CANADIAN ASSOCIATION OF RETIRED PERSONS

National Anti-Fraud Strategy Consultation Response

Department of Finance Canada

Submitted by Canadian Association of Retired Persons - April 28, 2026

Opening Position

The Canadian Association of Retired Persons, CARP, represents more than 250,000 members across Canada. CARP welcomes the federal government's decision to address the growing threat of fraud, but our position is direct: a national anti-fraud strategy will not, by itself, protect Canadians.

Canada needs a national anti-fraud action plan.

That action plan must include enforceable obligations, defined timelines, measurable outcomes, public reporting, and consequences for failure. It must also include a clear commitment that governments will require banks, telecommunications providers, digital platforms, law enforcement agencies, and regulators to play their part.

Fraud is no longer an isolated consumer-risk issue. It is organized, technologically enabled, and distributed through systems Canadians rely on every day: financial institutions, payment networks, telecommunications infrastructure, social media platforms, search engines, digital advertising systems, and messaging services.

The current model places too much responsibility on individuals and too little on the institutions that operate and profit from these systems. Older Canadians are told to be careful, watch for warning signs, and report suspicious activity. Many do exactly that. It has not been enough.

CARP's core position is that fraud prevention must become a system responsibility. If a regulated or commercial system allows fraud to be carried through its infrastructure, that system must share responsibility for the outcome.

CANADIAN ASSOCIATION OF RETIRED PERSONS

Context and Problem Definition

The federal consultation paper properly identifies fraud as a multi-sector problem. It recognizes that fraudsters engage victims through emails, text messages, phone calls, social media posts, paid advertisements, impersonation, coercion, and increasingly sophisticated digital tactics. It also recognizes that fraudsters exploit gaps between sectors.

The scale of the problem has changed. Canadians reported losing more than $704 million to fraud in 2025, with reported losses since 2022 exceeding $2.4 billion. The government's own materials note that only an estimated 5 to 10 percent of incidents are reported. The true scale of the harm is therefore far higher and will only grow without immediate intervention from industry, regulators and legislators.

Fraudsters are often outside Canada. They move quickly across jurisdictions. They use digital tools to obscure identity, target victims, impersonate trusted institutions, and move money before intervention is possible. Artificial intelligence and synthetic media will only increase the speed, credibility, and reach of these schemes.

Older Canadians face distinct and serious consequences. A fraud loss in later life is not simply a financial inconvenience. It may involve retirement savings, pension income, home equity, or funds accumulated over decades. Many older Canadians cannot re-enter the workforce, replace lost capital, or recover from a large financial loss. The harm is often permanent.

Canada has studied problems affecting older Canadians many times. A National Seniors Strategy was examined but never fully implemented. Long-term care standards were developed but remain uneven. Financial consumer protection frameworks have improved disclosure and process, but have not corrected the imbalance between institutions and individuals.

The pattern is familiar. Canada does not lack awareness of the problem. It lacks execution, accountability, and enforcement.

This consultation must not repeat that cycle.

CANADIAN ASSOCIATION OF RETIRED PERSONS

Evidence from CARP Members

CARP's National Omnibus Poll, conducted April 17 to 22, 2026, with 7,878 respondents, provides current evidence of the scale of fraud exposure among older Canadians.

More than 82 percent of respondents reported that someone had attempted to scam them by phone, in person, online, or through another channel. This is a routine feature of life for many older Canadians.

The channels used by fraudsters are consistent with the federal government's own description of modern fraud. Among respondents who had been targeted, 88.51 percent reported telephone-based scam attempts. Email scams were reported by 68.51 percent. Online scams through websites or advertisements were reported by 49.93 percent. Text-message scams were reported by 48.89 percent.

These results show that fraud is not confined to one sector. It is multi-channel and persistent. A credible response cannot focus only on banks, only on police, or only on public education. It must address the full path by which fraud reaches victims and extracts money.

Nearly 18 percent of respondents reported that they had been victims of fraud and lost money. Some respondents reported unauthorized withdrawals from bank accounts. Others reported credit card purchases, gift card purchases, or other transactions made under false pretenses. This distinction is central to the policy problem. Current protections are stronger for some unauthorized transactions than for transactions induced by deception, coercion, impersonation, or manipulation.

The reporting data reveals a second failure.

Among respondents, 86.39 percent said they would report fraud to their financial institution, and 88.33 percent said they would report it to police. Yet among those who had experienced fraud, only 58.48 percent reported it to their financial institution, 33.09 percent reported it to police, and 22.37 percent reported it to the Canadian Anti-Fraud Centre. More than 21 percent did not report the fraud at all.

That gap reflects a lack of confidence that reporting will lead to recovery, accountability, or justice.

CARP members strongly support government intervention. In the same poll, 88.66 percent of respondents said the government should do more to protect Canadians from fraud. More than 90 percent said the government should require phone and mobile service providers, including companies such as Rogers, Bell, and Telus, to do more to protect customers from robocalls, caller ID spoofing, and fraudulent text messages.

The direction from CARP members is clear. Older Canadians do not want fraud prevention left to individual vigilance. They expect governments to require institutions to do their part.

