Submission on the Proposed Consumer-Driven Banking Regulations

Canada Gazette, Part I, Volume 160, Number 26 (June 27, 2026)

Submitted by: Wendy MacKinnon, Founder and Chief Executive Officer, Twinvocate Inc., Toronto, ON

Date: Monday, August 24, 2026

About this submission

I have spent roughly 35 years in retail technology, payments and digital strategy. I founded SelfPay by Digital Retail Apps, hold multiple United States patents in mobile self-checkout, and co-founded Paytechs Canada in 2019, now FinTechs Canada. I completed a Master of Laws at the University of Toronto Faculty of Law in 2026, with a concentration in innovation and technology. I am currently building Twinvocate Inc., a Toronto company working on credentialing infrastructure for automated agents acting in consumer financial transactions.

I support the framework. My comments concern a single gap that I believe is fixable now at low cost and expensive to fix later.

Summary

The proposed Regulations establish who may access a consumer's financial data, under what security conditions, and with what consent. They do not address a distinct and increasingly urgent question: on whose behalf does the accessing entity act once it holds that data.

The framework as drafted was designed for applications. It will be used by agents. An accredited entity may deploy automated software that reads a consumer's financial position and then recommends, ranks, steers or executes. Nothing in the proposed Regulations requires that entity to disclose whether its recommendations are shaped by compensation it receives from third parties, and nothing in the consent architecture allows a consumer to distinguish between an accredited entity that works for them and an accredited entity that works on them.

Accreditation, as drafted, certifies competence and security. It does not certify loyalty. A consumer looking at the public registry will reasonably read inclusion as an assurance of both.

Two kinds of control

Two different kinds of control are available here, and the proposed Regulations rely almost entirely on one of them. Verification before the fact, ex ante, asks whether an entity is fit to be let in. Recourse after the fact, ex post, asks what happens once an accredited entity has acted and a consumer has been harmed. Accreditation, the security requirements and the public registry are all controls of the first kind.

Comparatively little in the framework is a control of the second kind. Liability is addressed as an allocation between participating entities and their service providers, and record-keeping is framed around demonstrating compliance rather than reconstructing on whose behalf a particular access occurred.

That imbalance is tolerable in the first phase, where read-only access limits the harm to data misuse. It will not survive the second. Once an entity can act on a consumer's instruction, a fitness test administered at the gate cannot carry the weight of an outcome guarantee, and the registry entry the consumer relied on will not tell them who bears the loss.

The recommendations below are addressed to both halves of the problem. Recommendations 1, 2, 5 and 6 concern controls that operate before the fact. Recommendation 4 concerns what happens after it. Recommendation 3 is the hinge between them.

Recommendations

1. Require disclosure of economic alignment at accreditation

Accreditation applications should require an applicant to disclose whether the applicant, or any affiliate, receives compensation that is contingent on the choices a consumer makes after accessing the framework. This includes referral fees, revenue sharing, placement payments, and any arrangement in which the applicant is paid by a party other than the consumer for influencing the consumer's decision.

This is a disclosure requirement, not a prohibition. Entities compensated by third parties should be able to participate. Consumers should be able to know.

2. Carry that disclosure into the public registry

The proposed Regulations contemplate a public registry of participating entities. A registry that lists who is accredited without indicating who each entity is paid by conveys an assurance of neutrality that the accreditation process does not actually provide.

I recommend the registry record, for each participating entity, whether it operates on a consumer-paid, third-party-paid or mixed compensation basis. This is a small addition to a field the registry will already maintain, and it converts the registry from a list of permitted parties into a tool a consumer can actually use.

3. Extend consent and record-keeping to cover purpose and authority

Consent as drafted answers what data is shared, with whom, and for how long. Where an accredited entity acts on the data through automated means, the record should also answer two further questions: on whose instruction the access occurred, and within what limits the consumer authorised action.

Record-keeping obligations should be sufficient that, after the fact, a supervisor or a consumer can reconstruct not only that access was authorised but what the accessing party was authorised to do. Without this, a dispute about an automated decision has no evidentiary basis to resolve on.

This recommendation is the hinge between verification before the fact and recourse after it. Recourse is possible only where the record made at the time captured purpose and authority, and not merely the fact of consent. That creates a design tension the Department should name rather than leave implicit: an evidentiary record sufficient to resolve a dispute about on whose behalf an entity acted is a richer record than data minimisation would otherwise support. The resolution is more likely to run through scoped, verifiable assertions of authority than through broader retention of transaction detail, and it is better settled in the standards work than discovered in the first contested case.

