DIACC CCIAN

From Trust to Growth: The Business Case for Digital Client Verification in Open Banking and Lending

DIACC Members Report

Industry Workshop 2025

Contents

01 Executive Summary

The Digital ID and Authentication Council of Canada (DIACC) convened an industry workshop in Montreal focused on exploring the business case for digital trust in open banking and lending. The session brought together stakeholders from government, financial services, technology providers, and legal sectors to examine how digital client identity verification (IDV) can drive measurable value while mitigating fraud and enabling growth.

Participants explored three core themes: quantifying fraud prevention and risk mitigation, converting trust into business growth, and leveraging digital trust and verification as a strategic competitive advantage. The discussions revealed strong consensus around treating digital trust and verification as critical infrastructure rather than compliance overhead, while highlighting the need for business-problem-solving standards and clearer metrics to demonstrate return on investment.

Key outcomes included recommendations to develop shared metrics for fraud prevention, prioritize frictionless user experiences, and position Canada's regulatory framework as a global differentiator in digital trust ecosystems.

02 Workshop Overview

Objective: To build a comprehensive business case for digital trust infrastructure in the context of open banking and lending, focusing on fraud prevention, growth enablement, and competitive positioning.

Format: Facilitated roundtable discussions organized around three thematic topics, with cross-sector participation and collaborative ideation.

Participants: Representatives from financial institutions, fintech companies, government agencies, identity verification providers, legal compliance teams, and business development professionals.

Topic 1: Quantifying Fraud Prevention & Risk Mitigation

Key Takeaways

Workshop participants emphasized that metrics for success vary significantly by stakeholder type. Government entities prioritize operational efficiency and regulatory compliance, while investors focus on market opportunity and business units concentrate on risk reduction. Despite these different perspectives, cost emerged as the dominant unifying metric across all tables.

Discussions centered on the dual anchors of "cost of fraud" versus "cost of prevention," with participants noting the importance of evaluating total cost of ownership throughout the fraud lifecycle. Several groups highlighted the tension between compliance-driven approaches, which prioritize risk reduction, and business-focused perspectives that emphasize return on investment and customer enablement.

02 Workshop Overview

Participants agreed that balancing up-front investment in digital trust and verification infrastructure against long-term lifecycle savings represents a critical framework for decision-making.

Barriers & Challenges

- **ROI Quantification Difficulties:** Organizations struggle to translate fraud prevention outcomes into clear financial metrics that resonate with executive leadership and board-level decision-makers.
- **Data Fragmentation:** Information about fraud incidents, prevention costs, and operational impacts remains siloed across different business units, making comprehensive analysis challenging.

Recommendations

1. **Develop Shared Industry Metrics:** Create standardized measurements for fraud avoided and efficiency gained that can be adopted across sectors to enable meaningful benchmarking.
2. **Lifecycle Cost Analysis:** Conduct thorough build-versus-buy assessments that capture total lifecycle cost benefits, including both direct and indirect savings from fraud prevention.

Topic 2: Converting Trust into Growth

Key Takeaways

Participants engaged in robust debate around the tension between maintaining security through verification processes and minimizing onboarding friction. The consensus view held that verified digital identities serve as enablers for improved access to capital, enhanced investor confidence, and stronger customer retention.

Tables identified several critical key performance indicators: conversion rates, fraud loss rates, customer lifetime value, and onboarding completion time. Groups also noted the operational cost benefits of better IDV systems, particularly in reducing help-desk traffic and downstream support costs.

Compelling industry data shared during the discussions revealed that 84% of firms experienced higher revenue after improving customer service quality, while 42% of customers abandon onboarding processes that are not frictionless.

Barriers & Challenges

- **Revenue Impact Quantification:** Organizations find it difficult to measure and attribute revenue losses specifically to friction in identity verification processes.
- **Integration Complexity:** Technical challenges exist in creating seamless integration between business-to-business and business-to-consumer IDV systems.

Recommendations

1. **Prioritize Frictionless Experience:** Treat user experience as a measurable growth driver with dedicated metrics and executive accountability.
2. **Capture Drop-off Metrics:** Implement comprehensive tracking of conversion drop-off points and onboarding speed to identify improvement opportunities.
3. **Enable Cross-Sector Data Sharing:** Encourage secure data sharing frameworks that expand market access to underserved populations, including underbanked individuals and newcomers to Canada.

Topic 3: Strategic Positioning & Competitive Advantage

Key Takeaways

Workshop participants positioned digital trust and verification as a foundational element of broader systems modernization and digital transformation initiatives across industries. Canada's institutional credibility through organizations such as the Bank of Canada, the Office of the Superintendent of Financial Institutions (OSFI), and its participation in the Financial Stability Board presents an opportunity to shape international IDV standards.

Discussions highlighted the business opportunities created by trusted ID ecosystems, including embedded finance applications, cross-sector credential reuse, and data-driven innovation. Participants noted that certification and compliance readiness through verified credentials strengthen competitive advantage in increasingly crowded markets.

Barriers & Challenges

- **Revenue Impact Quantification:** Organizations find it difficult to measure and attribute revenue losses specifically to friction in identity verification processes.
- **Integration Complexity:** Technical challenges exist in creating seamless integration between business-to-business and business-to-consumer IDV systems.

Recommendations

1. **Leverage Regulatory Credibility:** Position Canada's strong regulatory environment and institutional trust as a global differentiator in digital trust and verification markets.
2. **Build Cross-Sector Alignment:** Develop consensus around reusable, standards-based identity systems that work across industries and use cases.
3. **Frame IDV as Revenue Enabler:** Communicate digital trust and verification as a driver of new revenue streams, product innovation opportunities, and enhanced international competitiveness rather than simply a cost center.

03 Common Threads & Collective Insights

Primary Business Case Drivers

Across all discussion tables, three core drivers emerged consistently: cost reduction through fraud mitigation, enhanced customer trust, and trust-enabled business growth.

Critical Key Performance Indicators

- Cost of fraud (prevention and impact)
- Onboarding conversion rate
- Customer lifetime value
- Total cost of ownership for identity infrastructure

Systemic Barriers

- Data silos preventing comprehensive analysis
- Technical integration complexity across legacy and modern systems
- Unclear or inconsistent ROI quantification methodologies

Cross-Cutting Recommendations

1. **Infrastructure Mindset:** Treat digital trust and verification as foundational infrastructure rather than compliance overhead, similar to how organizations view payment systems or network security.
2. **Dual Measurement Framework:** Implement metrics that capture both risk reduction benefits and growth enablement outcomes to present a complete value proposition.
3. **Standards Advocacy:** Champion interoperable standards at the national, jurisdictional and industry levels to reduce duplication, lower costs, and establish Canada's competitive advantage in the global digital trust economy.

04 Conclusion

The Montreal workshop demonstrated strong industry consensus around the strategic value of digital trust infrastructure for open banking and lending. While challenges remain in quantification, integration, and regulatory alignment, participants identified clear pathways forward through shared metrics, improved user experience, and coordinated advocacy for national standards.

The business case for digital trust and verification extends beyond fraud prevention to encompass growth enablement, operational efficiency, and competitive positioning. As Canada continues to develop its digital trust and verification ecosystem, the insights from this workshop provide a foundation for cross-sector collaboration and evidence-based investment in digital trust infrastructure.

For more information about DIACC's work on digital trust and verification, visit diacc.ca.