System Failures and Gaps

The current system places responsibility on individuals after fraud occurs, rather than placing enforceable duties on institutions before fraud succeeds.

Financial institutions are the final gatekeepers of most financial losses. Fraudsters generally cannot extract money without using banking or payment infrastructure. Banks already use sophisticated systems to detect abnormal behaviour in other contexts, including anti-money laundering, credit risk, internal fraud, and account security. The same level of seriousness must apply to consumer-targeted fraud.

At present, reimbursement remains inconsistent. Consumers face different outcomes depending on the institution, the type of transaction, the interpretation of authorization, and the bank's internal policies.

Telecommunications providers carry fraudulent calls and text messages across their networks. Technical measures exist to authenticate calls, detect spoofing, flag suspicious traffic, and block known fraudulent patterns. These measures should not depend on voluntary adoption or uneven implementation. If telecom infrastructure is used to target Canadians, telecom providers must carry enforceable prevention and disruption duties.

Digital platforms are now central to the fraud ecosystem. Fraudulent advertisements, impersonation accounts, fake investment promotions, romance scams, and malicious links are delivered through platforms with enormous reach. Companies such as Meta and other major social media, messaging, search, and advertising platforms design the systems through which fraudulent content is distributed. They also earn revenue from paid advertising, including advertising placed by bad actors.

A platform that profits from fraudulent advertising cannot be treated as a passive bystander.

Complaint systems are fragmented. A victim may be told to contact a bank, a telecom provider, a digital platform, police, the Canadian Anti-Fraud Centre, or a regulator. Each has different procedures. Each may treat only part of the problem. The burden falls on the victim to navigate the system at the moment they are least equipped to do so.

Criminal enforcement has not kept pace. Fraud is a criminal offence, but many victims experience little sign that the criminal justice system can investigate, recover funds, or deliver accountability at the scale required. Reporting without visible action produces cynicism and underreporting.

The contrast with institutional losses is stark. When institutions lose money, the system responds quickly and decisively. The theft of $20M gold from Toronto Pearson International Airport triggered coordinated investigation, insurance response, and sustained public attention. That gold did not belong to individual Canadians. It belonged to an institution. The financial exposure and reputational risk were immediate.

Individual fraud victims do not receive the same response. Their losses are treated differently. Recovery is uncertain. Accountability is unclear. For many older Canadians, the loss remains with them for the rest of their lives.

CARP Perspective

CARP represents more than 250,000 members. We speak on their behalf, and for older Canadians who are not present in this consultation process. We are also speaking for those who have already lost money to fraud and scams, and for those who will be victimized unless the system changes.

Many victims did what they were told to do. They trusted the systems in front of them. They used regulated banks, recognized telecommunications networks, major digital platforms, and familiar payment tools. When those systems failed, the loss was theirs.

CARP members are not asking for more general warnings. They are asking for protection, accountability, and justice.

That means prevention must be embedded into the systems themselves. It means banks, telecommunications providers, digital platforms, regulators, and law enforcement agencies must have clear duties. It means liability must shift upstream where institutional failures contribute to loss. It means complaint processes must be binding, accessible, and designed around victims rather than institutional convenience. It means law enforcement must be funded and equipped to treat fraud as a serious economic crime.

A system that tells older Canadians to be careful, while failing to require institutions to prevent foreseeable harm, has the wrong priorities.

Recommendations

1. Replace strategy-only language with a national anti-fraud action plan.
The Government of Canada should commit to a national action plan with statutory obligations, implementation deadlines, measurable targets, public reporting, and enforcement consequences. The action plan should identify which institutions are responsible for which duties, how performance will be measured, and what happens when obligations are not met.

2. Establish a national liability framework.
Where a financial institution, telecommunications provider, digital platform, or other regulated organization fails to meet its prevention, detection, disruption, or response obligations, and that failure contributes to a victim's loss, the victim should be compensated. Where multiple institutions contributed to the failure, they should apportion responsibility among themselves after the victim is made whole.

3. Impose stronger duties on financial institutions.
Banks and payment providers should be required to implement real-time monitoring, behavioural analytics, mandatory intervention thresholds, delayed or reversible processing for high-risk transactions, payee verification, and customer-controlled safety settings. Reimbursement standards should be consistent nationally and should not depend on internal discretion.

4. Require telecommunications providers to prevent and disrupt fraud traffic.
Telecom providers should be required to implement call authentication, spoofing prevention, proactive blocking or flagging of known fraudulent traffic, text-message filtering, and real-time warnings for high-risk communications. These should be enforceable duties, not optional measures.

CANADIAN ASSOCIATION OF RETIRED PERSONS

5. Regulate digital platforms as active participants in fraud prevention.
Digital platforms, including Meta and other major social media, search, messaging, and advertising platforms, should be subject to advertiser verification, fraud-ad screening, impersonation controls, malicious-link detection, rapid takedown obligations, user notification requirements, and public fraud reporting. Civil liability should apply where platforms fail to meet their duties. Criminal consequences should be available where there is willful blindness, reckless disregard, repeated non-compliance, concealment, or knowing facilitation of fraud.

