating players and third-party providers are involved in the framework, there is also a risk that each assumes another party has already completed KYC or fraud checks, creating a false sense of security. A complex, interconnected system also creates more points where the weakest link could be exploited to access data and cause harm.

- **Expressed consent doesn't mean free consent:** Passing KYC or multi-factor authentication should not be treated as evidence that a consumer acted freely. A person may successfully complete these checks while acting under coercion, or while an abusive partner controls their device, email, or credentials. The reverse is also a risk: a person causing harm may intentionally block a victim-survivor from accessing their own accounts. Victim-survivors may not have safe, private access to a phone, computer, or email, and some depend on another person for technology altogether, making it harder for them to control their financial data or seek help safely.

- **Selective disclosure:** Transparency depends on who controls the setup process. If a person causing harm has access to initial credentials, is present during setup, or is the one who initiates the connection (a common pattern in economic abuse, where one partner "manages" the household's financial technology) that partner can determine what appears in the shared view. With granular consent, they could authenticate, see the full list of accounts at an institution, and deliberately deselect the one carrying coerced or fraudulent debt before sharing the rest, leaving the victim-survivor with a dashboard that gives a false sense of a comprehensive overview.

- **Unsafe notifications and safe communication preferences:** The proposed Regulations do not appear to require participating entities to let consumers choose a communication method they know to be safe, such as mail, phone, or email, for notices related to their account. The framework requires various notices to be sent to consumers, including changes to consent, account access, and security matters. An email, text message, app notification, or letter sent through a default or shared channel could alert a partner causing harm that a survivor has opened a new account, changed their access, or is taking steps to protect themselves, particularly where digital access is monitored or controlled. Consumers should be able to select a safe communication channel, and this preference should be treated as a distinct right, separate from general consent to data sharing.

- **Joint accounts and authorized users:** The proposed Regulations don't clearly address how consent, access, and data sharing operate where an account has more than one holder. It is unclear whose consent is required to share data from a joint account, what information one account holder can view or share unilaterally, how disagreements between joint holders are resolved, and how a survivor can safely separate their access from a joint product without alerting or requiring the agreement of the other holder. Given how often financial abuse involves joint accounts and authorized-user arrangements, this gap should be addressed together with financial institutions in relation to the Code of Conduct on the Prevention of Economic Abuse on how to prevent and mitigate economic abuse.

- **Barriers to digital access:** The benefits of consumer-driven banking assume a baseline of digital access that not all consumers have. Not everyone has a private device, reliable internet, government identification, digital literacy, accessible technology, or safe access to email and telephone services. People with experiences of economic abuse who have been isolated from technology or financial resources by a partner causing harm may be the least able to access or benefit from the framework, even as it is promoted as a tool for financial empowerment. The Regulations should consider how consumers without reliable digital access will be supported and protected.

- **Poor consumer awareness:** General awareness of open banking among Canadians remains low, with only 9% of surveyed consumers reporting they had heard of open banking (FCAC). This low level of awareness and understanding of how open banking applications work, particularly around linking accounts and sharing data, can increase consumer vulnerability to malicious actors. For survivors of economic abuse, this general awareness gap compounds for those experiencing economic abuse as they often don't fully understand what data is being shared, with whom, or how to review or revoke that access. They might be less able to recognize when the framework is being used against them, and less able to protect themselves within it. Consumer education efforts accompanying the rollout of this framework should specifically address these risks, rather than assuming general financial literacy is sufficient.

GBA+ Assessment

Given the potential negative implications outlined above for people with experiences of economic abuse and fraud, CCFWE is concerned that the GBA+ assessment did not identify any requirement for specific measures to address or mitigate GBA+ impacts.

As highlighted throughout this submission, a framework that consolidates sensitive financial information can have very different effects on women, people with disabilities, newcomers, older adults, low-income consumers, Indigenous people, racialized communities, rural and remote communities, and people experiencing economic abuse and gender-based violence.

Given that approximately 40% of Canadian women have experienced economic abuse, we encourage the government to revisit the GBA+ assessment with these impacts in mind, and to develop targeted mitigation measures in consultation with organizations with direct expertise in this area, such as CCFWE, before the Regulations are finalized.

RECOMMENDATIONS

- Include people with lived experience of economic harm, violence, and fraud into consultations to hear from them directly. This includes testing and piloting various features and processes with survivors and other vulnerable populations with intersectional backgrounds.
- Design the Act and TPP requirements with potential economic abuse and weaponizing of financial products by partners or family members causing harm in mind.
- Roll out awareness and information campaigns on consumer-driven banking particularly around consent and potential dangers of open banking for various audiences with intersectional backgrounds including information that is culturally sensitive and trauma-and violence-informed.
- Collaborate with CCFWE as well as other VAW organizations and social service providers to understand impacts of coercive control, economic abuse and gender-based violence to prevent and mitigate risks of increased financial control, surveillance and technology-facilitated economic abuse.
- Allow consumers to choose how and when they are contacted, including through a safe email address, telephone number, mail, or digital channel. Enable mandatory notifications for key account changes, such as new accounts, added or removed access, or changes to authentication or consent, that cannot be disabled. Allow consumers to route these to a private channel separate from shared contact information, so survivors are alerted to changes made by a person causing harm, without their own protective

changes being visible to that person. Ensure channel updates do not notify the old channel, and that notification previews are discreet by default.

- Ensure that this Act is monitored and course corrections can be made with changes in technology or approach, if it is found that open access is causing potential harm.
- Establish clear complaint procedures that specify where consumers should go amidst various players involved. Vulnerable consumers and survivors should not be passed between banks, fintechs, data providers, and third-party service providers.
- Train staff at complaint lines and helplines to recognize coercive control and avoid victim-blaming. When a person causing harm gains access to a survivor's passwords, devices, authentication codes, or personal information through coercion, threats, surveillance, dependency, disability, or intimate partner violence, this reflects the abuse, not a failure by the survivor, and should never be treated as gross negligence or fault, including when determining liability or eligibility for redress.

CONTACT

For more information or questions about this submission, please contact:

Michaela Mayer
Senior Director of Programs and Policy
Email: michaela.mayer@ccfwe.org
Visit our website: www.ccfwe.org

Meseret Haileyesus
Founder and Chief Executive Officer
Email: mesi.haileyesus@ccfwe.org