Prosper Canada

SUBMISSION TO FINANCE CANADA
Re: Consumer-targeted Fraud Regulations
December 22, 2025

Introduction

Established in 1986, Prosper Canada is a national charity driving bold change that enables more people to prosper. With government, business and community partners across Canada, we expand life-changing financial empowerment services, innovate for greater inclusion and impact, and remove barriers to financial well-being for people with low and modest incomes. Our goal is a Canada where everyone has the opportunity and support they need to achieve financial well-being and live with dignity, stability, and possibility.

The views expressed below are rooted in evidence and insights we have acquired through research and ongoing dialogue with consumer protection stakeholders and our community partners across Canada who work firsthand with low-income and vulnerable financial consumers to help them to build their financial capability, stability, and well-being. This includes empowering them to protect themselves from financial predation, fraud and scams that often target low-income communities, Indigenous communities, newcomers, seniors, and people living with disabilities.

In developing our recommendations, we considered the following factors, using the information and evidence available to us:

- Evidence on the relative fraud risk of different account capabilities.
- Evidence on the efficacy of proposed measures in reducing fraud.
- Evidence on their relative efficacy compared with alternative measures.
- The operational implications of proposed measures and their potential to increase consumer banking fees, costs and/or inconvenience.
- Alignment with established effective practices in consumer transparency, protection and empowerment.

We appreciate the opportunity to comment on the proposed regulations and would be happy to answer any questions.

Response to consultation questions

1. (a) Which account capabilities should require consumers' express consent to enable?

Recommendations

We recommend that banks and federally regulated credit unions be required to obtain express consent to enable wire transfers and global money transfers.

We recommend that banks and federally regulated credit unions continue to be required to obtain express consent for overdraft protection.

We do not recommend requiring express consent to enable other account features at this time, but suggest they be reviewed again as options in the future once there is more implementation experience to draw on.

Rationale

Because overdraft protection is a credit product, express consumer consent should always be required before activating this account feature. However, because express consent is already required in Canada, there is no need to make this a new requirement.

Wire transfers and global money transfers are the preferred payment option of fraudsters because they are typically used for high-value transactions. In 2023, the Canadian Anti-Fraud Centre reported that bank wire transfers were the top payment method in terms of dollar loss, often involving amounts over $10,000.

Once complete, the transfer of funds through these mechanisms is generally considered final and irrevocable. Criminals frequently use wire transfers to send stolen funds to foreign countries quickly, making recovery extremely difficult and impossible in many cases.

Most consumer deposit account holders do not make use of these functions on a regular basis, so requiring consent to activate is not an inconvenience for the majority. According to a 2024 Payments Canada study, only 20% of individuals sent money internationally using their bank account within a 12-month period. Among these, consumers were most likely to send money internationally using EFTs via their mobile banking app or online banking account (31%) and PayPal Transfer (30%). Wire transfers were used by 11%.

We, therefore, believe there is a strong case for requiring banks and federally regulated credit unions to seek express consent to activate wire transfer and global money transfer account features on the basis that fraudsters are most likely to use them to steal large sums of money, transferred funds are largely unrecoverable, and most consumers do not need or use these account capabilities. Multi-factor authentication is generally seen as the best way to ensure that "express consent" is genuinely coming from the authorized account holder.

Banks will need to make infrastructure investments and maintain chain of consent records for audit purposes if this approach is implemented. This could potentially drive-up fees for account holders. If effective in reducing risk of fraud and fraud losses, however, resulting bank savings could potentially offset the operational expense of enabling this protection, reducing the likelihood of flow-through costs to consumers. Monitoring over time will give a clearer picture of the impact.

It is possible that banks will experiment with defaulting additional account features to 'inactive without express consent' or be mandated to do so in other jurisdictions as part of their anti-fraud efforts. These experiences should be monitored to provide valuable insights into the cost effectiveness of extending this approach to additional account features. Once more implementation experience is available, Finance Canada should review the desirability of defaulting other account features to 'inactive without express consent.'

(b) Which account features should consumers be permitted to disable?

Recommendations

We recommend that consumers be permitted to disable wire transfers and global money transfers as a high priority because, (as noted above) these are the top methods used by fraudsters in terms of dollar loss and are typically final and irrevocable once processed, making fund recovery difficult.

Consideration should also be given to enabling consumers to disable online bill payments and other Electronic Funds Transfers (EFTs) as a medium priority. In the event of unauthorized access to their accounts, this has the potential to protect a sub-set of seniors and other individuals who prefer not to bank online or pay bills online, as long as multi-factor authentication is required to reactivate these features. Any attempt to reactivate a disabled feature should also trigger an alert to the consumer holding the account.

