DIACC CCIAN

THREAT BRIEFING • APRIL 2026

The New Fraud Landscape.

Synthetic Identities, Deepfakes, and How Canada's Defences Must Evolve

FRAUD RESILIENCE & AI READINESS

STRATEGIC PILLAR 04

A DIACC Threat Briefing prepared for members, policymakers, and Canada's digital trust ecosystem.

diacc.ca | contact@diacc.ca

Table of Contents

DIACC THREAT BRIEFING

01

Purpose, Scope, and Methodology

SECTION 01 OF 10

1. Purpose, Scope, and Methodology

This threat briefing provides Canadian organizations with a clear, evidence-based picture of how artificial intelligence is transforming identity fraud. It focuses specifically on two threat categories that have escalated dramatically since 2023: synthetic identity fraud and deepfake-enabled attacks targeting identity verification, authentication, and transaction systems. The briefing assumes no prior expertise in AI-enabled fraud techniques and builds from foundational concepts to strategic implications.

Sections 2 through 6 present the threat landscape: the structural shifts driving AI-enabled fraud, the actors behind the attacks, and the methods they use. Section 7 shifts from a description of the threat to strategic analysis, examining why current defences are insufficient at the ecosystem level. Section 8 maps the resulting exposure by sector, and sections 9 and 10 address emerging threats and DIACC's planned response.

A companion document, Quick-Start Guide: Immediate Defences Against AI Identity Fraud, provides specific, low-cost actions for small and medium enterprises, professional firms, and other resource-constrained organizations.

It is intended for risk leaders, security executives, policy professionals, and senior decision-makers across all sectors of the Canadian economy — particularly those responsible for enterprise risk posture, vendor evaluation, identity verification strategy, and engagement with Canada's digital trust ecosystem.

Methodology and Sources

This briefing synthesizes published threat intelligence, empirical data, and standards analysis from the following source categories:

Canadian government sources.

The Canadian Centre for Cyber Security (CCCS) National Cyber Threat Assessment 2025–2026 [8] and Cyber Threats to Canada's Democratic Process: 2025 Update [15] provide the authoritative Canadian government assessment of AI-enabled threats. The Canadian Anti-Fraud Centre (CAFC) 2024 Annual Statistical Report [1] provides the primary data on Canadian fraud losses. These sources are publicly available and represent the official positions of the Government of Canada.

International government sources.

The U.S. Financial Crimes Enforcement Network (FinCEN) Alert FIN-2024-Alert004 [16] provides regulatory typologies and red flag indicators for AI-enabled identity fraud. NIST Special Publication 800-63-4 [18] and NIST AI 100-4 [19] provide the primary technical standards and references for synthetic content detection. The European Telecommunications Standards Institute (ETSI) TS 119 461 v2 [20] provides the EU identity proofing standard. These are official publications of their respective governments or standards bodies.

DIACC member research.

Primary data on Canadian fraud trends, attack vector evolution, and biometric fraud patterns is drawn from published reports by Equifax Canada [2], iProov [5] [6], and Entrust [4] [13]. Analysis of AI-enabled fraud projections, organizational cybersecurity readiness, and market impact is drawn from Deloitte 2024 [3], Ernst & Young 2025 [22], and Accenture 2025 [23]. These organizations are DIACC members. Their published research is cited because it represents the best available data on the threat vectors, organizational readiness gaps, and

financial consequences this briefing addresses; their membership in DIACC does not constitute endorsement of their products or services. Where member data is the sole source for a claim, this is noted.

International non-governmental sources.

The World Economic Forum [7] [10] [12] provides cross-jurisdictional threat analysis and case documentation.

Analytical approach.

This briefing distinguishes between three categories of statement:

- Reported data: Statistics and findings published by the sources above, cited directly. These are presented as reported, with source attribution.
- Assessed findings: Analytical judgements made by DIACC based on synthesis of multiple sources. These are identified with language such as "DIACC assesses" or "available evidence supports." Assessed findings represent DIACC's professional judgement and are open to challenge.
- Emerging projections: Forward-looking statements drawn from published projections by credible sources (e.g., Deloitte, WEF). These are attributed to their source and should not be treated as predictions with known confidence intervals.

This briefing does not draw on classified intelligence and does not make attribution claims beyond those published by the Canadian and allied governments. Organizations should verify time-sensitive findings against current CCCS advisories and sector-specific intelligence feeds.

DIACC THREAT BRIEFING

02

Executive Assessment

SECTION 02 OF 10

2. Executive Assessment

Bottom line: AI-driven identity fraud has moved from an emerging risk to an active, material threat to Canadian organizations across every sector. The tools are cheap, the attacks are scalable, and Canada's defence posture has structural gaps that individual institutional investment cannot close.

FIVE ASSESSED FINDINGS THAT DEFINE THE CURRENT LANDSCAPE

1. The scale is staggering and growing.

The Canadian Anti-Fraud Centre (CAFC) recorded $638 million in reported fraud losses in 2024, up from $577 million in 2023 and $531 million in 2022 [1]. However, only 5–10% of fraud is reported. DIACC estimates, based on the CAFC's own reporting rate guidance, that actual Canadian fraud losses may range from $6.4 billion to $12.8 billion annually — a figure that should inform enterprise risk committee assessments. Cumulative reported losses since 2021 now exceed $2 billion [1]. Equifax Canada data shows synthetic identity fraud in credit applications nearly tripled in a single year, rising from 2.8% to 8% between Q2 2023 and Q2 2024 [2]. Deloitte's Center for Financial Services projects that generative AI could, on its own, drive U.S. fraud losses to $40 billion by 2027 [3]. The financial consequences extend beyond direct fraud losses: EY's analysis of Russell 3000 companies found that firms experiencing a cyber incident typically see their stock price decline by 1.5% over the following 90 days, demonstrating sustained market impact beyond immediate recovery costs [22].