6. Create a single complaint and dispute-resolution pathway.
Victims should not have to determine whether the bank, telecom provider, platform, or another actor failed them. The framework should create a single point of entry for complaints, coordinated cross-sector investigation, written reasons, defined timelines, and binding external dispute resolution.

7. Strengthen criminal enforcement.
The action plan should include dedicated funding for fraud investigation, stronger penalties for organized fraud, improved tools for asset tracing and freezing, better cross-border cooperation, and the ability to pursue entities that knowingly or recklessly allow their infrastructure to be used for fraud.

8. Mandate timely data sharing with safeguards.
Regulated organizations, regulators, government bodies, and law enforcement should be able to share targeted fraud-related information quickly enough to prevent loss. Safeguards should include purpose limitation, data minimization, retention limits, access controls, audit trails, and independent oversight.

9. Identify older Canadians as a priority group.
The framework should explicitly recognize older Canadians as a priority population. Their risk profile, reporting barriers, fixed incomes, reduced ability to rebuild savings, and greater consequences from permanent loss should shape the design of safeguards, complaint processes, reimbursement standards, and enforcement priorities.

CANADIAN ASSOCIATION OF RETIRED PERSONS

Appendix A

CARP Responses to Consultation Questions

A. Multi-Sector Anti-Fraud Framework

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

Yes. Financial institutions, telecommunications providers, and digital platforms are the correct starting point. These are the principal channels through which modern fraud is delivered, legitimized, and monetized.

A victim may first encounter fraud through a telephone call, text message, social media advertisement, impersonation account, email, or fraudulent website. The financial loss then often occurs through a bank account, credit card, wire transfer, electronic funds transfer, or other payment mechanism. Treating those sectors separately has allowed fraudsters to exploit the gaps between them.

The initial phase should include banks and other federally regulated financial institutions, telecommunications service providers, social media platforms, instant messaging services, search engines, and digital advertising systems. Future phases should consider payment processors, online marketplaces, crypto-asset intermediaries, and other entities where evidence shows they are facilitating fraud.

CARP's position is that scope should be based on function, not institutional category. If an organization's infrastructure is being used to reach victims, build credibility, move money, conceal identity, or avoid accountability, it should be within reach of the framework.

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

A central regulator should be the institutional answer to the fragmentation that defines modern fraud.

Fraud does not respect sector boundaries. A victim may be reached through a spoofed call, manipulated through a social media platform, and defrauded through a bank transfer. No single sector sees the full scheme. No single regulator has clear responsibility for the full outcome. That is the current failure.

A central regulator should establish baseline obligations, coordinate enforcement, collect standardized fraud data, publish performance results, oversee cross-sector complaints, issue binding compliance directions, and **refer serious matters for prosecution**. It should not replace sector regulators. It should ensure the framework operates as a single system rather than a collection of disconnected obligations.

For older Canadians, this is not a technical governance issue. It determines whether they can find help. A fraud victim should not have to understand federal regulatory architecture before they can report harm, seek recovery, or obtain a remedy.

The central regulator should be required to report publicly on whether the framework is reducing losses, shortening complaint timelines, increasing reimbursement, and improving enforcement outcomes. Without that public accountability, Canada will have another strategy with no reliable measure of whether it is working.

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

Sector-specific regulators should enforce the technical and operational rules within their areas of expertise. FCAC should oversee financial-sector obligations. The CRTC should oversee telecommunications obligations. A designated regulator should oversee digital platforms, including social media, search, messaging, and advertising systems.

Those regulators should not operate in silos. They should be required to share relevant fraud intelligence, coordinate supervisory activity, and participate in cross-sector enforcement where more than one sector contributed to harm.

The purpose of sector-specific regulation should be expertise, not fragmentation. A telecom regulator may understand spoofing and network traffic. A financial regulator may understand payment controls and account monitoring. A platform regulator may understand advertiser verification and content systems. The victim should not be forced to assemble those pieces.

4. How can effective oversight of the Framework be achieved, without duplication of existing oversight of the three sectors?

Effective oversight can be achieved through a clear division of responsibility. The central regulator should own the framework as a whole, including cross-sector standards, public reporting, complaint pathways, and systemic enforcement. Sector-specific regulators should enforce detailed technical rules in their domains.

Duplication is not the primary risk; fragmentation is. The current system already suffers from fragmented responsibility. A well-designed framework should reduce duplication by making roles explicit and by creating one visible point of accountability for victims.

The government should establish common definitions, common reporting standards, common timelines, and a single consumer-facing escalation route. Institutions can coordinate behind the scenes. The victim should not carry that burden.

B. Information Sharing Between Regulators

5. When should Framework regulators be permitted to share fraud-related information with each other to further the Strategy aims of preventing, detecting, disrupting and investigating fraud?

Regulators should be permitted to share fraud-related information as soon as there are reasonable grounds to believe that the information could prevent, detect, disrupt, investigate, or remediate fraud.

The threshold should not be so high that regulators must wait for full confirmation while losses accumulate. In fraud, delay favours the offender. Funds move quickly. Fraudulent advertisements disappear quickly. Spoofed numbers and malicious domains are replaced quickly. A cautious but slow information-sharing regime will fail victims.