Rationale

Determining which bank account features Canadian consumers should have the option to disable involves a trade-off between security, user convenience, and the inherent risk profile of each transaction type. The primary considerations include:

- **Fraud severity and irreversibility**: Features involving large sums of money and irreversible transactions pose the highest risk.

- **Transaction value and frequency**: Features used for large-value or less frequent transactions (like wire transfers) are less likely to disrupt daily life if disabled and provide a substantial security gain when enabled only for specific, verified use. Features used for frequent, everyday, low-value transactions (like near-field communication transactions or routine EFTs) offer high convenience. Disabling them would likely be a major inconvenience for daily commerce, so a simple on/off switch might be less practical than other controls like daily limits or mandatory PIN for certain amounts.

- **Alternative security measures**: The availability and effectiveness of existing security measures, such as multi-factor authentication (MFA), real-time transaction monitoring, and consumer liability policies, should also be considered. The goal of offering the *option* to disable is to allow the consumer an extra layer of control beyond the bank's default protections. This empowers consumers to manage their own risk tolerance.

- **Consumer control and transparency**: Canada's Financial Consumer Protection Framework emphasizes providing clear information and obtaining express consent for products and services. Offering the ability to disable features aligns with empowering consumers to manage their banking experience securely. However, banks should clearly communicate the risks, benefits, and how to enable/disable these features easily.

Ultimately, features that combine high potential loss with high irreversibility and low frequency of use should be prioritized for a user-controlled disable option. On this basis, wire transfers and global money transfers are a high priority for a 'disable' option due to high fraud loss and transaction finality.

Online bill payments and other EFTs should be a medium priority for a 'disable' option. While EFTs are generally lower risk within Canada on a per-transaction basis and may have more consumer protections or recourse, high-value or unusual patterns can still indicate fraud. A 'disable' option might be useful for highly risk-averse consumers and particularly useful for those who prefer not to bank or pay bills online at all.

A significant segment of seniors does not bank online and could benefit from the added protection of being able to disable EFTs to guard against theft in the event of unauthorized access to their accounts. According to Statistics Canada, in 2022, 14% of adults aged 65 and older were without Internet access. Even older adults who used the Internet were still less likely to adopt online banking than younger Canadians with just 76% of Internet users aged 65 to 74 banking online, while the remaining 24% either opted for more traditional banking methods (e.g., in-branch, phone or ATM) or had no chequing or savings accounts.

Near-field communication transactions are not a priority for a 'disable' option but should be a high priority for other security controls – e.g., spending limits, PIN requirements, due to their use in frequent, low-value daily commerce.

Implementing consumer option to disable certain account functions

Banks should give account holders the ability to easily disable and reactivate specific account features through online banking portals, mobile apps, and by contacting the bank directly. Consumers should be able to select the communication channel that is most convenient and works best for them.

Consumers should also be allowed to adjust their maximum transaction amounts when they wish via the same range of channels to protect themselves from potential fraud losses.

Banks should also establish internal policies and procedures to effectively manage these new consumer options and provide a clear chain of consent for audit purposes.

It's also recommended that banks adopt user experience guidelines to ensure that all aspects of consent and revocation are clear, simple, and consistent across all platforms, consistent with the new framework for consumer-driven banking.

2. How should banks be required to obtain 'express consent' for the purpose of enabling certain capabilities of consumers' personal deposit accounts?

Recommendations

Banks should obtain express consent through a clear, simple, succinct and not misleading communication explicitly stating that they are seeking consent to activate a specific account functionality.

This communication should also include clear, simple and succinct and not misleading information outlining:

- The risks and benefits of activating the function in question.
- That the consumer can reduce risk of fraud by not activating any functionality they don't think they need.
- Who is liable for losses incurred in the event:
    - of unauthorized account access and use of this functionality by someone other than the account holder.
    - the account holder is subjected to fraud and uses the functionality themselves to transfer funds to the fraudulent party.
- How consumers can revoke or activate consent in the future should they wish to.

Consumers should be invited to provide permission verbally or in writing (including electronically) via the communication channel of their choice (e.g., mobile app, website, in person, telephone).

Consent, once given, should be subsequently confirmed to the account holder in writing (electronically or on paper) so they have their own permanent record.

Obtaining consent to activate high-risk functions like wire and global money transfers should always include a multi-step verification process, such as out-of-band verification (e.g., a code sent via SMS to a verified phone number) to ensure the consenter is the actual account holder.

