DIACC CCIAN

Canada's Digital Trust Imperative

A 2031 Strategic Vision to Reduce Fraud, Lower Compliance Costs, and Enable Growth through Coordinated Industry and Government Action

January 2026

Contents

01 Executive Summary

Canada has the expertise, constitutional frameworks, and proven implementations to build a world-leading digital trust infrastructure. British Columbia, Quebec, Alberta, and industry leaders have already demonstrated that transformation is achievable. With coordinated action, Canada can harness the same AI capabilities that fuel fraud and use them to protect data and assets.

Consider a registered nurse in Nova Scotia who applies to work in Alberta to help address critical healthcare shortages. Her credential verification takes six weeks—six weeks of delays while patients wait. Or consider a young couple in Vancouver whose mortgage approval is delayed by two weeks because their lender cannot digitally verify their employment. These are everyday realities of a system built for paper.

The Crisis in Numbers

Synthetic identity fraud: Tripled in one year (2.8% → 8% of credit applications)
Annual fraud losses: $638 million to Canadians in 2024
Compliance costs: $61 billion annually (Canada and U.S.)
Canadian support: 71% believe public-private collaboration is the best path forward

01 Executive Summary

This paper proposes coordinated action across four priorities: harnessing AI to reduce fraud while building resilience; accelerating economic-sector ROI through proof; reducing regulatory burden through compliance alignment; and protecting Canada's digital sovereignty. Provinces and industry accelerate economic use cases while federal frameworks continue to develop. These efforts are complementary.

Independent Validation

Six provincial law societies, including Alberta, Manitoba, Ontario, British Columbia, Saskatchewan, and Nova Scotia, reference DIACC certification in their client verification guidance for anti-money laundering compliance. Manitoba specifically recommends "use a DIACC certified software service."

The Ask

- Provinces modernize credentials and enable interprovincial recognition.
- Industry deploys AI-enhanced verification and pursues Pan-Canadian Trust Framework™ certification.
- Federal government designates a liaison to receive provincial and industry evidence from our forum for consideration in policy development and regulatory guidance.

2031 Targets (from 2024 Baseline)

Demonstration Metric	2024 Baseline	2031 Targets	Measurement
Digital mortgage income verification	~15%	75%	CMHC survey data
Credential recognition	Limited	3 sectors operational	DIACC tracking
Identity fraud losses (annual)	$638M	50% reduction	CAFC annual report
Compliance cost reduction (PCTF adopters)	Baseline costs	20–30% reduction	Member surveys
Canadians with digital credential access	~25%	90%	Provincial reporting

DIACC will publish baseline methodology and annual progress assessments against these targets, beginning in 2027.

DIACC's Commitment

Our working groups will advance updated Pan-Canadian Trust Framework™ guidance with AI verification criteria and regulatory mapping, with publication targeted for late 2026.

Built on Canadian Values

Privacy by design: No centralized identity databases. Credentials remain on user devices. Canadians control what they share, with whom, and when.

No one left behind: Every digital service maintains a non-digital alternative. PCTF certification requires accessibility testing and inclusive design.

Provincial sovereignty respected: Provinces retain authority over their credentials. Federal coordination builds on provincial innovation.

Canadian control maintained: The Pan-Canadian Trust Framework™ ensures Canada sets its own rules for digital trust.

02 The Urgent Case for Action

A decade ago, DIACC warned that without coordinated action, Canada risked ceding control of digital trust to foreign platforms. That warning has become reality.

AI-generated deepfakes now spoof voices, photos, videos, and signatures with alarming accuracy. Traditional identity verification is breaking under pressure.

The Numbers Tell the Story

- Synthetic identity fraud has tripled in one year—from 2.8% to 8% of credit applications[1].
- Identity fraud now represents 48.3% of all fraudulent applications, up from 42.9% just one year ago[1].
- Canadians reported $638 million in fraud losses in 2024 alone[2].
- Businesses face $61 billion in annual compliance costs across Canada and the U.S., with 79% reporting increased KYC technology costs[3].

Research consistently shows Canadians support transformation: 71% believe collaboration between public and private sectors is the best path forward for digital trust and identity frameworks[4].

