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

Canadian Center for Women's Empowerment (CCFWE)

Submission on the National Anti-Fraud Strategy

April 23, 2026

ISSUE

1. 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.

Economic abuse is a prevalent and often overlooked form of domestic violence. According to CCFWE's research, approximately 96% of people who experience domestic violence also report experiencing economic abuse, confirming similar results from studies conducted in Australia, the United Kingdom and the United States.

2. RELEVANCE TO THE NATIONAL ANTI-FRAUD STRATEGY

Economic abuse is crucial to understand when developing a National Anti-Fraud Strategy, as fraud is often used as a tactic of economic abuse. For people with lived/living experience of economic abuse, the risks of fraud are even higher as fraud is not only committed by external actors, but also by intimate partners and family members. This creates distinct risks, barriers to reporting, and challenges for awareness and prevention. The Strategy must account for these dynamics and ensure responses are trauma-informed and grounded in lived experience.

This Strategy must also incorporate insights from ongoing federal work on the Code of Conduct on the Prevention of Economic Abuse, including findings from roundtables and written submissions (see CCFWE's submission). These contributions provide critical context on how economic abuse manifests in practice and how systems can unintentionally enable harm. Thus, they should directly inform the design of fraud prevention, detection, and response measures.

RESPONSES TO CONSULTATION QUESTIONS

1. Are the three described sectors appropriate for the initial phase of a Framework? Should other sectors be considered?

While the three sectors mentioned are important starting points, CCFWE strongly recommends explicitly incorporating the gender-based violence (GBV) and social services sector. Frontline organizations such as shelters, women's advocacy groups, and support workers are often the first to learn about fraud in the context of domestic violence, including coerced debt, identity misuse, and broader forms of economic abuse and fraud. They provide essential insight into how fraud intersects with power and control dynamics, which are not captured through traditional sectoral lenses.

Fraud still remains underreported, as the Canadian Anti-Fraud Centre (CAFC) estimates that less than 5% of people who experience fraud report their experiences (CAFC, 2026). It is critical to ensure that the perspectives of people with lived/living experience of economic abuse and fraud are directly included, as their insights are essential to fully understanding the impacts and gaps in current responses.

Expanding the proposed framework to include these perspectives would align with ongoing work to establish a voluntary Code of Conduct on the Prevention of Economic Abuse. Including this sector and perspectives would ensure that the framework captures the lived realities of people who have experienced fraud, strengthens prevention and response measures, and aligns with Canada's broader commitments to advancing gender equity and economic justice.

2. What role could a central regulator play in a Multi-Sector Anti-Fraud Framework?

A central regulator would play a key role in standardizing responses and ensuring accountability across the Multi-Sector Anti-Fraud Framework. It should establish minimum standards grounded in survivor-driven, intersectional and trauma- and violence-informed approaches. These approaches ensure those experiencing fraud are treated consistently and compassionately across sectors. The regulator should also coordinate efforts and information-sharing among participating organizations and governmental bodies, reducing the need for individuals to recount their experiences. Finally, the central regulator should also hold organizations accountable for meeting their obligations and monitoring compliance.

3. What role could sector-specific regulators play in the Framework?

Sector-specific regulators would play a critical role in operationalizing the Framework within their respective industries by developing detailed, sector-tailored standards that reflect the specific risks, practices, and touchpoints of fraud in each domain. Building on overarching guidance from a central regulator, they should translate minimum standards into clear protocols for prevention, detection, reporting, and response that are consistent across institutions within the

sector, while embedding intersectional and trauma-and violence-informed approaches. This would ensure that people who have experienced harm receive appropriate, consistent support regardless of the provider they interact with, and that sector-specific dynamics and barriers are effectively addressed.

Regulators should use a survivor-centred approach and also actively engage with people with lived/living experience as well as frontline workers, gender-based violence and fraud organizations to understand risk factors, barriers, lived experiences, and emerging needs. This can help ensure that sector responses remain effective, accessible, and grounded in the realities of those most impacted by fraud.