I note the precedent in the proposed amendments to the Financial Consumer Protection Framework Regulations published the same day, which would require express consent before enabling electronic funds transfer capabilities. The principle is the same: a capability that can move money should be affirmatively authorised rather than enabled by default. The same reasoning should apply to automated action taken on a consumer's behalf.

4. Address liability where the accessing entity acted in its own interest

The Regulations allocate liability for security failures and unauthorised access. They should also contemplate the case where access was properly authorised but the resulting recommendation or action served the accessing entity's economic interest rather than the consumer's stated purpose.

This is not a hypothetical harm. It is the ordinary operation of a business model in which the party holding the consumer's data is paid by someone else.

I recognise that a full redress pathway is not a first-phase question. Read-only access limits the harm, and the remedies that matter most will be the ones attached to write access. What the first phase can do is ensure that the record exists to support a determination later. I would encourage the Department to state expressly that recourse design will be taken up in the write-access consultation, so that the absence of a redress mechanism now is understood as sequencing rather than as a judgment that the question does not arise. The Department has already indicated that it will use this comment period to consult on elements of the second phase of consumer-driven banking.[1] If that is the intention, recourse design sits within the scope of the present consultation rather than a later one, and an express statement to that effect would let respondents address it while the sequencing is still open.

5. Set the standard for authority before write access arrives

Write access is not part of the first phase. That is the right sequencing, and it is also the reason to define the standard now. Once automated agents can initiate transactions rather than only read data, the question of what an agent was authorised to do stops being a disclosure matter and becomes a liability matter.

The industry itself anticipates this shift. On a Payments Canada panel published in August 2026, the Chief Banking Officer of Neo Financial described the Real-Time Rail and consumer-driven banking

[1] Payments Canada, "Productivity, prosperity and safety: Advancing Canada's economic priorities through payment policy," published 14 August 2026, recorded at The 2026 SUMMIT. Remarks of Judith Hamel, Director General, Financial Services Division, Financial Sector Policy Branch, Department of Finance Canada.

together as creating the conditions for an independent customer who owns their own data and information, concluding that going forward "the customer is going to own the customer."[2] The framework should be built for the customer who exercises that agency through software.

A recent Canadian example shows what institutions do when no verification standard exists. In June 2025, one of the six largest banks changed its pre-authorized debit process so that a credit card balance could be paid automatically only from a deposit account held at the same institution. Arrangements set up before the change were left in place. The rationale described by industry observers is that institutions have limited ability to confirm that the same person owns both accounts, and that the institution from which funds are drawn has up to 90 days to dispute the transfer. Faced with a counterparty it could not verify and a liability window it could not close, the institution withdrew the connection rather than build the verification. Consumers lost the ability to pay a balance in full automatically from an account held elsewhere, a capability that research associates with materially lower rates of missed payments and interest charges.[3]

The point is not that the decision was unreasonable. It is that restriction is the rational response when verification is unspecified. Consumer-driven banking is intended to move in the opposite direction, toward portability and choice, and the framework should not assume that institutions will build the verification the framework does not require. Where the standard is silent on how a receiving party confirms who is acting, and on whose authority, the safe commercial answer is to narrow the set of counterparties it will deal with. That instinct will apply with considerably more force to write access, and to instructions initiated by software acting for a consumer, than it does to a pre-authorized debit today.

Defining, at this stage, what an accredited entity must be able to demonstrate about the authority under which it acts will be substantially cheaper than retrofitting that requirement into a live framework. The same applies to the screen-scraping prohibition that remains subject to further consultation.

6. Treat verification as a two-directional problem

The framework verifies parties in one direction. Accreditation tells a participating entity, and the Bank of Canada, that a third party is competent to receive consumer data. It gives the consumer nothing with which to verify the party on the other side of a transaction.

That asymmetry is tolerable while a human is present at every step. A person checks a brand, an address bar, a prior relationship, a physical branch. Software acting for a consumer has none of those cues. As transactions become mediated by software on both sides, the consumer's side of verification stops being a matter of judgment and becomes a matter of infrastructure.