What's Broken

For Citizens

Multiple logins per service, with no portable credentials. Physical documents that can be lost, stolen, or forged. Inconsistent onboarding experiences. No meaningful control over personal data trapped in proprietary platforms.

For Businesses

Corporate banks spend $1,500–$3,000 per KYC review[5]. Manual employment verification adds 7–14 days to mortgage approvals[6]. Healthcare and construction face 2–4 week delays for interprovincial credential verification. Meanwhile, fraudsters adapt faster than security upgrades roll out.

For Governments

Digital trust spans multiple jurisdictions with distinct mandates. The federal government develops frameworks for citizen authentication. Provinces control local credentials, professional licensing, and vital statistics. Finance regulators focus on compliance. Each operates on different timelines.

Economic transformation can advance in parallel with the development of government-to-citizen authentication, with each track strengthening the other.

Canada is Falling Behind

Country	Achievement
Estonia	3,000+ government services via X-Road
Norway	95% citizen adoption via BankID
European Union	Digital Identity Wallet launching in 2026

Canada has the expertise to match these regions, and provincial and industry momentum is contributing to the foundation for coordinated national progress.

03 Canadian Momentum: What's Already Working

Canada isn't starting from zero. Provincial leadership and industry innovation have demonstrated what's possible when jurisdictions and businesses act decisively.

Jurisdiction	Initiative	Scale/Impact
British Columbia	BC Services Card	4.6M users (90% of the province)
British Columbia	OrgBook BC	1.4M entities, 3.8M credentials
Quebec	Bill 82 (Digital ID Law)	Legal framework, deployment through 2028
Alberta	Mobile Health Card	First in Canada, 1M projected signups
Interac	Sign-In Service	141M government interactions/year
MyCreds (ARUCC)	Academic Credentials	150+ institutions

Provincial Leadership Examples

British Columbia's Services Card

BC pioneered secure digital credentials starting in 2013. The BC Services Card now serves over 4.6 million British Columbians, representing more than 90% of the province[7]. In April 2018, BC launched its first public-facing online service with StudentAid BC[8], demonstrating that jurisdictional leadership can deliver immediate value while creating templates others adopt.

British Columbia's OrgBook

In January 2019, BC launched OrgBook BC, the first jurisdiction in North America to use blockchain technology for verified organizational credentials[9]. The public registry contains over 1.4 million active legal entities and more than 3.8 million verifiable credentials[10].

Quebec's Bill 82

Quebec launched its Government Authentication Service in February 2023, replacing the legacy clicSÉQUR system with 3.5 million accounts[11,12]. This operational system provided the foundation for Quebec's landmark Bill 82, passed in October 2025, establishing the legal framework for Quebec to deploy a comprehensive digital identity and wallet capability by 2028[13].

Alberta's Mobile Health Card

On August 29, 2025, Alberta launched Canada's first mobile health card through the Alberta Wallet app[14]. The provincial government anticipates approximately one million new digital wallet signups[15]. Parents can hold children's cards in their wallets, demonstrating how provincial health systems can modernize while maintaining paper alternatives.

Industry Innovation

Canada's private sector has deployed multiple digital trust solutions demonstrating market readiness. Interac's sign-in service connects over 141 million government-to-citizen interactions annually, processing 800 transactions per second during the COVID-19 surge in demand[16–18]. Major banks have implemented AI-enhanced KYC systems processing millions of verifications monthly.

Finance: Interac's document verification service, launched with the Canada Revenue Agency, eliminates multi-day wait times for paper security codes through instant verification[19]. Interac Verified's credential service enables identity verification once, with reuse for up to 12 months, and stores data locally on user devices.20,21

Education: MyCreds, Canada's bilingual national digital credential wallet, now serves over 150 colleges, universities, and government agencies[22]. In March 2024, Nova Scotia Apprenticeship Agency became the first apprenticeship authority in Canada to issue digital Certificates of Qualification through MyCreds[23]. In January 2025, ARUCC launched the MyCreds Member Trust Registry, enabling cross-border interoperability[24].