7. What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?

Information sharing should be centred on the realities of people with lived/living experience and include disaggregated data to capture diverse experiences of fraud. It should also ensure clear, transparent, and ongoing communication so individuals understand what information is being shared about them and what they are consenting to. Individuals should be notified of any information sharing through written communication and have the right to withdraw information sharing at any time.

1. Prevention

12. How should organizations be required to embed compliance with the Framework into their governance models?

Compliance should be mandatory to protect individuals. Organizations should be required to embed enforceable standards and safeguards. Requirements should also include ongoing monitoring and the ability to adapt regulations as risks evolve.

13. How can organizations ensure that anti-fraud training is effective and how should this be reflected in government policy or legislation?

Anti-fraud training should be survivor-led and co-developed with frontline workers and organizations such as CCFWE and other gender-based violence (GBV) and fraud prevention groups. For the development of the voluntary Code of Conduct on the Prevention of Economic Abuse, CCFWE collaborated with the federal government, particularly Finance Canada and WAGE, and organized a roundtable discussion with victim-survivors of economic abuse. This approach helped ensure that individuals with lived/living experience were included in the design of the Code of Conduct from the outset. CCFWE would welcome the opportunity to partner with the federal government to organize similar engagements to support the development of the Anti-Fraud Framework.

It should be tailored to all staff levels, from senior management to supervisors and client-facing employees. Training needs to address all forms of fraud, including economic abuse, coerced debt, and the intersections of fraud with other forms of GBV. It should also include response strategies, including trauma-and violence-informed communication and support to avoid revictimization. Training should also be supported by clear internal processes that define responsibilities at each level of the organization when fraud is suspected or identified, aligned with approaches reflected in the Code of Conduct on the Prevention of Economic Abuse.

14. When, and how, should organizations be required to validate the identity of users of their services?

When validating user identity, organizations have to conduct this in ways that are flexible and do not create barriers to access. People with lived/living experience often face barriers to support due to missing identification, sometimes left behind when fleeing violence or intentionally withheld by a partner causing harm. Therefore, requirements should include alternative verification options and exceptions, such as the FCAC Bulletin (Feb 22, 2023). This allows banks to use alternative methods of identification for groups who are vulnerable, specifically mentioning people with lived/living experience of domestic abuse. Anti-fraud measures must be designed to protect against risk without preventing people with lived/living experience of GBV from safely accessing essential services.

15. What fraud-related information should organizations be required to make available to individuals using, or who may use, their services?

Organizations should provide clear and accessible information on all forms of fraud, including economic abuse and coerced debt. Economic abuse is still not widely known and understood in support responses. Therefore, organizations can play an important role in raising awareness by informing customers early about how fraud can also occur within intimate or romantic relationships and what warning signs to look for. This helps to prevent harm from the outset. Organizations can also draw on existing resources developed by CCFWE and other GBV organizations, such as Women's Shelters Canada, to share with customers.

2. Detection

19. How should organizations be required to assess fraud-related harms to individuals using their services?

Organizations should proactively design and review their products and services to mitigate the risk of misuse, including intimate partners causing harm. This includes considering how joint accounts, loans, or digital tools could be exploited to control, monitor, or coerce people with lived/living experience of economic abuse and GBV. Product safety assessments should go beyond traditional fraud and cybersecurity concerns to explicitly address economic abuse as a potential threat.

Collaboration with people experiencing fraud, including economic abuse and organizations such as CCFWE is essential in this process. By consulting people with lived/living experience and conducting focus groups with those who have experienced GBV and IPV, organizations can better understand real-world tactics and vulnerabilities that may not be immediately apparent to internal teams.

Organizations should include people who experienced fraud in internal product risk assessments or reviews evaluating product safety. This ensures that products are assessed not only for technical and security risks but also for the ways they might get weaponized, creating stronger, survivor-informed safeguards from the outset.

Organizations should also establish clauses in their standard customer Terms and Conditions that explicitly prohibit the use of their products and services to perpetrate fraud or harm. Breaching these clauses could constitute a violation of the contract, allowing an organization to take appropriate action against the person causing harm, even as a customer, without creating a conflict of interest. This approach reinforces accountability and signals that organizations are committed to protecting people from experiencing financial harm.