High-risk functions, like wire and global money transfers, should also require a multi-step authorization process for each specific transaction to prevent fraud:

- A written (including electronic) agreement should be in place before the first transfer request is made. This agreement should outline who is authorized to initiate transfers, their contact information, and the security procedures the bank will use to authenticate requests.
- Access to banking systems used to initiate transfers should be protected with strong passwords and multi-factor authorization.
- There should be a multi-step verification process for the transaction details. This could involve a direct call back to a predetermined, trusted phone number that is previously on file (not a new/ different one provided in the transfer request).
- For electronic instructions, a one-time numerical code sent via text message to the customer's phone of record can be used as an out-of-band verification.

For each transfer, the customer should provide explicit authorization including:

- Customer name and account number.

- Beneficiary's full name, address, bank name, and account details (e.g., IBAN, SWIFT code).
- Transaction details: amount, currency, and date of transfer.
- Acknowledgment of associated fees/exchange rates
- A disclaimer regarding cancellation limitations.

Rationale

Clear, simple, and succinct communication that is not misleading is critical to the ability of consumers to make informed choices that further their best interests. Lengthy, dense disclosures written in legalistic language do not meet this standard. Core information should be transmissible in language that is comprehensible to anyone with a Grade 6 level of literacy.

Consumers need to be informed of the risks and benefits of activating the account functionality in question as this information is needed to make an informed choice and most consumers will not be fully aware of the fraud risks associated with specific functionalities.

Advising consumers that they can reduce their fraud risk by not activating account functionalities they do not, or are unlikely to, use will help consumers to make prudent choices in their best interest.

It is critical to provide clear information on who is liable for account losses associated with the functionality in question, in the event of unauthorized account access or transfers made by the account holder because of a fraud or scam. Without this, the consumer is not able to fully assess risk or making a fully informed choice about the functionality in question.

Because people’s circumstances, risk tolerance, and financial product needs change, consumers need to know how they can quicky and easily revoke or activate their consent at any future date of their choosing.

A consent process that offers comparable user experience across all communication channels ensures that banks are not inadvertently creating accessibility barriers for customers – e.g. people living with disabilities, customers lacking digital access and/or skills, customers with distance or mobility challenges, etc. Instead, they are enabling every customer to communicate in the way they find most manageable and convenient.

The use of out-of-band or multi-factor authentication to verify that the consenter is the true account holder is a critical step that protects account holders in the event someone has gained unauthorized access to their account and seeks to activate high-risk functionalities for the purposes of committing theft or fraud.

In the event of a fraud or loss of funds in connection with the functionality in question, it is critical that the account holder, as well as the bank, have a clear written record (paper or digitally) of any consents provided or revoked in connection with that functionality.

For high-risk transactions like wire and global money transfers, explicit consent must extend beyond function activation to each specific transaction to prevent fraud. Payment channels of choice for fraudulent actors need additional layers of verification to adequately protect consumers, particularly when, in this case, functions are generally used for large amounts and payments are largely irrevocable.

3. Are there other limits beside those in the proposed sub-section 627.132(1), that consumers should be able to adjust?

Recommendations

The proposed limits are a great place to start, particularly limiting the maximum withdrawal level and number of withdrawals in a given period as this enables consumers to limit potential losses arising from unauthorized account access.

For these to be effective any attempt to change these limits should trigger multi-factor authentication to confirm that the request is coming from the actual account holder.

Additional limits that consumers could benefit from the ability to adjust include:

- **Geographic transaction limits:** The ability to restrict where transactions can occur (e.g., within Canada only, or specific provinces) can help prevent international or inter-provincial fraud if a customer knows they will not be traveling.

- **Transaction type limits:** Customers could set limits for specific transaction types, such as setting a low or zero limit for in-person point-of-sale purchases by debit card if they primarily use a credit card for these.

- **Specific merchant/category limits:** The ability to block transactions from certain merchant categories (e.g., online gambling, adult entertainment) can help prevent fraud in specific areas of concern.

- **Time-of-day limits:** Restricting the time of day when transactions can be executed (e.g., no transactions between 12:00 AM and 6:00 AM) could help prevent fraudulent activity that often occurs overnight.

- **Per-transaction limits for specific payment methods:** While maximum withdrawal/transfer amounts are proposed, specific limits per payment method (e.g., e-transfer limits different from direct debit limits) could offer more granular control.