Workforce: Credivera provides real-time workforce credential verification, connecting employers, training providers, and workers through a secure exchange for verifiable digital credentials. The platform completed testing with Shared Services Canada under the Innovative Solutions Canada program, validating it for federal workforce applications. The Calgary-based platform serves regulated industries in over 30 countries, enabling workers to hold and share verified qualifications via a digital wallet.

Professional Regulatory Recognition

Professional regulatory bodies are recognizing trusted verification frameworks. Six provincial law societies, including Alberta, Manitoba, and Ontario, reference DIACC certification in their client verification guidance for anti-money laundering compliance, with Manitoba specifically recommending DIACC-certified software services[25].

These Canadian examples share common elements: provincial or industry leadership, privacy-by-design principles, interoperability with existing systems, and documented adoption at scale. Transformation requires courage to deploy, evidence to document, and commitment to standards that enable broader adoption.

The provincial, federal, and industry initiatives highlighted here represent a sample of the innovation occurring across Canada. For a complete list of DIACC members and Pan-Canadian Trust Framework™ certified service providers, visit **diacc.ca/membership/diacc-members** and **diacc.ca/certification-program/trusted-list/**.

04 Strategic Approach: Four Priorities for Action

Digital trust infrastructure develops most effectively through coordinated but independent tracks rather than sequential stages. The federal government rightfully focuses on frameworks for citizen authentication, requiring rigorous policy development. Simultaneously, economic transformation can accelerate through provincial and industry leadership.

DIACC's 2026–2031 strategy advances three interconnected priorities:

Four Strategic Priorities

1. **Reduce Fraud** — Deploy AI-enhanced verification to contain the synthetic identity crisis
2. **Accelerate Economic ROI** — Develop, measure, and amplify economic ROI evidence
3. **Reduce Regulatory Burden** — Map frameworks to cut compliance costs 20–30%
4. **Ensure Inclusive Digital Sovereignty** — Keep Canada in control of its digital trust infrastructure

This Pattern Is Proven

Canada has always built transformative infrastructure through coordinated independent action. Provinces built power grids independently, then interconnected them. Banks created Interac collaboratively while federal oversight evolved alongside demonstrated success. BC pioneered the Services Card, building evidence that informs national approaches. In each case, practical deployment built evidence that informed policy, creating virtuous cycles of innovation and governance.

Priority 1: Harness AI to Reduce Fraud While Building Resilience

AI simultaneously creates unprecedented fraud risk and offers powerful verification capabilities. Organizations must adopt AI-enhanced verification while defending against AI-powered attacks.

Early adopters of certified AI verification systems gain a competitive advantage through:

- Measurably lower fraud rates—sector programs and vendor case studies suggest AI-supported verification can reduce synthetic identity fraud by 40–60%, though results vary by implementation and sector[25].
- Regulatory readiness as AI governance frameworks emerge.
- Market differentiation for organizations deploying high-trust, responsible AI systems.
- Improved customer experience through faster, more accurate verification.

Explicit criteria for responsible AI use in verification, conformance testing protocols, and certification programs will give organizations confidence to deploy AI verification at scale.

Priority 2: Accelerate Economic Sector ROI Through Proof

Priority Sector Initiatives

Finance and Lending: Mortgage workflows rely on manual verification, adding 7–14 days to approval times[6]. Banks, credit unions, payroll providers, and fintechs can collaborate to implement standardized digital income and employment verification with AI-supported fraud detection.
Expected impact: 40–60% reduction in verification time[26].

Workforce Mobility: Healthcare, construction, and other priority sectors face critical labour shortages while credential verification delays reach weeks. Provincial regulators, trade associations, and employers can collaborate to support the exchange of digital credentials.
Expected impact: verification reduced from weeks to 24–48 hours.

Supply Chain Transparency: Critical mineral supply chains require verifiable ethical sourcing. Resource-rich provinces can convene mining companies, Natural Resources Canada, and customs authorities to explore digital traceability, positioning Canadian minerals as verifiably ethical.
Expected impact: Supply chain verification reduced from weeks to days, positioning Canadian minerals as verifiably ethical with real-time transparency.