2. Deepfakes have become an industrial capability.

Entrust's Cybersecurity Institute documented a deepfake attempt every five minutes in 2024, with digital document forgeries increasing 244% year-over-year [4]. iProov recorded a 2,665% increase in virtual camera injection attacks and a 300% surge in face swap attacks, driven by a crime-as-a-service ecosystem of nearly 24,000 users selling attack technologies [5].

3. Available evidence strongly supports the conclusion that humans can no longer serve as the primary detection layer.

An iProov study found that only 0.1% of participants could correctly identify all deepfakes when presented with a mix of real and synthetic content [6]. The World Economic Forum noted that human ability to identify deepfakes hovers at just 55–60%, barely better than chance [7]. This has direct implications for any identity verification or transaction authorization process that relies on human visual or auditory review as a control.

4. Canada faces specific and documented threat dynamics.

The CCCS National Cyber Threat Assessment 2025–2026 identifies generative AI and deepfakes as accelerating threats to Canadian critical infrastructure, financial systems, and democratic processes [8]. In June 2025, Canadian authorities issued a joint advisory documenting a deepfake impersonation campaign that used AI-generated voice messages and messaging accounts impersonating senior government officials and prominent public figures to defraud Canadians [9].

5. DIACC assesses that Canada's current defence posture contains structural gaps that individual institutional investment cannot close.

Published threat assessments, standards frameworks, and vendor-specific detection capabilities have advanced significantly. However, DIACC's analysis identifies three systemic weaknesses — fragmented threat intelligence, standards without Canadian implementation guidance, and absent cross-sector identity assurance interoperability — that require ecosystem-level coordination to address. These gaps are examined in Section 7.

DIACC THREAT BRIEFING

03

The Structural Shift: AI as a Fraud Accelerant

SECTION 03 OF 10

3. The Structural Shift: AI as a Fraud Accelerant

The identity fraud threat has undergone a structural transformation. Three converging developments have fundamentally altered the economics and capabilities available to threat actors.

3.1 The Cost of Fraud Has Collapsed

Generative AI has reduced the time, cost, and skill required to produce convincing synthetic content by orders of magnitude. Identity documents that once required specialized skills to fake can now be generated in seconds. Entrust's 2026 data shows that digital methods now account for a substantial share of identity document fraud, with digital forgeries representing 35% and digital counterfeits a further 9% of all document fraud attempts, while physical counterfeits remain the single largest category at 47% and physical forgeries account for the remaining 10% [13]. The sustained prevalence of digital methods reflects the accessibility of generative AI and open-source editing tools, which have collapsed the cost and skill required to produce convincing forgeries at scale. Arup's Chief Information Officer, Rob Greig, told the World Economic Forum that he created a real-time deepfake of himself using open-source software in approximately 45 minutes [10].

3.2 Attacks Have Gone Real-Time

The most dangerous shift is from static deception to real-time manipulation. Threat actors can now generate convincing deepfake videos during live verification sessions, clone voices from seconds of reference audio, inject synthetic media directly into device data streams using virtual cameras, and operate multiple synthetic identities simultaneously across institutions.

The severity of this shift was demonstrated in early 2024 when a finance employee at multinational engineering firm Arup was manipulated into wiring $25.6 million to fraudsters after joining a video call in which every other participant, including purported senior executives, was an AI-generated deepfake. Hong Kong police confirmed that the attackers used publicly available video and audio of the executives to generate the synthetic impersonations [10] [11].

3.3 Crime Has Been Industrialized

iProov's Threat Intelligence Report 2025 documents an online crime-as-a-service ecosystem of nearly 24,000 users selling identity fraud attack technologies [5]. These marketplaces offer synthetic identity generation tools, face-swap and injection attack software, dark web tutorials and technical support, and money mule networks for laundering proceeds. Entrust reports that it has identified 53 unique fraud rings since 2023, including four that have targeted multiple clients across different sectors, with defined roles spanning recruiters, organizers, enforcers, and technical specialists [13].

The World Economic Forum reports that AI fraud agents, combining generative AI, automation frameworks, and reinforcement learning, can now create synthetic identities, interact with verification systems in real time, and adjust behaviour based on outcomes. These agents are projected to become mainstream within 18 months, particularly in organized fraud networks [12].

