

*National Anti-Fraud Strategy Consultation*

---

**Submission of the Public Interest Advocacy Centre (PIAC)**

**28 April 2026**



**PUBLIC INTEREST ADVOCACY CENTRE**  
**LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC**

---

**Written by: Tahira Dawood**  
**Acting General Counsel, PIAC**

## Table of Contents

A- Introduction and Summary .....	4
B- Scope of this Consultation, Gaps and Expected Outcomes.....	4
C- Responses to Questions – Oversight, Information Sharing and Reporting to Law Enforcement .....	6
Q1 Are the three described sectors appropriate for the initial phase of a Framework? Should other sectors be considered? .....	6
Q2 What role could a central regulator play in a Multi-Sector Anti-Fraud Framework? .....	6
Q3 What role could sector-specific regulators play in the Framework?.....	7
Q4 How can effective oversight of the Framework be achieved, without duplication of existing oversight of the three sectors? .....	7
Q5 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? 8	8
Q6 If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared? .....	8
Q7 What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?.....	8
Q8 When should Framework regulators be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting, and investigating fraud? 9	9
Q9 When should law enforcement be permitted to share fraud-related information with private sector organizations? .....	9
Q10 If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared? .....	9
Q11 What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?.....	9
D- Responses to Question – Aspects of a Framework (Prevention).....	10
Q15 What fraud-related information should organizations be required to make available to individuals using, or who may use, their services? .....	10
Q16 How should the effectiveness of organizations' fraud education be assessed to ensure it meaningfully reduces harm? .....	10
E- Responses to Question – Aspects of a Framework (Response).....	11
Q36 How should organizations be required to facilitate users' reporting of fraud activity to organizations?.....	11
Q37 How could organizations effectively investigate cross-sector complaints? .....	11
Q38 How long should organizations have to internally investigate complaints?.....	12
Q39 What information should organizations be required to include in a summary of complaint? .....	12
Q40 Should organizations be held liable when they do not fulfill their obligations under the Framework? .....	12

Q41	What standards should apply in determining whether an organization fulfilled its obligations?.....	12
Q42	How should liability be apportioned when multiple organizations have not fulfilled their obligations?.....	12
Q43	What should inform how an external complaint body is chosen? .....	13
Q44	Should decisions of the external complaint body be binding? .....	13
Q45	How long should the external complaints body have to investigate escalated complaints? 13	
F-	Responses to Question – Empower Canadians to act against fraud .....	14
Q46	How can the government improve Canadians' awareness of the threat posed by fraud and better position them to protect themselves against fraud?.....	14
Q47	How can the government improve Canadians' awareness about the risk of misuse of government-issued identifiers, including social insurance numbers?.....	14

## A- Introduction and Summary

- 1- The Public Interest Advocacy Centre (PIAC) is writing to provide its comments to the consultation regarding the National Anti-fraud strategy. PIAC is a national not-for-profit organization and registered charity that provides legal and research services on behalf of consumer interests, and, in particular, vulnerable consumer interests, concerning the provision of important public services.
- 2- PIAC comments on specific issues raised in this consultation. We are grateful for the opportunity to participate and share our comments. We would be keen to participate in any further process related to the development of this anti-fraud strategy.
- 3- PIAC's submission points to the underlying gaps that should be considered to have a more comprehensive national anti-fraud policy. PIAC also submits that the measures being presently considered do not go far enough in terms of raising consumer awareness, as well as protecting against fraud. Consumer losses and liability are key issues that should be a central part of any anti-fraud strategy.
- 4- Importantly, PIAC notes that we need practical steps planned and executed to make any changes work, just peripheral discussion on these issues does not and cannot do much. Consumers have been suffering from fraud, particularly vulnerable consumers, including seniors with limited to no redress at times. Consumers in these cases are often left with considerable liabilities and/or losses that could in some cases jeopardize their entire life savings. It is about time for some clear and concrete action.
- 5- PIAC appeared before the Senate, the Standing Committee, Banking, Commerce and the Economy (BANC Committee) to discuss its views and concerns regarding Bill C-15, Division 16 (*Bank Act*, Consumer-targeted Fraud). These are submitted along with these comments as **Appendix A**.