Priority 3: Reduce Regulatory Burden Through Compliance Alignment

Organizations face rising compliance costs due to complex, fragmented, and inconsistently interpreted digital verification obligations. Industry research shows that automated KYC solutions achieve 20–30% cost reductions by reducing manual labour, speeding processing, and reducing errors[27].

DIACC's Role

- Map PCTF conformance to regulatory obligations (FINTRAC, OSFI, provincial licensing)
- Translate policy into implementable workflows and compliance templates
- Certify compliant services through the PCTF Trustmark program
- Provide a neutral voice in regulatory consultations

Expected Outcomes

- 20–30% compliance cost reduction for organizations using PCTF-mapped workflows
- Faster regulatory approvals through standardized verification processes
- PCTF certification becomes a competitive advantage in procurement

Priority 4: Ensure Inclusive Digital Sovereignty

Canada must maintain authority over its digital trust infrastructure. Foreign platforms and international bodies should not dictate how Canadians verify identity or control their data. Simultaneously, Canada must continue to foster partnerships with international partners who share our values and priorities.

Publish Sovereignty Principles

- Canadian authority-by-design embedded in PCTF standards
- Federal-provincial interoperability that respects constitutional jurisdiction
- Protection against platform concentration by foreign technology providers
- International partnerships that advance Canadian interests

Commit to Inclusivity by Design

Digital transformation must not leave anyone behind. DIACC commits to:

- Maintain non-digital alternatives for every service
- Exploratory dialogue with Indigenous organizations, including seeking guidance from the First Nations Information Governance Centre and relevant Métis and Inuit bodies, before finalizing sector programs affecting Indigenous communities
- Digital literacy programs accompanying deployment
- PCTF requires accessibility

Addressing the Fragmentation Concern

Some stakeholders question whether provincial and industry action risks creating fragmentation. This concern reflects important considerations about interoperability and national cohesion. However, the coordinated approach addresses these concerns while responding to urgent market realities:

Urgency: Fraud losses compound daily. Each year, inaction costs Canadians hundreds of millions of dollars.

Complementarity: Provincial and industry initiatives provide evidence to strengthen federal efforts. Real-world deployment generates insights that inform more effective national policy.

Interoperability by Design: When initiatives align with the Pan-Canadian Trust Framework™, they create interoperable building blocks rather than proprietary silos.

Intergovernmental Alignment: DIACC's role is distinct from formal federal-provincial-territorial mechanisms. While FPT tables like the Forum of Ministers Responsible for Digital Government coordinate policy across jurisdictions, DIACC convenes industry expertise to support intergovernmental objectives, translating policy direction into technical standards and enabling private-sector participation that government-only tables cannot access. We coordinate with, rather than duplicate, intergovernmental processes, and encourage provincial members to bring DIACC insights to FPT discussions where appropriate.

Proven Precedent: Canada's most successful infrastructure, from railways to payment systems, emerged through coordinated provincial and private-sector innovation with federal coordination building on demonstrated success.

Transformation requires clear direction with adaptive execution. DIACC proposes the following phased approach, with progress reported:

Phase 1: Foundation (2026)

Establish sector-specific working groups for Finance/Lending, Healthcare/Workforce, and Supply Chain, comprising provincial representatives, industry participants, and regulatory observers. Release updated Pan-Canadian Trust Framework™ guidance incorporating AI verification criteria and regulatory mapping. Initiate the first sector program in Finance/Lending with committed financial institutions and payroll providers.

Deliverables: Baseline metrics established; sector program design documented; FINTRAC regulatory mapping initiated; sovereignty principles whitepaper published; initial regulatory engagement completed.

Phase 2: Demonstration (2027–2028)

The Finance/Lending sector program becomes operational, with preliminary results published. Initiate Healthcare/Workforce sector program supporting interprovincial credential recognition for priority professions. Publish PCTF-to-PCMLTFA compliance mapping. Initiate scoping for the Supply Chain program with resource-rich provinces. Publish the first progress report against the 2031 targets and document comprehensive ROI from initial programs.

Deliverables: Operational sector programs with documented business cases; regulatory learnings incorporated into framework updates; compliance cost reduction case studies published.