DIACC THREAT BRIEFING

04

Canada Under Pressure: The Domestic Threat Picture

SECTION 04 OF 10

4. Canada Under Pressure: The Domestic Threat Picture

4.1 The Numbers

INDICATOR	DATA	SOURCE
Reported fraud losses (Canada, 2024)	$638 million (5–10% reporting rate)	CAFC [1]
Estimated actual fraud losses (Canada, 2024)	$6.4–$12.8 billion (DIACC estimate)	DIACC analysis of CAFC data [1]
Cumulative reported losses since 2021	Over $2 billion	CAFC [1]
Fraud reports received (2024)	108,878 reports; at least 34,621 victims	CAFC [1]
Identity fraud as % of flagged credit applications	48.4%, up from 43.2% YoY	Equifax Canada [2]
Synthetic identity fraud in credit applications	2.8% → 8% in one year (nearly tripled)	Equifax Canada [2]
Deepfake attempt frequency (global)	Once every five minutes	Entrust [4]
Digital document forgery growth (2024)	244% YoY	Entrust [4]
Document fraud type distribution (Sep 2024–Sep 2025)	Physical counterfeit 47%; digital forgery 35%; physical forgery 10%; digital counterfeit 9%	Entrust [13]
Deepfakes as % of biometric fraud attempts	1 in 5 (2025)	Entrust [13]
Injection attack growth	2,665% increase in virtual camera attacks	iProov [5]
Injection attack growth (corroborating)	~40% YoY increase in suspected rate	Entrust [13]
Face swap attack growth	300% increase vs. 2023	iProov [5]
iOS injection attack growth (H2 2025)	1,151% surge	iProov [24]
iOS injection attack growth (annual)	741% increase	iProov [24]
Regional attack concentration (Q3 2025)	Southeast Asia: 720% spike	iProov [24]
Human deepfake detection accuracy	0.1% correctly identify all deepfakes	iProov [6]
Projected generative AI fraud losses (U.S.)	$40 billion by 2027 (Deloitte projection)	Deloitte [3]

4.2 The Canadian Regulatory Landscape

Canadian organizations operate within an evolving but incomplete regulatory framework:

- PIPEDA / proposed CPPA require security safeguards proportionate to data sensitivity, but provide no specific guidance on AI-generated identity threats.
- Proposed AIDA would impose fines up to C$25 million or 5% of global revenue for AI safety non-compliance, but implementation details remain under development.
- Critical Cyber Systems Protection Act addresses critical infrastructure security obligations but lacks identity-specific AI threat guidance.
- OSFI/FINTRAC obligations impose financial sector compliance requirements that synthetic identity fraud directly threatens, yet sector-specific implementation guidance for AI-enabled fraud is lacking.
- Provincial digital identity programmes (BC Services Card at 4.6M users, Ontario, Quebec, Alberta) are scaling digital credential ecosystems that must be resilient against synthetic identity exploitation.

The CCCS's Cross-Sector Cyber Security Readiness Goals provide 36 foundational goals for Canadian organizations, but do not address the specific synthetic identity and deepfake threat vectors at the operational specificity required by organizations [8].

DIACC's Pan-Canadian Trust Framework (PCTF) provides a conformance framework for digital identity verification in Canada, with production-scale adoption demonstrated in the legal sector, where members reported over 700,000 client identity verification transactions between October 2023 and October 2024 [14] [17].

DIACC THREAT BRIEFING

05

Threat Actor Landscape

SECTION 05 OF 10

5. Who Is Behind the Attacks: Threat Actor Landscape

5.1 Organized Criminal Networks

Assessed threat trajectory: Increasing.

The primary driver of synthetic identity fraud in Canada. These operations run at an industrial scale with specialized roles: identity fabricators, document forgers, account openers, money mules, and cash-out operators. They increasingly use "sleeper" tactics, cultivating synthetic identities over months or years to build credit history before executing coordinated bust-out schemes. Equifax Canada data confirms that synthetic identity cultivation patterns are detectable but require specific analytics capabilities that many Canadian organizations have not yet deployed [2].

DIACC assesses that the threat from organized criminal networks deploying synthetic identities against Canadian financial institutions is increasing, driven by the availability of crime-as-a-service infrastructure documented in Section 3.3 and the cultivation lag that delays detection until monetization.

5.2 State-Sponsored Actors

Assessed threat trajectory: Increasing, with expanding scope.

The CCCS assesses that China, Russia, Iran, and North Korea have incorporated AI-generated deepfakes into their cyber operations targeting Canada [8]. The CCCS democratic process assessment documented deepfake use across at least 151 elections assessed between 2023 and 2024, including deepfake pornography used to harass women politicians and 2SLGBTQI+ identifying persons in politics [15]. In June 2025, Canadian authorities documented a deepfake impersonation campaign that used AI-generated voice messages and messaging accounts impersonating senior government officials and prominent public figures to defraud Canadians, specifically for financial fraud [9].

These actors are also using AI to process massive datasets collected on Canadian politicians, public figures, and diaspora communities, producing intelligence that enables more targeted and convincing social engineering [8] [15].

DIACC assesses that state-sponsored use of AI-enabled identity manipulation against Canadian targets is expanding beyond traditional espionage and influence operations into direct financial fraud, representing a convergence of state and criminal threat vectors.

5.3 Fraud-as-a-Service Operators

Assessed threat trajectory: Increasing, with barriers to entry lowering.

A growing intermediary layer between tool developers and end-user fraudsters. These operators provide the infrastructure, synthetic identity packages, injection-attack software, face-swap tools, and money-laundering networks that enable low-skilled actors to execute sophisticated fraud. The World Economic Forum describes this as a maturation from widespread, low-skill fraud to fewer, more coordinated, and more technologically advanced operations [12].