The purpose of inter-regulator sharing should be action. It should allow regulators to identify emerging patterns, warn counterpart regulators, trigger coordinated supervisory responses, and intervene before additional Canadians are harmed.

Privacy safeguards are necessary, but privacy should not become a reason for operational paralysis. Fraud-related information sharing can be narrow, purposeful, logged, reviewable, and still fast enough to prevent harm.

6. What specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?

Regulators should be able to share confirmed or suspected fraud indicators, suspicious account patterns, mule-account information, spoofed numbers, malicious domains, fraudulent advertisement identifiers, impersonation patterns, platform account data relevant to fraud, complaint trends, and loss data.

Information should be shared when there are reasonable grounds to suspect an active scheme, when more than one sector may be implicated, when victims are being targeted at scale, when older Canadians or other vulnerable groups appear to be affected, or when a regulated entity may have failed to meet its obligations.

The purpose should be limited to fraud prevention, detection, disruption, investigation, enforcement, complaint resolution, victim protection, and recovery. The framework should prohibit secondary use unrelated to those purposes.

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

The framework should require data minimization, purpose limitation, retention limits, access controls, audit trails, secure handling, and independent oversight. Every information-sharing authority should be linked to a defined fraud-prevention or enforcement purpose.

Canadians' privacy rights must be protected. At the same time, privacy must not be used as a blanket excuse for inaction where targeted sharing could prevent serious financial harm.

The government should require public reporting on the use of information-sharing powers, including the number of disclosures, general categories of information shared, and the purposes for which sharing occurred. That reporting should not compromise investigations, but it should permit democratic oversight.

C. Reporting Fraud-Related Information to Law Enforcement

8. When should Framework regulators be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting, and investigating fraud?

Framework regulators should be permitted to share fraud-related information with law enforcement early and routinely in serious matters.

This includes cases involving organized activity, repeat offenders, significant losses, vulnerable victims, older Canadians, cross-border activity, mule accounts, impersonation networks, or evidence that a regulated entity knowingly failed to act on clear fraud indicators.

CARP is concerned that fraud affecting individual Canadians, especially seniors, is too often treated as an unfortunate private loss rather than a serious economic crime. That approach does not match the harm. A senior who loses retirement savings to fraud may have lost money that cannot realistically be replaced.

Law enforcement should be brought in where the pattern, scale, or victim impact justifies a criminal investigation. **Serious institutional non-compliance should also be reportable to law enforcement**. If a company knowingly or recklessly allows its infrastructure to be used for fraud, the framework should not treat that only as a compliance issue.

9. When should law enforcement be permitted to share fraud-related information with private sector organizations?

Law enforcement should be permitted to share fraud-related information with private sector organizations when doing so can prevent further victimization, freeze or trace funds, remove fraudulent content, block fraudulent communications, identify exposed customers, or preserve evidence.

Fraud schemes move quickly. Law enforcement information that arrives too late may be useless. A properly designed framework should allow time-sensitive operational sharing while maintaining safeguards for privacy, investigations, and due process.

Once an organization receives credible fraud information from law enforcement, it should have a duty to act. It should not be able to claim ignorance after being alerted to an active threat.

10. What specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?

Law enforcement should be able to share active threat indicators, suspect account information, fraudulent phone numbers, malicious links, impersonation details, known scam scripts, fraudulent advertisement identifiers, and urgent warnings tied to active campaigns.

This information should be shared where it can help stop ongoing losses, protect identified or likely victims, support takedown activity, assist asset recovery, or preserve evidence for investigation.

The purpose should be immediate prevention, disruption, victim protection, and evidence preservation. The framework should not permit broad or unrelated use.

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

Information sharing with law enforcement should be governed by clear statutory authority, purpose limits, data minimization, secure channels, audit logs, and oversight. Where more intrusive information is involved, appropriate legal thresholds should apply.

The framework should respect the Charter and privacy rights while recognizing that the absence of timely information sharing imposes real costs on victims. Privacy protection and fraud prevention are not mutually exclusive. The issue is designing rules that allow targeted action without creating open-ended surveillance.

D. Prevention

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

Anti-fraud compliance should be a board-level and executive-level responsibility.

Fraud risk should not be treated as a customer service issue, a public relations matter, or a discretionary operational concern. For organizations that handle money, communications, identity, advertising, or digital engagement at scale, fraud risk is material. It should be governed accordingly.

Each regulated organization should be required to designate a senior executive responsible for framework compliance. A board committee should receive regular reports on fraud volumes,

losses, response times, complaint outcomes, reimbursement rates, enforcement actions, and emerging threats. Organizations should maintain written prevention, detection, disruption, and response procedures, subject to independent audit.

Governance rules should also require evidence of actual performance. It is not enough for an organization to have a policy. It must show that the policy reduces harm.

Where organizations fail to embed these responsibilities meaningfully, consequences should apply. Formal compliance language without operational change will not protect Canadians.

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

Training should be mandatory, role-specific, regularly updated, and tested. Frontline staff, complaints staff, fraud teams, executives, and third-party service providers should receive training tailored to their functions.

