

Brief to the House of Commons Standing Committee on Citizenship and Immigration (CIMM)

Bill C-12 – Strengthening Canada’s Immigration System and Borders Act

Submitted by: Jan Atkinson

Date: February 2026

This 10-page brief offers a whistleblower-informed perspective on how international outsourcing—especially in accounting, finance back-office and information processing—creates exploitable vulnerabilities for money laundering (including transaction/shadow laundering), trade-based money laundering (TBML), sanctions evasion and extortion attempts against workers, clients and contractors. It draws on public records concerning Abaca Solutions and subsequent enforcement outcomes, and on current Canadian policy developments around Bill C-12 (illicit financing, CBSA powers and information-sharing). The brief proposes concrete, implementation-ready measures that align with FATF standards and FINTRAC's 2024–2025 guidance updates.

Key points:

- Outsourcing chains fragment accountability and data, allowing illicit funds to be disguised as ordinary vendor invoices, payroll and consulting fees—classic transaction/shadow-laundering patterns (FATF 40 Recommendations; professional money launderers; TBML typologies).
- When accounting functions are offshored, access to sensitive ledgers, customer files and identity data increases the attack surface for coercion and extortion (e.g., threats to leak data or falsify entries to force payments).
- Canada's anti-money-laundering regime (PCMLTFA/FINTRAC) increasingly covers agents/mandataries and beneficial-ownership discrepancy reporting, but government-facing vendor chains tied to immigration and border workflows remain a blind spot unless contractually and operationally integrated.
- Bill C-12's goals to disrupt illicit financing and modernize CBSA/IRCC powers can be operationalized with targeted procurement clauses, joint red-flag indicators for services-based TBML/transaction laundering, and protected reporting channels for private-sector whistleblowers exposed to retaliation.
- Specific measures are proposed: (1) confidential, protected reporting; (2) vendor/agent AML 'equivalence' with audit rights; (3) cross-agency red-flags tailored to services and accounting flows; (4) mandatory escalation on beneficial-ownership discrepancies; and (5) secure handling requirements for outsourced accounting data to deter extortion risks.

Requested outcome: adopt the recommendations herein and invite myself to testify.

1) Background: Bill C-12, CIMM and Why Outsourcing Risks Matter

Bill C-12 seeks to strengthen border security and immigration integrity, disrupt organized crime and illicit financing, and expand CBSA authorities and information-sharing across government. These objectives are documented in the Government's overview and in LEGISinfo's legislative history. [Sources: Canada.ca overview of Bill C-12; LEGISinfo].

Outsourcing of accounting and information processing intersects directly with these goals. When sensitive finance workflows (general ledger, accounts payable/receivable, payroll, settlement files) and identity data (KYC, tax, immigration records) are processed by multi-layered, cross-border vendors, detection of criminal abuse becomes harder while the stakes for privacy, coercion and fraud increase.

2) Case Signal from the Public Record: Abaca Solutions

Public reporting and regulatory records indicate that Abaca Solutions promoted an outsourcing model contracting labour in the Philippines. In related criminal proceedings against James Russell ("Russ") Neilson, investors testified about solicitations and alleged misrepresentations; charges included fraud and money laundering. In 2022, the Alberta Securities Commission imposed permanent market-access bans after convictions for fraud, theft and money laundering, noting offshore transfers and cash movements that impeded recovery, with two fraud counts tied to investments in ABACA Solutions Inc. [Sources: Rocky Mountain Outlook report; ASC public interest order].

This case illustrates how cross-border vendor narratives can mask illicit flows, and why procurement and regulatory frameworks must impose visibility on beneficial ownership, payment corridors and service-delivery chains, not only on traditional financial institutions.

3) Mechanics: How Outsourcing Enables Illicit Finance

a) Transaction (shadow) laundering via services. Illicit proceeds are routed through seemingly legitimate service invoices ("consulting", "IT support", "BPO fees") and layered payroll/contractor payments. Fragmented books and offshore processors obscure origin, purpose and beneficial ownership. FATF standards emphasize risk-based controls, third-party oversight and that delegation does not absolve the principal's AML responsibilities.

b) Trade-Based Money Laundering (TBML) in services. TBML techniques—over/under-invoicing, multiple invoicing, phantom deliverables, mismatched documentation—apply to services as readily as goods. They exploit documentation opacity and jurisdictional fragmentation.

c) Canadian regime touchpoints. FINTRAC guidance covers KYC, EFT reporting and suspicious transaction reporting across reporting entities. The 2025 updates strengthened agent/mandatory verification (notably for MSBs) and introduced beneficial-ownership

discrepancy reporting—tools directly relevant to vendor chains that handle cross-border funds and client data.

4) Distinct Risks in Outsourcing Accounting and Finance Back-Office

- Access to master data and ledgers: Offshore staff can view/edit customer master files, AP/AR, bank details and journal entries—creating opportunities for falsification, diversion and coercion.
- Credential sprawl and shared workstations: Weak identity/access management in vendor environments can allow privilege abuse and hard-to-trace actions across teams and time zones.
- Invoice and vendor-creation fraud: Creation of shell vendors and duplicate invoices aligned with TBML techniques (over/under-invoicing, split billing).
- EFT and payroll rerouting: Changes to payee banking details via compromised workflows enable rapid, hard-to-reverse fund diversions across borders.
- Data residency and lawful-access conflicts: Foreign jurisdictions may compel disclosure or limit Canadian oversight, complicating investigations and remediation.
- Weak beneficial-ownership transparency for subcontractors: Layers of subs obscure who actually controls the cash and infrastructure.