DIACC assesses that this intermediary layer is the single most important structural enabler of the growth of AI-driven identity fraud because it decouples attack sophistication from attacker skill. The implication for Canadian organizations is that threat modelling based on assumed attacker capability is increasingly unreliable — the capability available to even unsophisticated actors now exceeds the detection threshold of many deployed identity verification systems.

5.4 Opportunistic Individuals

Assessed threat trajectory: Increasing by volume, stable by sophistication.

The fastest-growing category by volume. Consumer-grade generative AI tools enable individuals with no technical expertise to create fraudulent documents, clone voices, and generate synthetic photographs. Equifax Canada data show that first-party fraud, in which individuals falsify their own information, remains the most prevalent form of fraud in Canadian automotive lending, and that these actors are increasingly turning to AI tools to make their deception more convincing [2].

DIACC THREAT BRIEFING

06

Vectors and Methods

SECTION 06 OF 10

6. How the Attacks Work: Vectors and Methods

6.1 Synthetic Identity Creation

Synthetic identities combine stolen real personal information (Social Insurance Numbers, dates of birth, addresses) with AI-generated fabricated elements (names, photographs, documents). The result is an identity that passes conventional verification checks because some of its components are genuine.

AI has transformed every element of this process. Generative AI tools produce identity documents with realistic formatting, security features, and machine-readable zones. Generative Adversarial Network (GAN)-generated facial photographs are indistinguishable from real images. Financial documents (pay stubs, bank statements, tax records) can be created entirely from scratch, with no source. FinCEN's analysis of suspicious activity reports found that financial institutions often detect AI-generated identity documents by re-reviewing account-opening documents rather than during initial verification [16].

6.2 Identity Proofing Bypass

Identity proofing — the process of establishing that an applicant is who they claim to be — is now the primary attack surface globally. Entrust's 2026 Identity Fraud Report confirms that deepfakes account for one in five biometric fraud attempts, with deepfaked selfies increasing 58% year-over-year [13]. Deepfake attacks are concentrated in high-risk financial services sectors: cryptocurrency platforms absorb 60% of deepfake fraud, digital-first banks 22%, and payments and merchant services 13% [13].

The most dangerous attack vector is digital injection, in which attackers use virtual cameras or software manipulation to insert synthetic media directly into the verification data stream, bypassing the physical camera entirely. iProov documented a 2,665% increase in this attack type, driven partly by injection tools infiltrating mainstream app stores [5]. iProov's 2026 threat intelligence data shows the attack surface is also shifting by platform: injection attacks targeting iOS devices surged 1,151% in the second half of 2025, contributing to a 741% annual increase [24]. This platform shift erodes the long-held assumption that iOS offered structural resistance to injection attacks and requires Canadian organizations that rely on device-based liveness signals to revisit platform-specific risk assumptions.

Face swap attacks have surged 300%, with threat actors specifically adapting their tools to defeat systems that use liveness detection, indicating an adversarial arms race in which attackers target the specific defences organizations deploy [5].

6.3 Real-Time Impersonation

Deepfakes are no longer pre-recorded. Threat actors conduct live, interactive impersonation during video calls, voice authentication sessions, and remote verification processes. Voice cloning requires only seconds of reference audio: readily available from corporate websites, conference recordings, and social media. The World Economic Forum confirmed that deepfake-related fraud losses exceeded $200 million in Q1 2025 alone [7].

6.4 Monetisation

Synthetic identities and deepfakes enable a spectrum of financial crimes documented in FinCEN's November 2024 alert [16]: fraudulent account opening, credit bust-out schemes, authorized push payment fraud, benefits and loan fraud, and money mule recruitment using AI-generated personas.

DIACC THREAT BRIEFING

07

The Defence Gap: Why Current Protections Are Failing

SECTION 07 OF 10

7. The Defence Gap: Why Current Protections Are Failing

Canadian organizations, particularly financial institutions, are not standing still. Major banks are investing heavily in biometric fraud detection, transaction monitoring, and identity verification technology. Credit bureaus have deployed synthetic identity flagging capabilities. Payment processors have upgraded authentication requirements. These investments are real and have produced measurable improvements in detection rates for known fraud typologies.

However, these investments are occurring against a global backdrop of significant unpreparedness: Accenture's survey of over 2,200 cybersecurity executives found that 90% of organizations globally are not adequately prepared to secure their AI-driven operations, with 77% lacking essential data and AI security practices [23].

The gap is not in detection investment. DIACC's analysis identifies three structural areas where individual institutional investment cannot substitute for ecosystem-level coordination.

7.1 Fragmented Threat Intelligence

The CCCS National Cyber Threat Assessment, FinCEN alerts, and vendor threat reports all contribute to the overall picture. No single resource synthesizes them into a unified, Canadian-contextualized threat model with actionable implementation guidance. A financial institution's fraud team can subscribe to multiple intelligence feeds, but translating those feeds into calibrated controls that align with Canadian regulatory expectations requires a coordination layer that currently does not exist.

This briefing is itself an attempt to address part of this gap by synthesizing government, vendor, and international sources into a coherent Canadian threat picture. However, a point-in-time briefing is not a substitute for an ongoing, structured threat intelligence function serving the Canadian digital trust ecosystem.

7.2 Standards Without Canadian Implementation Guidance

Standards have advanced significantly, but a critical implementation gap remains — and it is particularly acute in Canada.