Training should include current scam typologies, indicators of coercion, elder financial abuse, social engineering, unusual transaction patterns, escalation duties, evidence preservation, and obligations under the framework.

Effectiveness should not be measured by attendance. It should be measured by performance: whether staff identify suspicious activity, escalate appropriately, intervene before loss occurs, and handle complaints properly.

Government policy should require regulated organizations to maintain training records, test competency, update content regularly, and report training compliance to regulators.

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

Identity validation should be required at points of heightened risk. These include account opening, creation of new payment recipients, changes to authentication details, changes to contact information, high-value transfers, unusual activity, advertiser onboarding, and recovery from account compromise.

For digital platforms, identity verification should apply to financial advertisers, investment promoters, impersonation-risk accounts, and users seeking to run paid advertisements in high-risk categories.

Identity validation must be strong enough to prevent fraud but accessible enough not to exclude older Canadians or people with limited digital access. The design should include alternative verification pathways and human support where needed.

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, accessible, plain-language information about current fraud risks, how their services are being misused, what protections are available, how to report fraud, what happens after a report, what rights consumers have, and when reimbursement may be available.

This information should not be buried in terms and conditions. It should be visible at points of risk, including when initiating large transfers, adding new payees, responding to suspicious communications, engaging with financial advertisements, or changing account security settings.

For older Canadians, accessibility matters. Information should be available by phone, online, in large print where appropriate, and through channels that do not assume high digital literacy.

16. How should the effectiveness of organizations' fraud education be assessed to ensure that it meaningfully reduces harm?

Fraud education should be assessed by outcomes, not by whether brochures, webpages, or warnings exist.

Relevant measures include reductions in fraud losses, fewer repeat victims, faster reporting, faster intervention, lower complaint volumes, improved reimbursement outcomes, and better public understanding of rights and reporting pathways.

Education is necessary, but it is not sufficient. CARP is concerned that awareness can become a substitute for accountability. Canadians have been told for years to be careful. Losses continue to rise. The framework should make clear that consumer education is a complement to system-level protections, not a replacement for them.

17. What sector-specific fraud prevention rules should be in place?

Sector-specific prevention rules should reflect the actual pathways through which fraud is executed.

Financial institutions should be required to provide real-time alerts, verify high-risk transactions, monitor behavioural anomalies, allow customer-controlled transaction limits, delay suspicious transfers, and provide meaningful controls over high-risk account capabilities. If a transaction departs sharply from a customer's normal pattern, the institution should have a duty to intervene before the money is gone.

Telecommunications providers should be required to authenticate calls, prevent spoofing, block or flag known fraudulent numbers, filter high-risk text traffic, and suppress active scam campaigns. These measures should not be left to voluntary adoption.

Digital platforms should be required to verify advertisers, screen financial and investment ads, prevent banned users from returning under new accounts, detect fraudulent profiles and pages, block malicious links, and remove fraudulent content quickly. Platforms such as Meta should not be permitted to earn revenue from fraudulent advertising while avoiding responsibility for the harm caused.

Across all sectors, prevention duties must be tied to liability. Without consequences, prevention will remain uneven.

E. Detection

18. How could organizations be incentivized to effectively detect and investigate potentially fraudulent activity on their services?

The strongest incentive is consequence.

Where the financial and operational consequences of fraud fall mainly on victims, institutions will not have sufficient reason to invest in prevention and detection at the scale required. The framework should reverse that incentive structure.

Organizations that fail to detect or investigate fraud where they reasonably should have done so should face civil liability, administrative penalties, public reporting consequences, and, in serious cases, referral for criminal investigation.

Detection performance should be publicly measured. Organizations should report fraud volumes, customer losses, reimbursement outcomes, response times, complaint results, repeat fraud, and takedown or disruption activity. If one bank, telecom provider, or platform performs materially worse than others, regulators and the public should know.

For older Canadians, detection is the difference between an interrupted scam and a permanent loss. It cannot depend on voluntary goodwill.

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

Organizations should be required to assess the full harm caused by fraud, not only the immediate amount lost.

That assessment should include direct financial loss, future financial exposure, compromised credentials, identity theft risk, account vulnerability, service disruption, emotional stress, loss of confidence, and risk of repeat victimization.

For older Canadians, the assessment must recognize that losses may be permanent. Retirement savings, pension income, or home equity cannot typically be replaced. A narrow transaction-based view of harm fails to capture the lived reality of senior victims. Organizations should also assess what remedial steps are required to prevent further harm, including account changes, monitoring, warnings, and support for navigating complaints and recovery.

20. What actions should organizations be required to take to assess risk of future harm to individuals impacted by fraud?

Organizations should be required to secure accounts, replace compromised credentials, monitor related activity, flag accounts for heightened protection, warn affected users, identify connected risks, and provide clear follow-up support.

Where personal information has been compromised, organizations should assess the risk of future identity theft, account takeover, and repeat targeting. Where a victim has been exposed through a fraudulent advertisement, spoofed call, or impersonation scheme, the relevant platform or telecom provider should identify whether other users were exposed and warn them.

Assessment should not stop at the individual victim. Fraud often targets groups. A proper harm assessment should identify whether the same scheme is likely affecting others.