5) Extortion and Coercion Risks When Accounting/Data Are Outsourced

When third-party staff have legitimate access to identity, immigration, payroll/tax and customer account data, criminal actors can weaponize that access. Common patterns include: (i) threats to leak or sell sensitive data unless paid; (ii) falsifying accounting entries or vendor bank details under duress; (iii) social-engineering clients using real records to bolster credibility.

Episodes documented by investigative journalism in Canada show a broader climate where intimidation can silence disclosures; while context varies, the chilling effect on whistleblowing is real. Criminal Code s.425.1 makes employer retaliation a crime when employees provide information to law enforcement, and the Competition Bureau offers confidentiality assurances. However, private-sector protections remain fragmented, leaving many at risk when reporting vendor-linked wrongdoing.

6) Practical Red-Flags for Services-Based TBML & Transaction Laundering (for CBSA/IRCC/FINTRAC & Procurement)

- Systematic over/under-invoicing of services versus market baselines; vague deliverables with high fees.

- Multiple invoicing for identical scopes; frequent "change orders" without corresponding output.
- Phantom deliverables or unverifiable milestones; heavy reliance on "management fees" crossings borders.
- Rapid, circular fund flows among vendors, payroll consolidators and foreign processors.
- Frequent ownership/management changes in vendor chains; use of high-risk jurisdictions.
- Unusual amendments to payee banking details; spikes in vendor creation aligned to reporting dates.

7) Recommendations for C-12 Implementation & Oversight

- Protected Disclosure Channel (FINTRAC-CBSA-IRCC). Establish a confidential, protected tipline for private-sector reports of illicit financing and vendor abuse tied to immigration/border processes; reference Criminal Code s.425.1 anti-reprisal and adopt Competition Bureau-style confidentiality assurances.
- Vendor/Agent AML Equivalence & Audit Rights. Require federal immigration/border programs to impose FATF-aligned AML controls on vendors/agents, including right-to-audit, books/records access, beneficial-ownership verification and periodic agent re-verification comparable to FINTRAC's 2025 rules.
- Joint Services-Specific Red-Flags. Publish shared FINTRAC-CBSA-IRCC indicators for services/accounting TBML and transaction laundering, and include them in procurement and vendor-risk assessments.
- Beneficial-Ownership Discrepancy Escalation. Mandate escalation to CBSA/FINTRAC when immigration-relevant vendors show material beneficial-ownership discrepancies or frequent opaque restructurings.
- Secure Handling of Outsourced Accounting Data. Require encryption at rest/in transit, privileged-access management, tamper-evident logging, data-loss prevention, and Canadian-jurisdiction auditability for immigration-relevant datasets handled offshore.
- Committee Accessibility. Encourage in-camera/anonymous testimony for at-risk private-sector witnesses; prioritize briefs from front-line accounting and vendor personnel.

8) Implementation Checklists (For Procurement & Program Leads)

A. Model Contract Clauses (excerpt):

- Vendor confirms ultimate beneficial owners ($\geq 25\%$) and agrees to notify changes within 10 business days; consents to verification against public registries and discrepancy reporting requirements.
- Right-to-audit (on-site/remote) of AML controls, data security, access logs and payment corridors; cooperation with FINTRAC/CBSA/IRCC inquiries.

- Agent/mandatory eligibility verification (criminal record checks; biennial re-verification) for all sub-agents handling payments or immigration-relevant data.
- Prohibition on undisclosed subcontracting; pre-approval required for any sub-processor with cross-border data access.
- Security controls: least-privilege access, MFA, PAM, SIEM logging retained ≥ 2 years, and breach notification ≤ 72 hours to designated authorities.

B. Operations & Monitoring (excerpt):

- Quarterly BO re-screening and sanctions checks on vendors/subs; reconciliation of invoices to delivered service evidence.
- Automated alerts for vendor bank-detail changes; segregation-of-duties for vendor creation and payment release.
- EFT corridor analytics for rapid circular flows; anomaly detection on invoice unit pricing versus peer benchmarks.
- Whistleblower channel testing (mystery reports) and response SLAs; anti-reprisal communication to vendor staff.

9) Alignment with FATF Standards and FINTRAC Guidance

The recommendations operationalize FATF's risk-based approach, beneficial-ownership transparency and responsibilities over third-party providers, and dovetail with FINTRAC's guidance on compliance programs, EFT reporting and the 2025 expansions concerning agent verification and BO discrepancy reporting.

10) Conclusion and Offer to Assist

Outsourcing accounting and information processing is now embedded in Canadian and global operations. Without targeted controls, these same efficiencies become channels for laundering and levers for extortion. The Committee can ensure Bill C-12's illicit-finance ambitions translate into practical safeguards where the risks are highest—inside vendor chains that handle money and data. I respectfully request the opportunity to appear as a witness and to provide expanded annexes (technical indicators, model clauses and control mappings).

References (selected)

- Government of Canada. Understanding Strengthening Canada's Immigration System and Borders Act (Bill C-12).
- LEGISinfo. C-12 (45-1) – Progress and Senate Committee referral.
- Rocky Mountain Outlook. Investors testify at trial how they lost money in Canmore-based Abaca Solutions (Jan. 13, 2020).

- Alberta Securities Commission. Public interest orders in response to criminal fraud conviction against James Russell Neilson (Oct. 21, 2022).
- FATF. The FATF Recommendations (global AML/CFT standard).
- FATF. Trade-Based Money Laundering (2006) and subsequent typologies.
- FATF. Professional Money Laundering (2018).
- FINTRAC. Obligations and guidance portal; EFT reporting guidance; 2025 updates on agents/mandataries and BO discrepancy reporting.
- House of Commons. Guide for Submitting Briefs to Committees.
- CBC's the fifth estate. Dawson Creek: Behind the Fear (program page/archives).
- Criminal Code s.425.1 (anti-reprisal for disclosures to law enforcement); Competition Bureau whistleblower confidentiality.