Internationally, NIST SP 800-63-4 (July 2025) is the first major identity assurance framework to mandate controls for deepfakes and injection attacks at IAL2 and above [18]. It tells organizations which controls are required, but not how to deploy, configure, and operationalize them in the Canadian regulatory and operational context. NIST AI 100-4 provides the most comprehensive technical reference on synthetic content detection, but explicitly acknowledges that most approaches are years from widespread deployment [19].

The European standard is emerging but not directly applicable. ETSI TS 119 461 v2 (February 2025) defines rigorous identity proofing requirements, including liveness and injection-attack defences [20]. CEN TS 18099 establishes the European standard for testing injection attack detection. These are technically important but designed for the EU regulatory context.

Canada does not have a domestic identity assurance standard comparable in scope to NIST SP 800-63-4. The existing Canadian guidance, the Communications Security Establishment's ITSP.30.031 v3, is aligned to the earlier NIST SP 800-63-2 and predates the generative AI threat landscape entirely. This means Canadian

organizations seeking to implement deepfake and injection-attack defences must interpret U.S. or EU frameworks without Canadian regulatory mapping, sector-specific adaptation, or conformance criteria designed for the Canadian operational environment. DIACC assesses this as a significant gap that increases both implementation cost and compliance risk for Canadian organizations.

7.3 Interoperability and Cross-Sector Coordination

The most significant gap is not within individual institutions but between them. Synthetic identity fraud is inherently cross-institutional — a fabricated identity that opens an account at one bank, builds credit history through another, and monetizes through a third, exploiting the absence of shared identity assurance across the ecosystem. Individual investment in detection technology, no matter how substantial, cannot close this gap without common standards for identity-verification assurance, shared indicators of synthetic-identity compromise, and cross-sector interoperability that enables identity verification conducted in one context (e.g., legal) to be trusted in another (e.g., financial services).

No Canadian mechanism currently exists to provide this interoperability at scale. The PCTF conformance framework demonstrates that cross-sector identity verification trust is technically achievable; production-scale deployment in the legal sector confirms this [17]. However, extending this model across financial services, healthcare, government, and telecommunications requires deliberate ecosystem coordination that no single institution can undertake alone.

DIACC THREAT BRIEFING

08

What Is at Stake: Sector-Specific Exposure

SECTION 08 OF 10

8. What Is at Stake: Sector-Specific Exposure

The structural defence gaps identified in Section 7 create differentiated exposure across Canadian economic sectors. The following analysis maps primary threat vectors to sector-specific risk factors in Canada.

SECTOR	PRIMARY THREAT VECTORS	CANADIAN-SPECIFIC RISK FACTORS
Financial Services	Synthetic identity account opening; credit bust-out; deepfake-authorized payments; AML evasion	OSFI/FINTRAC obligations; open banking expansion; Payments Canada integrity; credit union exposure
Legal	Remote client identity verification fraud; trust account exploitation; deepfake impersonation for conveyancing fraud	700K+ remote IDV transactions reported by members [17]; expanding remote practice; passports account for 44% of fraudulent documents submitted in the professional services sector globally [13]
Healthcare	Patient identity fraud; prescription fraud; benefits fraud; health data access	Provincial health card verification; Canada Health Infoway standards; health privacy legislation
Government	Benefits fraud; synthetic identity for credential issuance; election interference; citizen service exploitation	Provincial digital ID programmes (BC: 4.6M users); federal service delivery; democratic process integrity
Telecommunications	SIM swap fraud; subscriber identity fraud; account takeover; deepfake customer service manipulation	Telcos as identity verification anchor for other sectors; CRTC requirements
Energy / Critical Infrastructure	Insider identity compromise; SCADA/OT access via identity exploitation; supply chain identity fraud	CCCS critical infrastructure designation; CI protection legislation; OT/IT convergence

Threat vector distribution by sector. Entrust's global identity verification network data show that new account fraud and account takeover (ATO) fraud are concentrated differently across sectors. New account fraud dominates in contexts where upfront incentives or rapid onboarding are offered: 67% of fraud attempts in crypto occur during onboarding, and 64% of professional services fraud is new account fraud. Account takeover fraud dominates where accounts hold long-term value: 82% of payments-sector fraud and 55% of digital-first bank fraud occur after onboarding [13]. Canadian organizations should calibrate control investment to the dominant vector in their sector — onboarding-stage controls for high-incentive businesses, post-onboarding monitoring and authentication controls for high-value account environments.

> **Cyber insurance coverage gap.**

All organizations, regardless of sector, should review their cyber insurance coverage. Many standard policies exclude losses when an employee "voluntarily" initiates a transfer, even when a deepfake impersonation induces that action. Organizations should verify that their policies specifically cover social engineering, funds transfer fraud (FTF), and AI-enabled impersonation scenarios. This coverage gap represents a material uninsured risk for organizations that have not recently audited their policies.

8.1 Immediate Actions for Resource-Constrained Organizations

DIACC has developed a standalone companion document, Quick-Start Guide: Immediate Defences Against AI Identity Fraud, providing eight specific, low-cost actions that small and medium enterprises, professional firms, and resource-constrained organizations can deploy within days. The Quick-Start Guide covers mandatory call-back verification, cooling periods, dual authorization, pre-shared authentication keys, phishing-resistant authentication capabilities, email domain authentication, physical-first onboarding, and cyber insurance audit guidance.