Phase 3: Scaling (2029–2030)

Expand successful sector programs to additional provinces and institutions. Target the broad adoption of digital income verification among major financial institutions. Support interprovincial credential recognition for healthcare, construction, and skilled trades. Integrate with federal frameworks where applicable.

Deliverables: Scaled implementation with national coverage emerging; measurable fraud reduction demonstrated; compliance cost savings quantified.

Phase 4: Maturity (2031)

Achievement of 2031 targets. Canada's digital trust ecosystem operates with seamless interoperability across provinces and sectors —Canadian solutions positioned for international adoption.

Deliverables: Final assessment report; advanced 2031–2036 strategic plan.

06 Challenges and Mitigations

Any transformation of this scale faces obstacles. DIACC has identified the primary challenges and proposes concrete mitigations:

Challenge	Mitigation
Privacy Concerns	PCTF mandates privacy-by-design principles: data minimization, user consent controls, and the prohibition of centralized databases. Certification requires independent privacy impact assessments.
Implementation Costs	Sector programs will document ROI. Shared infrastructure reduces per-organization costs. Phased implementation starts with the highest-impact use cases. DIACC will advocate for SME adoption incentives.
Regulatory Complexity	PCTF-to-regulatory mapping reduces interpretation burden. Compliance templates accelerate adoption. Regular regulator engagement ensures alignment.
Interoperability	PCTF provides technical standards. DIACC certification verifies compliance. Regular convenings align provincial approaches. Alignment with international standards (ISO/IEC 18013-5, W3C) ensures global compatibility.

06 Challenges and Mitigations

Challenge	Mitigation
Digital Divide	All implementations maintain non-digital alternatives (e.g., Alberta's paper option). DIACC advocates for inclusive design principles and accessibility testing. Digital literacy programs accompany deployment.
Cybersecurity	A decentralized architecture (credentials on user devices) reduces the attack surface. PCTF requires security audits and incident response protocols. Regular penetration testing informs improvements.
Jurisdictional Complexity	The approach acknowledges jurisdictional complexity rather than avoiding it. The provinces and federal government each act within constitutional authority. Success builds momentum. DIACC serves as a neutral convener.
Platform Concentration	Canadian-controlled standards (PCTF) ensure sovereignty. Open standards prevent vendor lock-in. The certification program creates a competitive market for domestic providers.

Supporting Public Confidence

Digital initiatives succeed or fail on public trust. DIACC recognizes that provincial leaders face legitimate questions about privacy, surveillance, and digital exclusion. We commit to providing members with:

- Key messages addressing common public concerns
- Documentation of how provincial implementations (BC, Alberta, Quebec) have navigated public communications
- Privacy impact assessment templates aligned with provincial FOIP/FIPPA requirements

Ministers should be able to answer questions about digital trust initiatives with confidence. DIACC will develop communications resources to support that goal.

07 Call to Action

Building Canada's digital trust infrastructure requires vision, coordination, and sustained effort across all sectors. Provincial segments can operate independently while building toward interconnection. Industry innovations can prove value rapidly. Federal coordination can build on evidence from deployment.

No single government or organization can create this infrastructure alone.

Why DIACC?

Provincial governments can modernize credentials independently, and interprovincial recognition benefits from federal coordination. Supporting economic growth requires pragmatic problem-solving. DIACC is a neutral organization with deep expertise in implementing digital trust. Our members, including financial institutions, telecoms, technology providers, and governments, have deployed verification systems at scale and learned what works in practice.

We've developed the Pan-Canadian Trust Framework™ through this operational experience. We're proposing a structured engagement to explore how PCTF criteria align with federal and provincial requirements, identify gaps, and determine where industry evidence can inform policy development. That conversation benefits from honest acknowledgment of our perspective: we represent organizations that have invested in digital trust infrastructure and have societal and commercial interests in its success. Those interests align with public policy goals; DIACC seeks to test alignments through rigorous engagement.