The Government's own fraud analysis makes the case. Authorized push payment fraud succeeds precisely because the consumer authorizes the payment correctly. What fails is the consumer's ability to

[2] Payments Canada, The PayPod, Episode 44: "Banking in disguise: When every app becomes a bank," published 5 August 2026, recorded at The 2026 SUMMIT. Remarks of Tim Morris, Chief Banking Officer, Neo Financial.

[3] Mariya Postelnyak, "BMO's auto-pay policy may help limit fraud but could also lead to missed payments, experts say," The Globe and Mail, 12 August 2026. On the consumer effect, a United States Federal Reserve study of approximately 63,000 credit card accounts between 2018 and 2020 found that automatic payment services increased the likelihood of a minimum payment being made by 20 to 29 percentage points and reduced charge-offs by 13 to 19 percentage points.

establish who is on the receiving end. Verification that runs only toward the institution does nothing about this, and the Real-Time Rail will make the consequences irreversible more quickly.

The registry is the obvious starting point, and it costs little. I recommend the Regulations require the public registry to be published in machine-readable form with a programmatic interface, so that software acting on a consumer's behalf can confirm accreditation status directly rather than relying on a consumer to read a web page. A registry that only a human can query will not be used by the agents that will shortly be doing the querying.

This would not be the first Canadian regulator to treat its own framework as data. The Ontario Securities Commission consulted this spring on publishing a machine-readable dataset of its rules and regulatory documents, and its 2026 to 2027 Statement of Priorities commits to a proof of concept for a machine-readable version of Ontario securities regulation.[4]

The scope of that work is rule text rather than entity status, so it does not answer the question raised here. It does establish that the premise is accepted: regulatory information that software must act on should be published in a form software can read. Machine-readable rules tell software what the law says. A machine-readable registry tells software who is authorised. An agent transacting for a consumer needs the second, and needs it at the moment of the transaction rather than at the moment of system design. Specifying the registry as machine-readable and programmatically accessible at the outset will be materially cheaper than retrofitting it once third-party access, and in later phases write access, are already in operation.

This is not a view held only by those building for agents. At Payments Canada's 2026 SUMMIT, Deloitte Canada's payments leader put the question to regulators directly, arguing that controlling fraud, enabling agentic activity, and keeping citizens rather than institutions in control of their own affairs "requires us to have some form of digital identity or at least digital authentication," and that individual institutions cannot supply that on their own.[5] The recommendation above is the narrow, sector-specific version of that argument. A registry that already exists under the Act, published in a form software can read, gives an entity acting for a consumer the same assurance the Act gives participating entities, without waiting on a national identity framework.

Verification should also be proportionate to what is at risk. A requirement that imposes the same check on a $4 payment as on a $40,000 one will be routed around rather than complied with, so the cost of establishing who is on the other side has to scale with the value of the transaction.

Beyond the registry, I would encourage the Department and the Bank of Canada to treat reciprocal verification as in scope for the phase-two design work rather than a problem the market will solve after

---

[4] Ontario Securities Commission, "Transforming how we share Ontario's securities regulation," consultation opened 30 March 2026 and closed 30 June 2026; OSC Statement of Priorities 2026–2027, commitment to develop a proof of concept for a machine-readable version of Ontario securities regulation.

[5] Payments Canada, The PayPod, Episode 45: "Takin' care of business (every working hour): the RTR reality," published 12 August 2026, recorded at The 2026 SUMMIT. Remarks of Todd Roberts, Senior Partner, Market Infrastructure and Payments Leader, Deloitte Canada.

the fact. Establishing the requirement before write access exists is substantially cheaper than adding it to a live framework, for the reason set out above.

Why the timing matters

The Government's own analysis of consumer-targeted fraud, published alongside these Regulations, estimates losses of $704 million in 2025 and acknowledges that this figure likely represents only 5-10% of actual losses. The Real-Time Rail is anticipated to launch in the fourth quarter of 2026. Automated agents capable of acting on consumer financial data are already in commercial deployment.

Canada is building the data-sharing framework, the payment rail and the fraud regime at the same moment. That is an unusual and favourable position. The framework will be materially stronger if it establishes, from the outset, that a consumer is entitled to know whose interests the party holding their data is serving.

I would welcome the opportunity to discuss any of this further.

Wendy MacKinnon

Founder and Chief Executive Officer
Twinvocate Inc.
100 King Street West, Suite 6200
1 First Canadian Place
Toronto, Ontario M5X 1B8
wendy@twinvocate.ai