DIACC THREAT BRIEFING

09

What Comes Next: Emerging Threats on the Horizon

SECTION 09 OF 10

9. What Comes Next: Emerging Threats on the Horizon

Organizations should plan for the following developments over the next 12–24 months:

Autonomous AI fraud agents. The World Economic Forum projects that AI agents combining generative AI, automation, and reinforcement learning will autonomously create synthetic identities, interact with verification systems, and adapt based on outcomes [12]. These agents will operate at machine speed, potentially overwhelming manual review processes. DIACC assesses that this represents the most significant near-term escalation of the threat landscape, because it removes the human bottleneck that currently limits the throughput of sophisticated fraud operations.

Real-time multimodal deepfakes. Current deepfakes typically target a single modality (face, voice, or document). Convergence toward simultaneous face-voice-document deepfaking during live interactions will challenge defences that rely on cross-modal consistency checks. No published Canadian or international standard currently addresses the requirements for multimodal deepfake detection.

Deepfake attacks on digital credential ecosystems. As Canada and the EU scale verifiable credential and digital wallet infrastructure, threat actors will target the issuance, presentation, and revocation processes. Compromised issuers, cloned wallets, and synthetic credential presentation are emerging threat vectors for systems that are still being designed. Organizations involved in credential ecosystem design should incorporate adversarial threat modelling from the outset rather than retrofitting defences.

AI-powered insider threats. Deepfake technology enables impersonation of internal employees to escalate privileges, exfiltrate data, and manipulate identity governance systems. Organizations with remote workforces are particularly exposed.

Deepfake impersonation in enterprise workflows. iProov's 2026 threat intelligence reports that deepfake impersonation is expanding within enterprises across everyday corporate workflows, particularly video-based interactions [24]. The Arup case documented in Section 3.2 is no longer an outlier; routine video meetings, approval calls, and internal verification conversations are becoming viable attack surfaces. Canadian organizations should assume that any video-mediated workflow authorizing payment, access, or decision-making is within the threat envelope, and should deploy out-of-band verification controls for material transactions regardless of the apparent seniority or familiarity of the person on the call.

Deepfake-enabled recruitment fraud. AI-generated identities, synthetic resumes, and live deepfake video interviews are being used to place fraudulent candidates inside target organizations, enabling downstream data theft, malware introduction, and financial fraud. Entrust reports that recruitment is now among the most-targeted non-financial sectors, and Gartner projects that one in four job applicants globally will be fake by 2028 [13]. Canadian organizations with distributed or remote hiring processes — particularly those onboarding contractors, technical staff, or privileged-access roles without in-person verification — should treat hiring as an identity-assurance control point rather than solely an HR process.

Regulatory acceleration. The EU AI Act's phased implementation (2025–2026), Canada's proposed Artificial Intelligence and Data Act (AIDA), and evolving provincial digital identity legislation will create new compliance

obligations. Organizations that invest proactively in synthetic identity and deepfake defences will be better positioned as requirements crystallize.

DIACC THREAT BRIEFING

10

DIACC's Planned Response

SECTION 10 OF 10

10. DIACC's Planned Response

This threat briefing is the first in a series of resources DIACC is developing under the Fraud Resilience & AI Readiness pillar of its 2025–2030 Strategic Framework. Planned resources include an Implementation Guide for Managing AI Threat Vectors: Synthetic Identities & Deepfakes, which provides controls mapped to PCTF conformance criteria and NIST SP 800-63-4; a PCTF Conformance Criteria Addendum for AI-supported identity verification; and Sector-Specific Resources, beginning with financial services and legal.

Get Involved

DIACC invites member organizations and partners to review and respond to this briefing, contribute threat intelligence and implementation experience to strengthen the evidence base, and engage with the Trust Framework Expert Committee (TFEC) in developing conformance criteria. Contact: contact@diacc.ca

References

[1] Canadian Anti-Fraud Centre, 2024 Annual Statistical Report and Fraud Prevention Month 2025. $638 million in reported losses in 2024 (up from $577M in 2023, $531M in 2022); 108,878 reports received; at least 34,621 victims; 5–10% reporting rate. Cumulative reported losses since 2021 exceed $2 billion. Government of Canada.
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.html

[2] Equifax Canada, H1 2024 Market Pulse Fraud Trends, September 2024. Synthetic identity fraud rose from 2.8% to 8% of credit applications between Q2 2023 and Q2 2024. Identity fraud: 48.4% of all flagged fraudulent applications, up from 43.2%. (DIACC member)
https://assets.equifax.com/marketing/canada/assets/reports_white_papers/h1-2024-fraud-trends-en.pdf

[3] Deloitte Center for Financial Services, Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking, 2024. Projects AI-enabled fraud to reach $40 billion annually by 2027 in the United States. As cited by the World Economic Forum and UNESCO. (DIACC member)
https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

[4] Entrust Cybersecurity Institute, 2025 Identity Fraud Report, November 2024. Deepfake attempts occurred every 5 minutes in 2024; digital document forgeries increased 244% YoY; digital forgeries now account for 57% of all document fraud. (DIACC member)
https://www.entrust.com/company/newsroom/deepfake-attacks-strike-every-five-minutes-amid-244-surge-in-digital-document-forgeries