23. What privacy safeguards or oversight mechanisms should be in place for such information sharing initiatives?

Strong safeguards are needed to ensure that sensitive customer information is not shared with intimate partners as joint account holders, as it could enable economic abuse and potential harm. For instance, organizations should prevent disclosures of sensitive customer information changes even where accounts are shared, such as updated addresses or contact details, as this could alert the partner, causing harm. Information-sharing initiatives must account for these risks, with clear protocols, staff training, and oversight to prioritize the safety and privacy of people who are experiencing economic abuse and/or GBV.

3. Disruption

31. How can a balance be struck to limit use of industry infrastructure for fraudulent purposes, while ensuring that legitimate users are not unreasonably cut off from use of services?

As noted in question 19, organizations need to hear directly from individuals experiencing fraud and economic abuse. This can be done through a dedicated advisory group of people with lived/living experience, as was done with the National Code of Conduct for the Prevention of Economic Abuse. This is critical to understanding how fraud can occur in real-life contexts, particularly where systems may be misused by an intimate partner causing harm. This can also give insight into the barriers to reporting and accessing support for fraud.

There is a real risk that partners causing violence falsely report fraud as a form of coercive control, especially in post-separation contexts, thus reversing the victim and offender roles. If

not carefully assessed, this can lead to people experiencing the harm losing access to their accounts and financial resources, increasing vulnerability and potentially forcing a return to unsafe situations. Similar unintended consequences have been identified in other policy contexts such as considerations on the criminalization of coercive control.

4. Response

36. How should organizations be required to facilitate users' reporting of fraud activity to organizations?

Organizations should be required to make fraud reporting accessible, simple, and safe for all users, taking into account intersectional barriers such as language, disability, cultural and racial background, digital access, literacy, and safety concerns. This includes offering multiple reporting channels (online, phone, in-person), culturally and linguistically appropriate services, and options that protect the privacy and safety of people who are experiencing the harm, particularly those experiencing economic abuse or coercive control. Reporting processes should be trauma-informed and designed to reduce barriers, ensuring all individuals can report fraud without risk, undue burden or re-traumatization.

39. What information should organizations be required to include in a summary of complaint?

Summaries of complaints should include relevant contextual information to help identify patterns of harm, including whether fraud may be linked to GBV or IPV. Where appropriate, organizations should collect this data in collaboration with anti-violence shelters and community organizations, to better understand whether incidents are isolated or part of a broader pattern of violence, while ensuring privacy and safety are maintained.

5. Empower Canadians to act against fraud

46. How can the government improve Canadians' awareness of the threat posed by fraud and better position them to protect themselves against fraud?

The government should require organizations to share clear, accessible information on all forms of fraud, including economic abuse and fraud by intimate partners, as noted in question 15.

Public education efforts on fraud should adopt a trauma- and violence-informed, GBV lens and target populations most impacted such as seniors, young people, immigrants, refugees and newcomers, people with disabilities, First Nation, Metis, and Inuit, Black and other racialized communities. This could include data literacy training for older adults, and materials that are available in multiple languages and culturally sensitive formats to ensure broad, equitable, and accessible access.

About the Canadian Center for Women's Empowerment (CCFWE)

The Canadian Center for Women's Empowerment (CCFWE) is Canada's only national non-profit organization dedicated to addressing economic abuse through education, research, economic empowerment, policy influencing, and systems change.

CCFWE works to advance financial safety and long-term economic security for survivors by developing survivor-centered, culturally responsive, and evidence-informed approaches. The organization collaborates with community organizations, financial institutions, policymakers, researchers, and advocates to strengthen prevention, improve institutional responses, and support survivors in rebuilding their economic independence.

Through research, training, public education, and policy advocacy, CCFWE works to close systemic gaps that allow economic abuse to persist and to promote financial systems that are safe, equitable, and accessible for all.

Contact:
Michaela Mayer, Senior Director of Programs and Policy, CCFWE
Email: michaela.mayer@ccfwe.org

Meseret Haileyesus, Executive Director, CCFWE
Email: mesi.haileyesus@ccfwe.org