## B- Scope of this Consultation, Gaps and Expected Outcomes

- 6- The discussion paper for this consultation asks for feedback on three initial measures that are meant to advance the government's National Anti-Fraud Strategy (the Strategy), which is to provide anti-fraud solutions across the financial, and telecommunication sectors as well as digital platforms.<sup>1</sup> These three measures entail the following:
  - A Multi-Sector Anti-Fraud Framework to protect Canadians- new and enhanced market-conduct obligations for the federal financial sector, the telecommunications sector, and digital platforms.

---

<sup>1</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026) online: <<https://www.canada.ca/en/department-finance/programs/consultations/2026/national-anti-fraud-strategy-discussion-paper.html>>.

- Empower Canadians to act against fraud- help Canadians protect their information and accounts and make sure they know about their rights and how to report fraud.
  - Support law enforcement's ability to combat fraud-require organizations to report fraud, improve information sharing, and strengthen the Canadian Anti-Fraud Centre.<sup>2</sup>
- 7- PIAC welcomes this initiative to have a broader dialogue on consumer targeted fraud that continues to evolve and hurt Canadians.<sup>3</sup> The measures set out in this consultation indicate potential for improving how consumer fraud has been and could be dealt with in the three sectors identified in the paper. That said, at this stage it is not clear how many aspects of how these measures will be implemented and enforced.
- 8- PIAC is also concerned that the measures being considered do not go far enough in terms of raising consumer awareness, as well as protecting against fraud. Consumer losses and liability are key issues that should be a central part of any anti-fraud strategy. Unless this issue is specifically and directly addressed, the outcomes of this consultation and any other processes issued may not do much in terms of providing Canadians actual redress.
- 9- PIAC notes that empowering law enforcement on its own will not necessarily result in recoveries of all lost funds and/or consumers being reimbursed for these losses. What can regulators do in the three sectors under review to protect Canadians against liabilities is integral from a consumer perspective. The specific practices considered for these sectors can also be lessons for other sectors to protect Canadians against fraud.
- 10- Under the first measure, the underlying focus has been on improving and changing market conduct obligations in relation to how the federal financial, telecommunications and digital platforms handle consumer fraud. PIAC emphasizes that without clear legislative and regulatory obligations, any market conduct changes cannot be tracked, monitored and enforced, which could result in this whole exercise being of limited value, if at all. Enforcement, transparency and accountability are not just principles, these are critical tools to gauge whether and how any changes to tackle consumer fraud are working or not.
- 11- Further, in terms of next steps, the discussion paper notes that the Framework could require regulated organizations to fulfill a set of general obligations applicable regardless of industry sector, reinforced by separate industry-specific obligations pertaining to market conduct unique to certain sectors.<sup>4</sup> PIAC notes that the financial and telecommunications sectors have their own legal and regulatory regime. Thus, how changes discussed in this consultation would be transitioned need a serious consideration. The digital platforms do

---

<sup>2</sup> *Ibid.*

<sup>3</sup> CAFC, "Fraud Prevention Month 2026," online: <https://antifraudcentre-centreantifraude.ca/features-vedette/2026/02/month-prevention-mois-eng.htm>. See: In 2025, the Canadian Anti-Fraud Centre received over 112,000 fraud reports involving over \$704 million in reported losses.

<sup>4</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026)

not have legal obligations in relation to consumer targeted fraud,<sup>5</sup> with some attempts made at regulating these platforms in relation to online harms<sup>6</sup> but these have so far not materialized. Thus, again how would digital platforms be held to comply and account for any fraud prevention, detection and disruption should be questioned in this consultation with a clear action plan put in place.

12- We need practical steps planned and executed to make any changes work, just peripheral discussion on these issues does not and cannot do much. Consumers have been suffering from fraud, particularly vulnerable consumers, including seniors with limited to no redress at times. Consumers in these cases are often left with considerable liabilities and/or losses that could in some cases jeopardize their entire life savings.<sup>7</sup> It is about time for some clear and concrete action.

### **C- Responses to Questions – Oversight, Information Sharing and Reporting to Law Enforcement**

#### **Q1 Are the three described sectors appropriate for the initial phase of a Framework? Should other sectors be considered?**

13- The three described sectors are critical federal sectors. It is important to cover them in the initial phase of a Framework. However, scams are not just limited to these sectors. The overall determination on this should be based on findings regarding how fraud manifests across different sectors in Canada, and where and how consumers are actually subject to scams, and need protection. Some examples of other sectors are provincial credit unions, and online marketplaces.<sup>8</sup> It is crucial to have a broader understanding from the start of all other sectors that have victims of fraud to have a well-informed strategy, including how these platforms can prevent and identify fraud, even if the focus is on the three federal sectors to begin with.