What DIACC Offers

DIACC offers public and private sector partners practical support:

- **Industry intelligence:** Aggregated data on verification outcomes, fraud patterns, and compliance costs from our membership
- **Regulatory navigation:** PCTF-to-regulatory mapping that cuts compliance costs and reduces audit risk
- **Provincial Convening:** Engagement forum for provincial digital trust programs, informed by implementation experience across jurisdictions
- **Program capacity:** Test verification approaches with financial institutions, telecoms, and technology providers before broader rollout
- **Convening power:** Forum for cross-sector consultation where industry expertise can inform policy development

Getting Started: Entry Points by Readiness

Provinces and organizations are at different stages of digital trust maturity. There is no single path forward—each can engage based on current capacity:

If your organization has...	Your entry point might be...
Established digital trust program	Interprovincial collaboration; PCTF contributions; working group leadership
Health card modernization underway	Alberta Wallet model adaptation; healthcare credentials sector program
Strong trades/resource sector	Workforce mobility and supply chain traceability programs
Compliance cost pressures	PCTF certification; regulatory mapping resources; compliance templates
Limited capacity	Observer status; learn from early movers; targeted consultation

Provincial Governments

1. Modernize credentials with digital verification capabilities.
2. Enable interprovincial recognition for priority sectors (healthcare, construction, trades).
3. Facilitate sector programs and rigorously document outcomes.
4. Collaborate through neutral forums like DIACC to align approaches.

Industry Leaders

1. Deploy AI-enhanced verification systems and document fraud reduction.
2. Participate in sector programs that prove business cases.
3. Pursue Pan-Canadian Trust Framework™ certification to differentiate services and reduce compliance burden.
4. Engage constructively with regulators to demonstrate compliance and inform policy.

Federal Government

1. Continue to lead essential work on government-to-citizen authentication frameworks.
2. Incorporate evidence from provincial and industry deployments into policy evolution.
3. Consider PCTF alignment when developing regulatory guidance.
4. Explore with DIACC how PCTF criteria relate to existing federal frameworks such as ITPIN and PBMM.
5. Participate in neutral convenings to identify alignment opportunities.

DIACC Commitments

In 2026: Working groups mobilize around Finance/Lending, with Healthcare/Workforce and Supply Chain scoping to follow. Advance updated Pan-Canadian Trust Framework™ guidance incorporating AI verification criteria and regulatory mapping. Grow the trusted list of certified providers. Publish the sovereignty principles whitepaper. Initiate the first sector program in Finance/Lending.

In 2027 and beyond: Expand sector programs to Healthcare/Workforce and Supply Chain sectors. Publish PCTF-to-PCMLTFA compliance mapping. Publish the first progress report against the 2031 targets.

Ongoing accountability: Publish progress reports that transparently document successes and challenges.

The AI verification crisis demands urgency. Synthetic identity fraud tripled in one year. Compliance costs strain innovation. Canadians lose hundreds of millions to preventable fraud. Canada has the expertise, the constitutional authority, and the economic imperative to act. The opportunity is to build evidence through parallel innovation that informs and accelerates coordination across all levels of government and industry.

Immediate Next Steps

Provincial leaders: Contact DIACC to join sector working groups (initiated by mid-2026)

Industry executives: Request PCTF certification briefing at voila@diacc.ca

Federal partners: Participate in neutral convenings

Contact: contact@diacc.ca | www.diacc.ca

08 About DIACC

The Digital ID and Authentication Council of Canada (DIACC) is Canada's bridge between regulators, innovators, and markets, turning standards and policy into trusted, market-ready solutions.

As Canada's non-profit public-private forum focused exclusively on digital trust and verification, DIACC operationalizes standards through a proven approach: convene stakeholders across government, industry, and civil society; define problems with clarity and quantify impacts; develop industry standards like the Pan-Canadian Trust Framework™; certify compliant services through the PCTF Trustmark program; and prove viability through targeted programs that demonstrate ROI.

Since 2012, DIACC has delivered the Pan-Canadian Trust Framework™, conducted research that reduces market uncertainty, and equipped regulators with evidence-based conformance tools. Our members include Canada's major financial institutions, telecommunications providers, technology companies, and federal, provincial, and municipal governments.