21. When should regulated private sector organizations be able to share fraud-related information with each other?

Organizations should be able to share fraud-related information when there are reasonable grounds to suspect fraud and when sharing can help prevent harm, stop ongoing activity, protect victims, trace funds, or support an investigation.

The current system is too slow and fragmented. A bank may see suspicious transfers. A telecom provider may see the spoofed calls. A platform may host the fraudulent advertisement. Unless those entities can share timely information, each sees only part of the scheme.

Information sharing should be lawful, narrow, and purposeful. It should also be operationally useful. **A framework that allows sharing only after losses are complete will not protect Canadians.**

22. If so, what precise information should be shared, under what circumstances should it be shared and for what precise purposes should it be shared?

Organizations should be able to share suspicious account identifiers, transaction patterns, payee information, mule-account indicators, fraudulent phone numbers, malicious links, ad identifiers, impersonation account data, scam scripts, and complaint clusters.

Sharing should occur when there is credible suspicion of fraud, a cross-sector pattern, an active campaign, repeated complaints, or exposure of multiple users.

The purposes should be prevention, detection, disruption, complaint resolution, victim protection, evidence preservation, and recovery. The framework should prohibit unrelated commercial use.

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

Private-sector information sharing should be governed by strict purpose limits, access controls, secure channels, retention limits, audit logs, and penalties for misuse.

Organizations should be required to document why information was shared, with whom, and for what purpose. Regulators should have access to those records.

The framework should also prohibit organizations from using fraud-related sharing as a basis for unrelated profiling, marketing, or commercial decision-making.

24. When should organizations be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting and investigating fraud?

Organizations should be permitted, and in serious cases required, to share fraud-related information with law enforcement when credible evidence suggests organized, repeated, large-scale, cross-border, or high-harm activity.

Law enforcement too often receives reports after funds have moved, accounts have been closed, and fraudulent infrastructure has disappeared. That model is poorly suited to modern fraud. Early sharing should occur where there are mule accounts, repeat fraud indicators, major losses, vulnerable victims, organized networks, platform-based fraud campaigns, or evidence of institutional non-compliance.

This is also a justice issue. CARP members do not only want warnings. They want fraud against older Canadians to be treated as a serious crime.

25. When should law enforcement be permitted to share fraud-related information with private sector organizations?

Law enforcement should be permitted to share information with private sector organizations when doing so can prevent further loss, support asset recovery, remove fraudulent content, block communications, identify victims, or preserve evidence.

This should include urgent alerts to banks, telecom providers, digital platforms, and payment intermediaries. The information should be targeted and linked to fraud prevention or enforcement.

Once an organization receives such information, it should be required to act within defined timelines.

26. When should the government be permitted to share fraud-related information with law enforcement?

The government should be permitted to share information with law enforcement when government identifiers, accounts, programs, benefits, or brands are being used in fraud.

This includes misuse of Social Insurance Numbers, government impersonation, benefit redirection, account compromise, and fraudulent claims involving government services.

Governments should not be a passive observer when its own systems or identifiers are used to facilitate fraud.

27. When should the government be permitted to share fraud-related information with private sector organizations?

The government should be permitted to share information with private sector organizations when doing so can prevent impersonation, protect users, verify fraudulent claims of official status, or help institutions stop misuse of government identifiers.

For example, if fraudsters are impersonating a government department through calls, texts, websites, or social media advertisements, relevant telecommunications providers, platforms, and financial institutions should be alerted quickly.

The purpose should be prevention and disruption, not general information exchange.

28. If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?

Governments should be able to share impersonation alerts, compromised identifier trends, fraudulent website or domain information, scam scripts using government names, false benefit claims, malicious contact points, and warnings tied to active campaigns.

Sharing should occur when a fraud campaign uses government identity, government-issued identifiers, or government programs to deceive Canadians.

The purpose should be to prevent harm, remove fraudulent content, block communications, stop account compromise, and support enforcement.

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

The same safeguards should apply: purpose limitation, data minimization, secure handling, retention limits, audit trails, and independent oversight.

Government information sharing should also be subject to transparent public reporting. Canadians should know that fraud-related sharing is occurring for protective purposes and under defined limits.

30. What sector-specific fraud detection rules should be in place?

Financial institutions should be required to monitor account activity in real time, use behavioural analytics, detect unusual transactions, verify suspicious new payees, and escalate high-risk activity before funds are released.

Telecommunications providers should be required to detect spoofing patterns, suspicious call volumes, fraudulent text traffic, and known scam campaigns. They should not be able to avoid responsibility by describing themselves only as carriers where technical detection capacity exists.

Digital platforms should be required to proactively detect fraudulent advertisements, impersonation accounts, malicious links, cloned profiles, and attempts by banned actors to return. They should report fraud volume, takedown times, recurrence rates, and user exposure.

Across all sectors, detection must be mandatory and tied to consequences. General statements about taking fraud seriously are not enough.

F. 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?

The framework should use risk-based intervention, fast review, written reasons, accessible appeals, and clear safeguards against improper suspension.