- **Alert thresholds for specific activities:** While balance alerts are currently required when an account drops below $100 (or a customer-set value), allowing consumers to set alerts for other unusual activities (e.g., a transaction occurring in a new location, first-time transaction with a new merchant, any transaction over a custom amount) provides proactive fraud detection.

- **Temporary lock/freeze function:** The ability to instantly lock or freeze specific functions of an account (e.g., freeze online international transactions while keeping domestic ones active) via a mobile app, online banking, or telephone, would allow for immediate self-protection in case of a suspected breach.

Implementation should be phased in over time while monitoring impact, as the potential impact, and operational effort and investment to implement, will vary for different measures. This will help to ensure a smooth, manageable, and effective roll-out for financial institutions and consumers alike.

First priority should be given to controls that can be easily implemented at little expense, and those that offer the highest potential to reduce fraud risk and/or limit dollar losses, even if more costly to implement.

Rationale

These controls would empower consumers to tailor their account security to their specific lifestyle and risk tolerance, reducing potential losses in the event of their account details being compromised.

In peer jurisdictions like the UK, Australia, and the US, some banks have been voluntarily introducing some of these controls – in particular allowing consumers to block payments to certain categories of merchants and to freeze and unfreeze cards. These features don't appear to be offered by Canadian banks.

We're unable to assess the operational investment required to enable these additional consumer controls, but this would need to be weighed against the potential reduction in fraud risk/losses in each case to determine whether the control in question is cost-effective and should be implemented and what priority to assign to it. Assessing relevant experiences of banks in other jurisdictions can help to capture important insights and evidence to inform this analysis.

4. Should the minimum period for banks to implement a limit change set by the consumer be set at 12 hours and the maximum period to 48 hours? If not, what should the period be?

Recommendations (with rationale)

We recommend setting the minimum period to implement a limit change at 24 hours to increase the likelihood of the consumer reflecting and/or seeking advice if they are being pressured by someone intent on defrauding them. This also provides more time for the financial institution to intervene during business hours to question suspect transactions.

Some clients may have legitimate emergencies requiring faster access to increased limits. To accommodate this, without weakening fraud-prevention safeguards, financial institutions could be allowed to accelerate the change after verifying the client's identity and confirming the legitimacy of the request through enhanced authentication. This authentication process, however, must take into account that one of the most common frauds is the use of artificial intelligence to mimic family members in distress requesting immediate international financial transfers – e.g. for bail, ransoms, etc. Banks need to establish a robust way to differentiate true emergencies from these types of frauds, if making exceptions to the 24-hour minimum limit.

We agree with the maximum period being set at 48 hours, as long as financial institutions retain the right to extend this if they detect likelihood of fraud and opt to investigate. This is critical if banks are to be able to take timely action to protect consumers and their own institutions against fraud losses.

5. Are there additional criteria beyond those outlined in the proposed sub-section 627.134(2) that banks should have in their policies and procedures?

Recommendations

We recommend adding the following considerations for inclusion in bank policies and procedures governing the detection, prevention and mitigation of consumer-targeted fraud:

- The timeframe within which a decision to suspend or cancel a transaction must be communicated to the consumer.

- The basis on which, and process by which, a consumer may challenge and the bank reconsider a decision to suspend or cancel a transaction.

- The timeframes within which a challenge may be raised, reconsideration will take place, and the consumer must receive a decision with respect to their challenge. This should provide a prioritized fast-track option for cases where real financial harm is a potential outcome and time is of the essence.

- To reduce risk of financial harm from interrupting legitimate transactions, banks should educate consumers on types of transactions they should alert their bank to beforehand to prevent delays and ensure their transactions are processed smoothly.

Rationale

Banks frequently rely on algorithms to identify potentially fraudulent transactions and take action accordingly, but algorithms are not foolproof. When an algorithm mistakenly identifies a transaction as fraudulent and it is refused, this can be disruptive to the consumer and even cause real financial harm in some cases – e.g., causing consumers to miss important payment deadlines or to default on contractual obligations.

Consumers should be given the opportunity to challenge such decisions and to achieve speedy resolution when their bank is mistaken. Providing clear guidance on appropriate grounds for a challenge, when and how a challenge may be raised, and a timeframe in which a consumer can expect a response to their challenge, will help to ensure a transparent, efficient, and timely recourse process.

Banks can empower consumers to prevent delays in processing important transactions by letting them know what types of transactions are typically subject to verification delays and encouraging them to inform their bank beforehand when they are planning an important transaction that could be at risk, so that it can be pre-verified by their bank.