Our vision: A Canada where digital trust and verification powers economic growth, strengthens fraud resilience, and enhances safe, efficient, and privacy-protecting interactions for all participants.

For more information, visit **www.diacc.ca** or contact us at **contact@diacc.ca**.

Acknowledgments

This paper builds on DIACC's 2015 white paper "Building Canada's Digital Future." It reflects input from DIACC members, government partners, industry leaders, and civil society stakeholders—special thanks to all who contributed insights and expertise.

09 References

1. Equifax Canada (September 24, 2024). "Equifax Canada Reports Rise in Automotive Fraud." Synthetic identity fraud rose from 2.8% in Q2 2023 to 8% in Q2 2024; identity fraud represents 48.3% of fraudulent applications. Available at: https://www.equifax.ca/about-equifax/press-releases/-/intlpress/equifax-canada-reports-rise-in-automotive-fraud/
2. Canadian Anti-Fraud Centre (2025). "Fraud Prevention Month 2025." Canadians lost $638 million to fraud in 2024. Available at: https://www.canada.ca/en/competition-bureau/news/2025/02/fraud-prevention-month-to-focus-on-impersonation-fraud-one-of-the-fastest-growing-forms-of-fraud-affecting-canadians.html
3. LexisNexis Risk Solutions (2024). "True Cost of Financial Crime Compliance Study—U.S. and Canada." Total compliance costs reached $61 billion in 2023; 79% of organizations report increased KYC technology costs. Available at: https://risk.lexisnexis.com/about-us/press-room/press-release/20240221-true-cost-of-compliance-us-ca
4. DIACC (April 2023). "2022 Digital Identity Perspectives Research." 71% of Canadians believe that collaboration between the public and private sectors is the best approach to digital identity frameworks. Available at: https://diacc.ca/2023/04/20/canadians-continue-to-demand-transparency-and-control-over-personal-data/
5. Fenergo (2022). "KYC Trends in 2022: Global Research Report." A survey of 1,000+ C-suite executives found that 54% spend $1,500–$3,000 per KYC review, with 7% spending over $3,000. Available at: https://resources.fenergo.com/blogs/kyc-compliance-for-banks-addressing-the-cost
6. Analysis based on Canadian mortgage industry data. Clover Mortgage, nesto, and Ratehub report approval timelines of 7–14 days for full approval after pre-approval. Digital verification efficiency estimates derived from Blend (2023), "The State of Digital Lending," reporting 2–4× faster onboarding with digital income verification, and Equifax Workforce Solutions case studies indicating 18-minute reduction in manual review time per verification. See also: Mortgage Professionals Canada (2024), "Annual State of the Residential Mortgage Market in Canada."

7. DIACC (March 2019). "Identity in Action Case Study: BC Services Card." Over 4.6 million BC Services Cards in circulation with more than 90% of British Columbians as current cardholders. Available at: https://diacc.ca/2019/03/05/identity-in-action-case-study-bc-services-card/

8. Government of British Columbia. "BC Services Card Authentication Service." First public-facing service launched April 2018 with StudentAid BC. Available at: https://digital.gov.bc.ca/bcgov-common-components/bc-services-card/

9. Government of BC News (January 2019). "New service transforms how business, government share information." British Columbia first jurisdiction in North America to use blockchain technology for government-business interactions. Available at: https://news.gov.bc.ca/releases/2019CITZ0002-000062

10. Government of BC Digital (June 2021). "OrgBook BC." Over 1.4 million active legal entities and over 3.8 million verifiable credentials. Available at: https://digital.gov.bc.ca/2023/07/26/orgbook-bc/

11. MTL Blog (January 2023). "The SAAQ Is Making It Easier Than Ever To Avoid The SAAQ." SAAQclic launched February 20, 2023. Available at: https://www.mtlblog.com/the-saaq-is-making-it-easier-than-ever-to-avoid-the-saaq

12. clicSÉQUR. "What is clicSÉQUR?" Over 3.5 million accounts. Government Authentication Service launched to replace clicSÉQUR. Available at: https://www.info.clicsequr.gouv.qc.ca/en/citoyens/what-is-clicsequr/