The current balance is not neutral. It allows many suspicious transactions, calls, ads, and accounts to proceed uninterrupted, while victims bear the consequences after the fact. In serious cases, a temporary pause is preferable to irreversible loss.

Legitimate users should have prompt recourse. But fraudsters should not benefit from systems designed to avoid any friction at all.

32. In what situations should regulated entities be required to pause potentially fraudulent activity?

Regulated entities should be required to pause activity where there are reasonable grounds to believe that a transaction, communication, account action, or advertisement may be linked to fraud and where delay could prevent irreversible harm.

This includes unusually high-value transfers, rapid addition of new payees followed by payment activity, large withdrawals inconsistent with normal behaviour, suspicious changes to authentication details, spoofed communications, fraudulent advertisements, and accounts linked to known scams.

For seniors, pause mechanisms are especially important. Many scams are engineered to create panic and urgency. A pause creates time for review, verification, and intervention.

33. What measures, safeguards and recourse should be put in place to ensure that individuals' access is not improperly suspended or removed?

Organizations should provide immediate notice, plain-language explanations, fast human review, accessible appeal channels, and clear timelines.

Where access is suspended improperly, it should be restored quickly. Where a transaction is paused, the customer should be told what must be verified and how long the process will take.

Safeguards should protect legitimate users without weakening the duty to prevent foreseeable fraud.

34. How can notifications of suspected fraudulent activity be effective?

Notifications must be immediate, clear, specific, and actionable. They should tell the user what risk has been identified, what action has been paused or flagged, what steps the user should take, and how to reach support.

Generic warnings are not enough. A vague message that “fraud may occur” is unlikely to stop a sophisticated scam.

For older Canadians, notifications should include live-support options and should avoid technical language. Where the risk is high, institutions should be required to make direct contact.

35. What sector-specific fraud disruption rules should be in place?

Banks should be required to freeze suspicious transfers, block known fraudulent recipient accounts, allow customers to disable risky account features, and preserve evidence for recovery and investigation. Telecommunications providers should block or intercept calls and messages from known fraudulent sources, suppress active scam campaigns, and remove access for accounts tied to fraud.

Digital platforms should immediately suspend suspicious advertisements, remove fraudulent and impersonation accounts, warn exposed users, and prevent repeat access by banned actors.

Where institutions fail to disrupt clearly suspicious activity that they identified or should have identified, that failure should be relevant to liability.

G. Response

36. How should organizations be required to make it easy for users to report fraud activity to them?

Organizations should provide visible, dedicated, and accessible fraud-reporting channels. These should include staffed telephone lines, simple online tools, confirmation of receipt, clear next steps, and access for people who are not comfortable with digital-only processes.

Fraud reporting should not be buried in general customer-service queues. It is time-sensitive. Delays can determine whether funds are recovered or lost permanently.

Reporting systems should be designed around the victim, not around institutional convenience.

37. How could organizations effectively investigate cross-sector complaints?

Cross-sector complaints should be handled through a single point of entry and a coordinated process.

A victim should not have to decide whether the failure occurred at the bank, the telecom provider, or the platform. Modern fraud often involves all three. Institutions should share information, maintain a common case file, and determine responsibility between themselves.

The victim should submit one complaint and receive one coherent response. Institutions can allocate fault afterward. The burden of fragmentation should not fall on the victim.

38. How long should organizations have to internally investigate complaints?

Organizations should be subject to short, defined timelines. Expedited timelines should apply where funds may still be recoverable, where active fraud is ongoing, or where the victim is older or vulnerable.

Fraud complaints cannot be treated like ordinary service disputes. Delay can destroy recovery options and deepen harm.

If an organization cannot complete its review within the defined timeline, the matter should escalate automatically.

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

Complaint summaries should include the facts established, obligations engaged, evidence considered, steps taken, findings on compliance, reasons for the outcome, remedy offered, and escalation rights.

The summary should be specific enough to allow review by the victim, an external complaint body, and regulators. Formulaic responses are not acceptable.

Written reasons are essential. Without them, complaint systems become shields against accountability.

40. Should organizations be held liable when they do not fulfill their obligations under the Framework?

Yes. This is central to CARP's position.

Without liability, the framework will amount to guidance. Guidance does not change incentives. Liability does.

If an organization fails to meet its prevention, detection, disruption, or response obligations, and that failure can be linked to a victim's loss, the organization should be required to make the victim whole. Where more than one organization contributed to the failure, they should apportion responsibility among themselves after the victim has been compensated.

If organizations operate the infrastructure through which fraud is carried out, and if they are in a position to reduce foreseeable harm, they should not be able to externalize the cost of failure onto victims.

For seniors, this is essential. The current model often leaves an older victim blamed for being deceived, denied reimbursement, and forced through an opaque complaint process. That is not consumer protection.

41. What standards should apply in determining whether an organization fulfilled its obligations?

Compliance should be judged against objective, statutory, and externally reviewable standards.

The test should consider what the organization knew or should reasonably have known, what safeguards were available, whether it acted promptly, whether it responded to known indicators, whether it complied with sector-specific duties, and whether its systems were reasonably designed to prevent foreseeable harm.

Internal policy alone should not define compliance. Institutions should not be allowed to set the standard by which they are judged.