6. What data should banks be required to include in the annual fraud report to the Commissioner?

Recommendations (with rationale)

We recommend that banks be required to report on both incidence of fraud and incidence of attempted fraud as a means of assessing their success rate in thwarting fraud attempts. Significant differences between banks can potentially highlight weaknesses in the approaches that should be addressed, and/or highly effective fraud-prevention approaches that should be shared and adopted more broadly.

We recommend that the value of fraudulent transactions be reported, as this data can be used to prioritize the most harmful types of fraud – to consumers and to banks – and to orient prevention efforts accordingly.

7. Should data reporting be segmented by fraud authorization type (e.g., coerced transactions vs. unauthorized transactions)? If yes, how?

Recommendations

We support differentiated reporting of unauthorized consumer-targeted fraud events and fraud resulting from transactions authorized by a consumer. Effective prevention may require very different approaches in each of these cases, so it is important to understand the relative incidence of each type and to tailor and target prevention strategies accordingly.

In our view, coerced transactions should not be classified as authorized by the consumer, as consent provided under conditions of fear or intimidation is involuntary and, therefore, not true consent.

FCAC should work with banks and law enforcement stakeholders to develop a differentiated taxonomy for fraud complaints, and an accompanying coding system that banks can use to enable more detailed analysis of fraud data and evidence-informed prevention and law enforcement efforts.

Rationale

When customers report fraudulent transactions, bank investigation teams typically classify these based on the method used by the fraudster and the level of customer involvement:

- **Unauthorized transactions:** These are transactions that the consumer did not make or approve. In cases of coercion (e.g., the customer was forced to provide a PIN or approve a payment), the customer is not considered to have "voluntarily" authorized the transaction. Banks are required to investigate all relevant factors, including whether circumstances were beyond the cardholder's control, and must not automatically hold the customer liable just because an authentication method (like a correct PIN) was used.

- **Authorized Push Payment (APP) fraud (non-coerced):** In traditional APP fraud, the customer is tricked into initiating a payment to a fraudster but is not typically acting under direct duress or coercion involving an immediate threat. The crucial difference

in reporting is that in many jurisdictions, current consumer protection laws historically offered less liability protection for this type of fraud because the customer technically "authorized" the payment themselves, although new regulations are emerging (such as in the UK) that mandate reimbursement for eligible victims.

- **Coerced transactions:** These are typically explicitly considered a form of unauthorized transaction for liability and reporting purposes because the customer's consent was not freely given. The investigation would look for evidence of duress, intimidation, or force.

Banks currently submit records of all customer complaints to the Financial Consumer Agency of Canada (FCAC). As we understand it, these complaints are classified and the "nature of the complaint" description would typically specify cases of coercion to allow the regulator to track these specific trends.

By working with the banks and relevant law enforcement stakeholders to develop a more differentiated taxonomy of fraud classifications, FCAC can develop a system whereby complaints are coded to indicate specific fraud categories, e.g.:

- **Card Not Present**: Online theft
- **Card Present**: Physical card theft
- **Social Engineering/APP:** Customer is tricked into sending money
- **Coercion/Duress**: Customer forced to transact.

This explicit segmentation ensures data analysis reflects the true nature of the crime. By documenting the specific circumstances of coercion during the investigation and using detailed internal and regulatory reporting codes, banks can effectively segment this data to inform better consumer protection measures and assist law enforcement.

8. When should banks be required to annually report to FCAC (e.g., following the end of calendar year or bank's financial year)? Should the reporting be aligned with banks' other reporting obligations (e.g., annual complaints report, board and committee reporting)?

We do not have a recommendation on this as we are unable to weigh the operational and cost implications for banks of the two options in question. Consistent reporting across the banking sector will be important in order to facilitate trend and comparative analysis.

9. Should institutions be required to disclose, upon personal deposit account opening, that prescribed capabilities will not be enabled without express consent and can be disabled, and that withdrawal and transfer limits can be adjusted?

Recommendations (with rationale)

Yes, institutions should be required to disclose this information on personal account opening so that consumers can make a determination then about whether they wish to activate certain account features and so they can benefit fully from the options available to them to set their own withdrawal and transaction limits.

It is also important that consumers be informed at account opening that they can adjust any of these account settings in future should they wish to do so.

Conclusion

Thank you very much for considering our views on this important topic. Should you have questions or wish to discuss any of the above recommendations, please do not hesitate to contact:

Liz Mulholland
CEO, Prosper Canada
lmulholland@prospercanada.org
Mobile: 416 294-3373