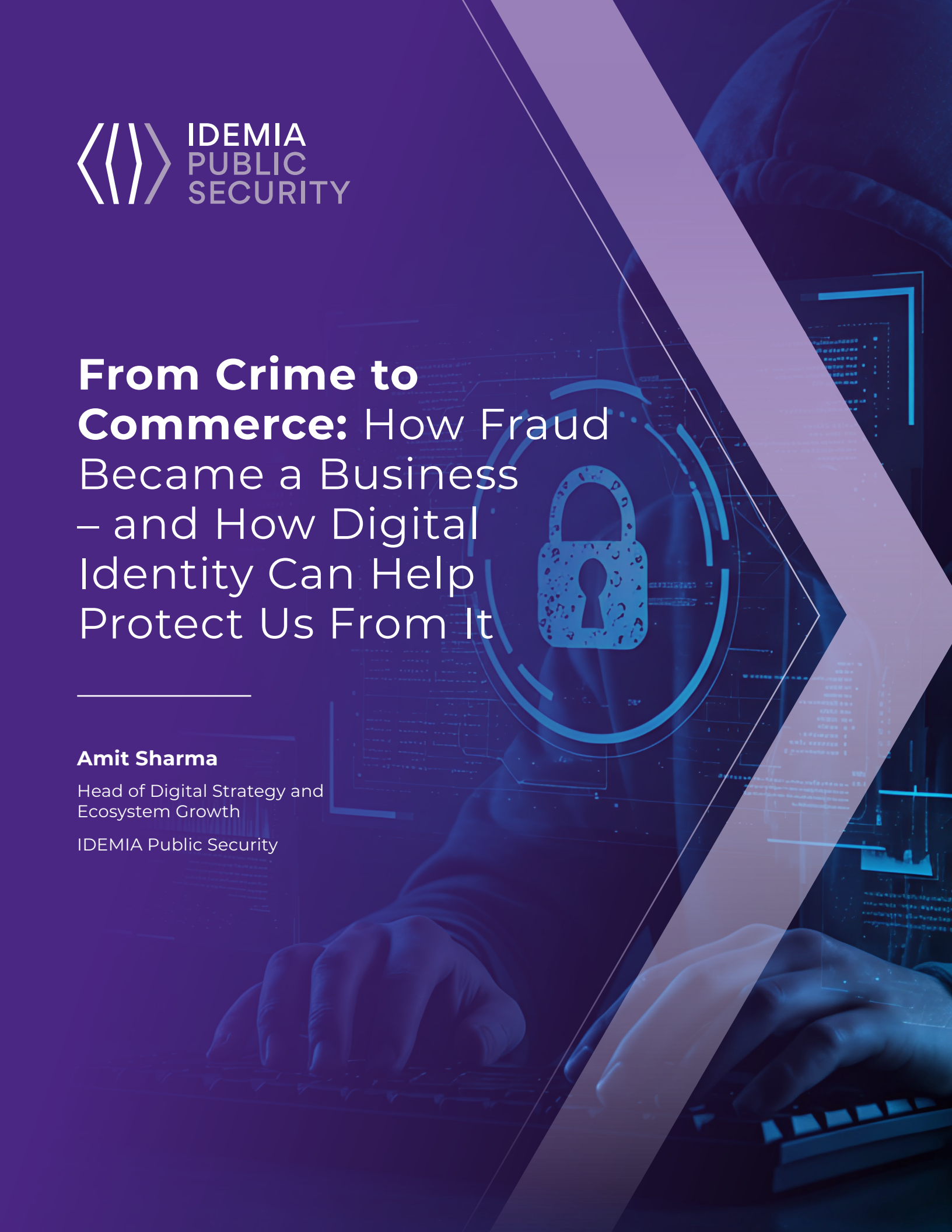
IDEMIA PUBLIC SECURITY

From Crime to Commerce: How Fraud Became a Business – and How Digital Identity Can Help Protect Us From It



Amit Sharma

Head of Digital Strategy and Ecosystem Growth

IDEMIA Public Security

2

Fraud's Structural Transformation

For decades, fraud has been understood as a largely opportunistic, person-to-person crime. Attackers target an individual, often by exploiting a moment of trust that can exploit a data weakness, extract exploitable information or relevant value, and move on.

That model no longer holds.

Today, fraud has evolved into a repeatable, scalable business service, driven by digital platforms, global connectivity, and, increasingly, by artificial intelligence scouring the Internet for the activity signals and personal data we all share for seemingly every transaction. What once required human skill, proximity, and patience has become industrialized, automated, and optimized like any other online enterprise.

In the United States alone, consumer-reported fraud and identity theft losses exceeded $12.5–$12.7 billion in 2024, a nearly 25% year-over-year increase, while total reports rose to 6.5 million, up 20% in a single year. Identity theft reports increased nearly 10% year-over-year, and losses have grown at a compounding rate of roughly 27% annually since 2021, signaling a structural escalation rather than a temporary spike.