#### **Q2 What role could a central regulator play in a Multi-Sector Anti-Fraud Framework?**

14- The discussion paper does not suggest who would be the central regulator responsible for monitoring and enforcing compliance and how would it do so. Though, reference is made to the sector-specific rules that could be overseen and enforced by industry regulators with

---

<sup>5</sup> *Ibid.*

<sup>6</sup> Proposed Bill to address Online Harms, online: <<https://www.canada.ca/en/canadian-heritage/services/online-harms.html>>.

<sup>7</sup> Erica Johnson, and Ana Komnenic, “RBC and CIBC allow 89-year-old to drain life savings, lose \$1.7M to scammers,” *CBC Go Public* (27 October 2025), online: <<https://www.cbc.ca/news/gopublic/bank-investigator-fraud-scam-9.6950754>>.

<sup>8</sup> William Eltherington, “Buyer beware: Cybersecurity expert warns about Amazon Prime Day scams,” *CTV News* (9 October 2024), online: <<https://www.ctvnews.ca/ottawa/article/buyer-beware-cybersecurity-expert-warns-about-amazon-prime-day-scams/>>.

knowledge and expertise of their sectors.<sup>9</sup> PIAC agrees that sector specific rules could be enforced by relevant regulators already in place in different sectors.

15- However, the underlying issue is who is this central regulator, what role could they play and on what basis. Our research indicates that there are different organizations at the federal level seeking to combat fraud within a specific scope. We note a few names, such as the Canadian Anti-Fraud Centre, Royal Canadian Mounted Police (RCMP), the Canadian Radio-television and Telecommunications Commission (in relation to telecommunications matters), and the Financial Crimes Agency.<sup>10</sup> This is not an exhaustive list, rather it suggests that different organizations at the federal level review, and handle consumer fraud in different ways.

16- If one central regulator is going to be responsible for overseeing this framework, they need to be given the necessary legislative authority to do so. Another important consideration is how would this regulator's authority and work overlap with those of other federal departments and/or provincial departments (if and when applicable).

17- As of now, how consumer fraud is reviewed and combated at the federal and even provincial or territorial levels remains confusing for an average consumer to follow. This strategy should clarify who will be this central regulator, with priorities, roles and responsibilities of relevant stakeholders clarified to ensure this new regime is efficient and effective.

**Q3 What role could sector-specific regulators play in the Framework?**

**Q4 How can effective oversight of the Framework be achieved, without duplication of existing oversight of the three sectors?**

18- The role played by each sector-specific regulator would depend on the specific obligations that result from this strategy. Sector specific regulators are crucial because they have the expertise, as well as authority to impose and monitor compliance in their sectors. PIAC briefly notes few comments:

- Firstly, depending on the new requirements, it is possible that these regulators may need more clear and/or specific authority under the new framework. PIAC strictly advises against relying on voluntary compliance from the industry, and suggests that necessary mandate, and powers should be granted to these regulators.
- Secondly, a clear workable system should be put in place with clarity as to who is responsible for monitoring what obligations and how. This should be created in

---

<sup>9</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026).

<sup>10</sup> Department of Finance Canada, "Minister Champagne takes aim at financial scams and abuse, announces Anti-Fraud Strategy and new Financial Crimes Agency," online: <<https://www.canada.ca/en/department-finance/news/2025/10/minister-champagne-takes-aim-at-financial-scams-and-abuse-announces-anti-fraud-strategy-and-new-financial-crimes-agency.html>>.

collaboration with the central regulator and all sector specific as well as any other relevant regulators.

- A key part of this system is also how will public reporting happen, as well as how consumers will be informed, and provided a clear mechanism to reach out, share inquiries and/or complaints. Doing this on a sector-specific level might be more manageable but how such results and findings are shared and managed nationally needs to be carefully considered.

**Q5 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?**

**Q6 If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?**

**Q7 What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?**

19- The discussion paper notes that “[a]ccess to timely information can position regulators to better understand the evolving nature of fraud and inform anti-fraud oversight of their respective industries and public-facing anti-fraud messaging.”<sup>11</sup> PIAC agrees to the extent that timely sharing of important information across sectors can be helpful in mitigating risks by enabling a better understanding of identifying and preventing fraud. This will be particularly useful if information is shared while the fraud is still transpiring and/or strongly suspected to transpire.