13. ID Tech (October 2025). "Quebec Passes Landmark Digital ID Law Emphasizing Privacy and User Control." Bill 82 passed October 28, 2025. Available at: https://idtechwire.com/quebec-passes-landmark-digital-id-law-emphasizing-privacy-and-user-control/

14. ID Tech (September 2025). "Alberta Launches Canada's First Mobile Health Card Through Alberta Wallet." Launched August 29, 2025. Available at: https://idtechwire.com/alberta-launches-canadas-first-mobile-health-card-through-alberta-wallet/

15. Alberta Medical Association (August 2025). "AHCIP cards go digital." Government anticipating approximately one million new MyHealth Records signups. Available at: https://www.albertadoctors.org/news/publications/presidents-letter/ahcip-cards-go-digital/

16. Retail Banker International (May 2017). "SecureKey builds federated digital ID network in Canada." SecureKey Concierge launched 2012 with major Canadian financial institutions. Available at: https://www.retailbankerinternational.com/features/securekey-builds-federated-digital-id-network-in-canada-5688029/

17. American Banker (June 2020). "Coronavirus Lockdown Spurs Widespread Adoption of Digital ID Tech in Canada." SecureKey processed 800 government aid transactions per second; 1 million new users added in April 2020. Available at: https://www.americanbanker.com/news/coronavirus-lockdown-spurs-widespread-adoption-of-digital-id-tech-in-canada

18. Interac (October 2025). "Secure. Trusted. Helping Canada navigate a digital future." Interac sign-in service supports more than 141 million interactions with government services in 2024. Available at: https://www.interac.ca/en/company/about/secure-trusted-helping-canada-navigate-a-digital-future/

19. Interac (April 2024). "The CRA leverages Interac document verification service." Enables immediate CRA account, eliminating the 10-day wait for security codes. Available at: https://www.interac.ca/en/content/news/the-cra-leverages-interac-document-verification-service/

20. Interac (May 2025). "Interac launches the Interac Verified credential service." FCT first partner to deploy credential service in real estate ecosystem. Available at: https://www.interac.ca/en/content/news/interac-launches-the-interac-verified-credential-service-to-enhance-secure-identity-verification/

21. Interac (May 2025). "Interac Verified credential service." Reusable for up to 12 months; data stored on user's smartphone with Advanced Encryption Standard, not in cloud.

22. CB Insights (2025). "MyCreds." Over 150 colleges, universities, and government agencies issuing through the network. Available at: https://www.cbinsights.com/company/mycreds

23. MyCreds (March 2024). "MyCreds Announces NSAA as First Canadian Apprenticeship Authority to Adopt Digital Credentialing." Available at: https://mycreds.ca/2024/03/15/mycreds-announces-nsaa-as-first-canadian-apprenticeship-authority-to-adopt-digital-credentialing/

24. CNW (January 2025). "ARUCC MyCreds|MesCertif Unveils New Member Trust Registry in Partnership with MATTR." Available at: https://www.newswire.ca/news-releases/arucc-mycreds-mescertif-unveils-new-member-trust-registry-in-partnership-with-mattr-856924033.html

25. DIACC analysis of provincial law society client verification guidance (January 2026). Six law societies reference DIACC certification: Law Society of Alberta, Law Society of Manitoba, Law Society of Ontario, Law Society of British Columbia, Law Society of Saskatchewan, and Nova Scotia Barristers' Society. Manitoba's guidance specifically states "use a DIACC certified software service." These are recommendations, not mandates.

26. AI fraud reduction estimates based on vendor case studies and industry pilot programs. Sources include: Socure (2024), "The State of Synthetic Identity Fraud"; Jumio (2024), "Identity Verification Benchmark Report"; and ACFE (2024), "Report to the Nations." Actual results vary significantly by implementation quality, sector, and fraud patterns. DIACC will document specific outcomes through pilot programs to establish Canadian-specific benchmarks.

27. Middesk (2025). "The True Cost of Manual ID Verification: Case Studies & Data." Organizations implementing automated KYC achieve 20–30% cost reductions. Available at: https://www.middesk.com/blog/manual-identity-verification