[5] iProov, Threat Intelligence Report 2025: Remote Identity Under Attack, February 2025. Native virtual camera attacks increased 2,665%; face swap attacks surged 300%; crime-as-a-service ecosystem of nearly 24,000 users. (DIACC member)
https://www.iproov.com/reports/threat-intelligence-report-2025

[6] iProov, Deepfake Consumer Study, February 2025. Only 0.1% of 2,000 UK and US consumers correctly identified all deepfake and real stimuli. (DIACC member)
https://www.iproov.com/blog/deepfakes-statistics-solutions-biometric-protection

[7] World Economic Forum, "Detecting dangerous AI is essential in the deepfake era," July 2025. Human deepfake detection accuracy at 55–60%; over $200 million in confirmed deepfake-related fraud losses in Q1 2025 alone. (Non-profit)
https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/

[8] Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025–2026, October 2024. Identifies AI-enhanced disinformation, deepfakes, and state-sponsored cyber threats as accelerating risks. Cross-Sector Cyber Security Readiness Goals: 36 foundational goals. (Government of Canada; DIACC member)
https://www.canada.ca/en/communications-security/news/2024/10/canadian-centre-for-cyber-security-releases-national-cyber-threat-assessment-2025-2026.html

[9] Canadian Anti-Fraud Centre / CCCS, Joint Advisory: Deepfake Impersonation Campaign Targeting Canadians, June 2025. Documented AI-generated voice messages and messaging accounts impersonating senior government officials and prominent public figures, used in financial fraud targeting Canadians. (Government of Canada)
https://antifraudcentre-centreantifraude.ca/news-nouvelles/2025/2025-06-23-eng.htm

[10] World Economic Forum, "Cybercrime: Lessons learned from a $25m deepfake attack," February 2025. Interview with Arup CIO Rob Greig on the $25.6 million deepfake fraud case. Greig created a deepfake of himself in 45 minutes using open-source software. (Non-profit)*https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/*

[11] Hong Kong Police Force, press briefing, February 2024. Confirmed that AI-generated deepfakes were used to impersonate the CFO and colleagues of a multinational firm, resulting in $25.6 million (HK$200 million) in fraudulent transfers. No direct URL available; incident reported by World Economic Forum [10]. (Government)

[12] World Economic Forum, "How identity fraud is changing in the age of AI," December 2025. Documents the rise of AI fraud agents combining generative AI, automation, and reinforcement learning. Projects these agents could become mainstream within 18 months. Multi-step fraud attacks rose 180% YoY. (Non-profit)
https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/

[13] Entrust Cybersecurity Institute, 2026 Identity Fraud Report, November 2025. Deepfakes account for 1 in 5 biometric fraud attempts; deepfaked selfies increased 58%; injection attacks surged 40% YoY. (DIACC member)
https://www.entrust.com/company/newsroom/deepfakes-social-engineering-and-injection-attacks-on-the-rise

[14] DIACC, AI Consultation Submission to the Federal Government, October 2025. Policy position calling for recognition of identity, authentication, verification, and trust-framework services as critical infrastructure to underpin secure and trustworthy AI ecosystem scaling. DIACC Strategic Framework 2025–2030: targets 50% reduction in fraud losses by 2031. (DIACC)
https://diacc.ca/2025/11/03/diacc-ai-consultation-submission-to-the-federal-government/

[15] CCCS, Cyber Threats to Canada's Democratic Process: 2025 Update. Assessed 151 elections (2023–2024); at least 6 had deepfake harassment of politicians. Deepfake pornography targeting women and 2SLGBTQI+ identifying persons. State actors using AI to process datasets on Canadian politicians and diaspora communities. (Government of Canada)
https://www.cse-cst.gc.ca/en/information-resources/news/communications-security-establishment-canada-releases-2025-update-report-cyber-threats-canadas-democratic-process

[16] FinCEN, FIN-2024-Alert004: Fraud Schemes Involving Deepfake Media, November 13, 2024. Red flag indicators for financial institutions; SAR reporting requirements; typologies including fraudulent account opening and synthetic identity fraud. (U.S. Government)
https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial

[17] DIACC, PCTF Legal Professionals Profile Final Recommendation V1.1, October 2025. PCTF-certified identity verification providers in the legal sector include Chicago Title, FCT, Treefort Technologies, and Vaultie (all LOA2, Verified Person Component). Over 700,000 client identity verification transactions were reported by members across multiple vendors, Oct 2023–Oct 2024. (DIACC)
https://diacc.ca/2025/09/22/the-diacc-releases-its-pctf-legal-professionals-profile-final-recommendation-v1-1/

[18] NIST Special Publication 800-63-4, Digital Identity Guidelines, July 2025. First major framework to mandate controls for injection attacks and deepfakes at IAL2 and above. (U.S. Government)*https://pages.nist.gov/800-63-4/*

[19] NIST AI 100-4, Reducing Risks Posed by Synthetic Content, November 2024. Technical reference for detection, watermarking, provenance tracking. Acknowledges most approaches years from widespread deployment. (U.S. Government)
https://www.nist.gov/publications/reducing-risks-posed-synthetic-content-overview-technical-approaches-digital-content

[20] ETSI TS 119 461 v2, February 2025. Identity-proofing requirements, including liveness detection and defences against injection attacks. Two Levels of Identity Proofing (Baseline and Extended). (European standards body)*https://www.signicat.com/blog/etsi-119-461-v2-1-1-updates-you-need-to-know*