20- That said, all such cases will inevitably include victims’ information, particularly, their sensitive data and information, including their phone numbers, banking information and/or other details, which must be strictly reviewed and guarded. Data de-identification and anonymization can be complicated<sup>12</sup> and has its own risks and concerns. Thus, PIAC suggests working with the Office of Privacy Commissioner of Canada as well as all relevant provincial and territorial bodies to have a system that is in compliance with all the privacy laws and regulations. The privacy regulators should be a regular part of this process, and not just consulted at this initial stage.

21- PIAC suggests that insight should also be drawn from how authorities in other jurisdictions share information that is aimed at preventing, detecting and investigating scams. For instance, the UK’s Information Commissioner’s Office notes the following regarding its regulatory approach:

---

<sup>11</sup> Department of Finance Canada, “National Anti-Fraud Strategy Discussion Paper,” (2026).

<sup>12</sup> Office of Privacy Commissioner of Canada, “Reducing identifiability in cross-national perspective: Statutory and policy definitions for anonymization, pseudonymization, and de-identification in G7 jurisdictions,” (11 October 2024), online: <[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/de-id\\_20241011/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/de-id_20241011/)>.

The ICO's regulatory approach seeks to create an environment in which people are protected, while ensuring that organisations which process personal information can operate and innovate efficiently. This involves us providing regulatory certainty about what the law requires, reducing the cost of compliance and improving standards.

It is also important for us to clarify how we plan to exercise our powers. We take fair, proportionate and timely regulatory action to protect people's information rights. When considering whether a regulatory response is necessary, we will take into account any steps you have taken in good faith to share personal information in line with the law to protect people from harm.

While every case is different, we will always use our powers in a robust, targeted and proportionate manner, ensuring that organisations are not worried that we may impose disproportionate sanctions.<sup>13</sup>

**Q8 When should Framework regulators be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting, and investigating fraud?**

**Q9 When should law enforcement be permitted to share fraud-related information with private sector organizations?**

**Q10 If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?**

**Q11 What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?**

22- PIAC again emphasizes that when it comes to sharing fraud-related information with law enforcement, there should be clear and secure safeguards to particularly protect victims' personal information. The consultation paper broadly states that information-sharing authorities would need to be narrowly and precisely defined to ensure that safeguards under the Charter and privacy rights are respected at all times,<sup>14</sup> but it does not state how.

23- If law enforcement agencies are permitted to share fraud-related information with private sector organizations, there should also be a comprehensive vetting process to ensure there are no false positives. This means that records of persons and/or organizations suspected of fraud are based on thorough data and no innocent consumers are wrongly embroiled in such databases and/or records.

24- The type of information that would need to be shared with law enforcement and/or private sector may vary from one case to another. It would be useful to have clear and strict policies and processes regarding when, how and the scope of information to be shared. Some cases involving coordinated and/or sophisticated fraud might require a more

---

<sup>13</sup> Information Commissioner's Office, "Sharing personal information when preventing, detecting and investigating scams and frauds," online: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-information-when-preventing-detecting-and-investigating-scams-and-frauds/>>.

<sup>14</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026).

detailed disclosure than other cases. The precise criteria should be informed by actual fraud cases, and updated, as necessary.

25- All law enforcement as well as private organizations should be given the requisite personnel training and be informed about the relevant privacy laws and requirements. It is critical that information sharing is strictly and clearly limited to preventing, identifying and disrupting fraud, with processes put in place to oversee this and to prevent any misuse of such data and/or information.

#### **D- Responses to Question – Aspects of a Framework (Prevention)**

**Q15 What fraud-related information should organizations be required to make available to individuals using, or who may use, their services?**

**Q16 How should the effectiveness of organizations' fraud education be assessed to ensure it meaningfully reduces harm?**

26- All relevant organizations should be required to provide individuals using their services and/or who may use their services clear information in simple and plain language regarding any past cases of fraud that the organization has faced. Organizations should also provide prominent details on any known fraud patterns and trends (such as spoofing, phishing, social engineering,<sup>15</sup> and disconnection scams<sup>16</sup> to name a few).

27- The information shared with consumers should also include any known signs and/or red flags that they should be wary of as well as indicate steps that consumers should consider taking to ensure that they are not being subject to a scam.