Clear statutory standards will improve consistency, fairness, and enforceability.

42. How should liability be apportioned when multiple organizations have not fulfilled their obligations?

Liability should be apportioned according to fault, but the victim should not have to wait for institutions to resolve allocation.

In a multi-sector fraud case, a bank may point to a platform, the platform may point to a telecom provider, and the telecom provider may point back to the bank. That cannot become a reason to delay compensation.

The framework should require that the victim be made whole first, where non-compliance is established. Institutions can then resolve contributions among themselves.

Consumer protection should not be suspended while institutions argue over exposure.

43. What should inform how an external complaint body is chosen?

The external complaint body should be independent, accessible, expert, national in scope, and free from industry capture.

It must be designed for real users, including older Canadians who may not have legal support, technical fluency, or the ability to navigate complex institutional processes.

The body should have expertise across banking, telecommunications, digital platforms, fraud typologies, consumer protection, and dispute resolution.

44. Should decisions of the external complaint body be binding?

Yes. Non-binding outcomes are inadequate.

If an external body can only recommend relief, institutions may absorb criticism and refuse meaningful remedies. That does not correct the imbalance between an individual victim and a large institution.

A binding authority is necessary to rebuild confidence and produce consistent outcomes. CARP has supported binding authority in ombudsman contexts. The same principle applies here.

Where the stakes involve permanent losses, fragmented responsibility, and serious power imbalance, recommendations are not enough.

45. How long should the external complaints body have to investigate escalated complaints?

The external body should be subject to defined service standards, with expedited timelines for urgent cases, older victims, active fraud, or situations where funds may still be recoverable.

Timeliness is part of the remedy. A decision that arrives after recovery is impossible has limited value.

The body should publish performance data, including timelines, outcomes, compliance rates, and reimbursement results.

H. 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?

Governments should improve awareness, but it should do so with realism. **Awareness is not a substitute for accountability.**

Canadians have been warned for years to protect themselves. Fraud losses continue to rise. That demonstrates the limits of an education-led response.

Public awareness should be practical, current, targeted, and tied to actual reporting and recovery pathways. It should reflect how people are being targeted: phone, email, text, social media, search, online ads, and impersonation schemes.

For older Canadians, messaging should be plain-language, repeated through trusted channels, and paired with live support options.

The government should not frame fraud primarily as a failure of individual vigilance. The primary failure is systemic.

47. How can the government improve Canadians' awareness about the risk of misuse of government-issued identifiers, including social insurance numbers?

Governments should provide clear guidance on how identifiers are misused, what Canadians should do if their information is compromised, and what protections exist across government and private-sector systems.

Awareness should include government impersonation, benefit redirection, account takeover, synthetic identity creation, and financial-account compromise.

However, awareness must be paired with stronger systems. If government-issued identifiers are used to access services or redirect payments, government and regulated institutions must strengthen verification, monitoring, and response.

Canadians should not be left to manage identifier misuse alone.

I. Support Law Enforcement’s Ability to Combat Fraud

48. What can be done to support federal law enforcement's ability to investigate fraud and collect fraud-related intelligence?

Federal law enforcement needs capacity, mandate clarity, coordination tools, and sustained funding.

Fraud is more complex, more digital, and more cross-border than the current response system was designed to handle. The government should increase dedicated fraud-investigation resources, expand specialized units, improve asset tracing and freezing powers, strengthen international cooperation, and ensure that intelligence gathered through the framework is operationally useful.

There is also a public-confidence issue. Victims need to see that fraud is treated as a serious crime. A strategy that generates more reports without increasing investigative capacity will deepen frustration.

Fraud against older Canadians should not be treated as a low priority because it is complex. Complexity is precisely why federal leadership is required.

49. What should be done to improve coordination between Canadian law enforcement across federal, provincial and territorial and municipal levels, and between those law enforcement bodies and international partners?

Canada should establish formal national coordination protocols for fraud enforcement. These should include lead-agency rules, common case-handling principles, shared intelligence standards, escalation thresholds, and regular public reporting.

Fraud does not fit neatly into jurisdictional boundaries. Victims, fraudsters, infrastructure, accounts, platforms, and money flows may all be in different places. The response should make that complexity less important, not more.

International coordination must be built into the action plan. Many scams targeting Canadians originate outside Canada or rely on foreign routing of funds, communications, or digital infrastructure. Canada should use bilateral and multilateral law enforcement channels to improve asset recovery, intelligence sharing, and prosecution.

50. What role should the CAFC play in advancing the Strategy?

The Canadian Anti-Fraud Centre should remain the national reporting and intelligence hub, but its role must be strengthened.

At present, many Canadians understand the CAFC as a place to report fraud, but not necessarily as a body that produces recovery, enforcement, or visible justice. That perception contributes to underreporting.

The CAFC should be better resourced, more closely integrated with regulators and law enforcement, and equipped to support real-time alerts, trend analysis, victim navigation, referral of serious matters, and national reporting.

A stronger CAFC should not replace law enforcement or regulatory accountability. It should connect them.

If governments expect Canadians to report fraud, reporting must lead somewhere meaningful.