[21] iProov, November 2025. First and only vendor independently certified against NIST SP 800-63-4 biometric verification requirements via CEN TS 18099 Level 2 testing by Ingenium Biometrics. (DIACC member)
https://www.iproov.com/press/nist-digital-identity-requirements-first-biometrics-vendor-demonstrating-deepfake-resilience

[22] Ernst & Young LLP, 2025 EY Cybersecurity Study: Bridging the C-suite Disconnect, April 2025. Survey of 800 US C-level executives. A separate EY analysis of Russell 3000 companies found that those experiencing a cyber incident typically see their stock prices decrease by 1.5% over the following 90 days. (DIACC member
)*https://www.ey.com/en_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds*

[23] Accenture, State of Cybersecurity Resilience 2025, June 2025. Survey of 2,286 cybersecurity and technology executives across 17 countries. 90% of organizations are not adequately prepared to secure their AI-driven future; 77% lack essential data and AI security practices. (DIACC member)
https://newsroom.accenture.com/news/2025/only-one-in-10-organizations-globally-are-ready-to-protect-against-ai-augmented-cyber-threats

[24] iProov, Threat Intelligence Report 2026. Injection attacks targeting iOS devices surged 1,151% in H2 2025, contributing to a 741% annual increase; deepfake impersonation expanding across enterprise video-based workflows; Southeast Asia experienced a 720% spike in attacks in Q3 2025. (DIACC member)
https://www.iproov.com/reports/threat-intelligence-report-2026

Appendix A: DIACC Ecosystem References

The threat briefing body (Sections 1–10) is vendor-neutral. This appendix summarizes the capabilities offered by DIACC member organizations whose published research contributed to the threat intelligence in this briefing, as well as PCTF-certified providers referenced in the analysis.

Accenture · **PROFESSIONAL SERVICES & ADVISORY**
Professional services and cybersecurity advisory firm. Contributed analysis on global organizational cybersecurity readiness through its State of Cybersecurity Resilience 2025 report [23].

Chicago Title · **PCTF-CERTIFIED PROVIDER**
PCTF-certified identity verification provider. Certified at LOA2 under the PCTF Verified Person Component [17].

Deloitte · **PROFESSIONAL SERVICES & ADVISORY**
Global professional services firm providing leading audit, tax, consulting and advisory services. Contributed projections on generative AI fraud losses ($40 billion by 2027 in the U.S.) through its Center for Financial Services report in 2024 [3]. Deloitte Canada provides risk, regulatory & forensics services, cybersecurity, Gen AI and more.

Entrust · **IDENTITY VERIFICATION & CYBERSECURITY**
Identity verification and cybersecurity platform provider. Contributed global data on document forgery, deepfake frequency, and sector-specific fraud trends through its Cybersecurity Institute annual reports [4] [13]. Offers integrated identity verification, authentication, and lifecycle management capabilities, including deepfake detection.

Equifax Canada · **CREDIT BUREAU & FRAUD ANALYTICS**
Credit bureau and fraud analytics provider. Contributed Canadian-specific fraud trend data to this briefing, including synthetic identity fraud rates, sector-specific fraud analysis, and credit application fraud metrics [2]. Offers FraudIQ analytics for fraud detection and prevention during onboarding.

Ernst & Young · **PROFESSIONAL SERVICES & ADVISORY**
Professional services and cybersecurity advisory firm. Contributed analysis on the financial impact of cybersecurity incidents on publicly traded companies through its 2025 Cybersecurity Study [22].

FCT · **PCTF-CERTIFIED PROVIDER**
PCTF-certified identity verification provider (technology partnered with Bluink). Certified at LOA2 under the PCTF Verified Person Component. Deployed at production scale in the Canadian legal sector [17].

iProov · **BIOMETRIC VERIFICATION**
Biometric verification and liveness detection provider. Contributed injection attack and face swap trend data through its Threat Intelligence Report 2025 [5], Threat Intelligence Report 2026 [24], and consumer deepfake detection research [6]. Independently certified against NIST SP 800-63-4 biometric verification requirements via CEN TS 18099 Level 2 testing by Ingenium Biometrics [21]. Operates the iProov Security Operations Centre (iSOC), providing real-time threat intelligence on biometric attack vectors.

Treefort Technologies · **PCTF-CERTIFIED PROVIDER**
Treefort is SOC 2 Type II compliant across all five trust criteria and is a PCTF-certified identity verification provider, certified at LOA2 under the PCTF Verified Person Component. The platform uses a layered, multi-factor approach, triangulating data across more than 1,750 authentication data points from trusted sources rather than relying on a single verification method [17].

Vaultie · **PCTF-CERTIFIED PROVIDER**
PCTF-certified identity verification provider. Certified at LOA2 under the PCTF Verified Person Component and LOA3 under the PCTF Digital Wallet Component [17].

Research Note: This briefing was developed using Anthropic's Claude AI as a research and drafting tool. Claude was used to identify, retrieve, and synthesize publicly available data from government, academic, and industry sources. All statistics were independently verified against primary sources, and the final analysis and editorial judgments reflect DIACC staff review. Source URLs are provided for independent verification.

DIACC — Where Digital Trust Means Business.