28- PIAC would like to clarify that the onus in these situations to prevent, detect and/or disrupt a fraud should be on the pertinent organization, not on the individuals. This means that the private sector organizations should take all reasonable steps to ensure that fraud is prevented, detected and/or disrupted, and not merely rely on the individual to exercise caution. Placing this burden on vulnerable consumers who often have limited knowledge and resources to manage these situations is unfair, which must be addressed in the resulting strategy.

29- Consumers should also be provided clear information regarding any recourse, redress and/or reimbursement options available to them in these situations.

30- In terms of assessing the effectiveness of organizations' fraud education, this should be based on feedback from consumers as well as detailed reporting. The reporting should be

---

<sup>15</sup> Office of the Privacy Commissioner of Canada (OPC), Deceptive and manipulative: social engineering techniques, online: <[https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/gd\\_se/](https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/gd_se/)>.

<sup>16</sup> Enbridge Gas, Scam Awareness, "Don't fall for scammers pretending to be Enbridge Gas," online: <<https://www.enbridgegas.com/ontario/contact-us/scam-awareness>>.

based on how organizations' practices have increased users' understanding of exposure to fraud as well as a review of how their materials made consumers' rethink their actions and plans to better identify and prevent falling for a scam.

## **E- Responses to Question – Aspects of a Framework (Response)**

### **Q36 How should organizations be required to facilitate users' reporting of fraud activity to organizations?**

31- PIAC agrees with the recommendations presented in the discussion paper concerning organizations having dedicated and distinct reporting channels to allow customers to report alleged incidents of fraud.<sup>17</sup> Importantly, this whole process should be simple, and must allow for prompt intake of comments and/or concerns. Consumers should not have to face long wait times to reach the organization. There should also be multiple channels to report fraud activity, with reporting facilitated and permitted in different formats to enable consumers with special needs to also reasonably access and use these services. The organizations should also be required to inform all their customers of these reporting channels and/or services, rather than consumers required to inquire about them.

32- Many consumers who might be reporting fraudulent activity might feel vulnerable and/or overwhelmed, it is extremely important that all organizations train their staff on how to interact with customers as well as know and implement certain safeguards on an immediate basis, as required. These safeguards and what consumers should expect should also be communicated clearly and promptly to consumers.

33- The form of safeguards required would likely vary depending on the sector involved as well as the risk and type of fraud involved. For example, if a user calls a telecommunications service provider to report SIM-swap fraud, the protocol would be to do due-diligence and prevent the number porting, while in the case of an unauthorized e-transfer, the protocol would be to block the e-transfer.

### **Q37 How could organizations effectively investigate cross-sector complaints?**

34- Organizations could effectively investigate cross-sector complaints through a coordinated system, which should be provided in this strategy. More specifically, these investigations could be based on a process within the system to check whether and how does a complaint affect other sectors, with each complaint checked against this system to review and check for any overlaps. Such a system should also strictly consider privacy implications as well as what information can be placed in and what factors indicate cross-sector overlap. Some cases, such as the SIM-swap fraud might make this overlap more apparent because of the connection of a cellphone number to access different websites,

---

<sup>17</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026).

services and apps, including email and/or banking accounts. It should also be considered how the central regulator assist and/or at least oversee such cross-sector complaints.

**Q38 How long should organizations have to internally investigate complaints?**

35- The discussion paper notes that the victims of fraud should have access to clear dispute resolution system, and that each organization could be required to have a public-facing dispute resolution procedures.<sup>18</sup> PIAC concurs with this suggestion, and agrees that it can be beneficial to have a single-point of entry for cross-sector complaints<sup>19</sup> to ease the dispute resolution process for consumers.

36- We believe a reasonable period of time for internally investigating complaints should not be more than 15 days. Generally, fraud related transactions require urgent attention and necessary steps to prevent any or further losses need to be taken immediately. Thus, those urgent measures should be implemented on an immediate basis. The 15 days recommendation is for organizations to internally investigate complaints and/or reimburse customers if applicable, including cases where customers do not agree with the conclusion and approach of the service provider. When it comes to matters like reimbursement, PIAC recommends that practices in other jurisdictions should be reviewed.<sup>20</sup>

**Q39 What information should organizations be required to include in a summary of complaint?**

37- The summary of a complaint from an organization should include key facts, any fiscal amounts involved, service providers' review, process, and determination, timelines involved and consumers' concerns. If a specific complaint is a cross-sector complaint, the summary should indicate that as well as briefly explain how this complaint relates to the different sectors. Additionally, all relevant evidence and information should be available for consumers and the central regulator to be able to access, and review.

**Q40 Should organizations be held liable when they do not fulfill their obligations under the Framework?**

**Q41 What standards should apply in determining whether an organization fulfilled its obligations?**

**Q42 How should liability be apportioned when multiple organizations have not fulfilled their obligations?**

---

<sup>18</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026).

<sup>19</sup> *Ibid.*

<sup>20</sup> Payment Systems Regulator, APP fraud reimbursement protections, online:

<<https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/>>.

38- PIAC briefly comments that yes, organizations should be held liable for not fulfilling their obligations under the Framework. This is a key consumer protection measure because in instances when the pertinent service providers' fail to conduct due diligence in preventing, identifying and/or disrupting fraud as per this strategy and other processes that follow this strategy, consumers could be facing significant losses with hardly any or limited recourse. The burden to prevent and identify fraud should be on organizations, not consumers.

39- PIAC agrees with the following proposal in the discussion paper:

In the event an organization's investigation of a complaint determines that it did not fulfill its Framework obligations, and that an individual suffered financial harm as a result, organizations could be required to make the individual whole, either solely by a single organization or, in the case where multiple organizations have not met their obligations, the individual could be made whole through an arrangement between organizations that apportions blame proportionate to the fault of the implicated organizations (for example, a text from a known fraudster leads to an individual making an electronic funds transfer payment to the fraudster).<sup>21</sup> [Emphasis added]

**Q43 What should inform how an external complaint body is chosen?**

**Q44 Should decisions of the external complaint body be binding?**

**Q45 How long should the external complaints body have to investigate escalated complaints?**

40- The telecommunications and the financial sector each already have an ombudsman in place to oversee complaints. The federal government can consider whether and how these existing complaint handling bodies or their existing processes can be used to form a single external complaint body to handle fraud related issues, provided that this body is given the requisite legal authority, clear mandate and resources to work with. Any such body must remain independent, and impartial. The governance, operation and membership of this body must be independent from the affected industries.

41- All decisions of the external complaint body should be binding on regulated organizations. Otherwise, there is a clear risk that industry representatives may not comply with the recommendations and/or the decision(s) made by this body. Alternately, the private organizations might settle for amounts that are much lower than those recommended by this body, as has been the case with non-binding OBSI determinations.<sup>22</sup>

42- PIAC considers 30-45 days to be a reasonable time limit to start with for this body to review these fraud related complaints. Considering that fraud related matters are often time-sensitive and can involve fiscal amounts, a longer time limit than 30-45 days can have serious financial and other implications on consumers. Meanwhile, a shorter period of time could be hard for a new external complaint body to manage. That said, after this external

---

<sup>21</sup> Department of Finance Canada, "National Anti-Fraud Strategy Discussion Paper," (2026).

<sup>22</sup> Staff, "The High Costs of Low-Ball Offers," Consumers Council of Canada News (29 April 2025), online: <https://consumerscouncil.com/the-high-costs-of-low-ball-offers/>

complaint body is well-settled in the new system, a shorter period should be considered for reviewing and processing these complaints.

## **F- Responses to Question – Empower Canadians to act against fraud**

**Q46 How can the government improve Canadians' awareness of the threat posed by fraud and better position them to protect themselves against fraud?**

**Q47 How can the government improve Canadians' awareness about the risk of misuse of government-issued identifiers, including social insurance numbers?**

43- The government's fraud awareness campaign has to be national, targeted, uniform and beyond just one month, it has to happen at regular and frequent intervals. Importantly, the responsibility for raising consumer awareness should be shared by the different private organizations in the sectors covered by this strategy. These organizations have closer interactions with consumers, and can play a considerable role in raising awareness.

44- These campaigns should be more than just mere warnings, they should explain how fraud manifests, what are important red flags to watch out for, what are the next steps, remedies and recourse options available to victims of fraud.

45- The government-issued identifiers, including social insurance numbers are critical pieces of information that require specific attention and a more stringent approach, not just in terms of telling Canadians not to share this information but also in terms of restricting how others collect this information. A high and clear threshold should be identified and well-publicized for the purposes of collecting this information, which should be strictly limited to essential cases.

\*\*\*End of Document\*\*\*