What is driving this transformation is not simply "more crime," but a fundamental change in the economics of fraud reflecting the realities of what makes fraud easier and profitable. Digital channels, remote engagement, and large-scale identity exposure have created an environment in which fraudsters can operate like software companies: sourcing identities, automating attacks, iterating tactics, and monetizing at scale. A new cottage industry has emerged - fraud-as-a-service – and identity is the raw material that fuels it.

Identity Compromise + Artificial Intelligence = Fraud-as-a-Service

At the center of modern fraud is identity – and this is not just stolen data; it's compromised trust. Names, social security numbers, login credentials, employee roles, student status, and account access are among the many identity-related attributes that are now widely available through breaches, leaks, phishing, and third-party compromises. The Federal Trade Commission (FTC) reports that identity theft and identity-driven scams dominate both volume and losses across all fraud cases.

In 2024, **identity theft accounted for approximately 17% of all consumer reports,** while identity-adjacent categories – such as imposter scams, account takeovers, loan fraud, and credit card fraud – represent a substantial portion of the remaining cases. When combined, **the majority of reported fraud has a direct identity nexus,** meaning identity compromise, impersonation, or misuse is a necessary condition for the crime.

The rise of synthetic identity fraud underscores how far fraud has come, moving from traditional identity theft to a broader scalable activity. Synthetic identities are constructed by blending real and fabricated data, and now accounts for roughly 11% of all reported cases globally, growing eightfold in 2025 alone. This makes it the fastest-growing fraud category worldwide. These identities are rarely stolen outright; they are manufactured, aged, and monetized, often without a single human victim realizing harm until months or years later.

This is not crime of opportunity – it is identity manufacturing at scale.

Financial Services: Know your Customer Processes as an Opportunity for Fraudsters

Nowhere is the industrialization of fraud more apparent than in **financial services.** Banks, fintechs, Third-Party payments platforms, digital asset services, and other providers increasingly depend on remote (web-based) onboarding, facilitating near-instant access to services, and frictionless experiences and transactions – conditions that fraud-as-a-service exploits aggressively.

In 2024, the FTC recorded 2.6 million fraud reports tied to financial exploitation. These cases came alongside 1.1 million identity theft reports, with credit card fraud, loan and lease fraud, and account takeover (ATO) among the most common categories. These crimes rely on identity compromise rather than simple deception. Fraud rings now use AI to automate credential stuffing, hijack legitimate accounts, and deploy impersonation scams that are personalized, timely, and convincing.

Large-scale transaction data shows that account takeover represents roughly 17% of all detected fraud, while First-Party abuse, identity misuse, and synthetic identity schemes together account for the majority of loss-driving incidents. Critically, many of these attacks succeed not because controls are absent, but because they are anchored to static, easily replicated identity signals – passwords, knowledge-based questions, uploaded documents – that AI can bypass or mimic at scale. Further, each time identity attributes need to be verified this poses a vulnerability, given the exposures that can be compromised.

Education: Exploiting a "Target-rich, Trust-poor" Sector

The education sector illustrates how fraud-as-a-service expands rapidly wherever identity may be weakly verified, where there are many physical, logical and digital access channels, and diverse individuals representing differing risk personas are increasingly moving funds for different purposes.

Universities, colleges, and training institutions hold enormous volumes of sensitive identity data, rely heavily on digital onboarding, and increasingly disburse financial aid through automated systems – making them prime targets.

In 2025, education became the most attacked sector globally, averaging 4,388 cyberattacks per organization per week, a 31% year-over-year increase. In California alone, community colleges lost $13 million in a single year to financial-aid fraud driven by "ghost students" and impersonation, a 74% year-over-year increase. Education providers report that AI-generated IDs, transcripts, and supporting documents now account for roughly 30% of high-risk onboarding alerts, and that organized fraud rings automate enrollment, participation, and aid withdrawal. Fraudulent applications and enrollments have been growing especially as online and hybrid programs proliferate.

Once again, the pattern is clear: **digital scale** (paired with AI tooling), plus **weak identity assurance** in an environment with multiple identity-exposing activities **leads to programmatic fraud.**

Workforce and Employee Systems: Identity = Access

Workforce and employee identity systems are not immune from the scourge – HR platforms, payroll systems, contractor onboarding, and privileged access have all become central attack vectors. Globally, organizations lose an estimated 5% of annual revenue to occupational fraud, translating to approximately $50 billion per year in the U.S. alone. Insiders – malicious or compromised – account for over 90% of major internal theft losses and roughly 20% of data breaches, often through credential misuse or impersonation.

AI amplifies these risks by enabling highly convincing business email compromise, payroll redirection scams, and executive impersonation using cloned voices and writing styles. With falsified employee backgrounds and resumes and expanding remote work and digital onboarding, workforce identity has become another reusable asset in the fraud supply chain.

Artificial Intelligence Turns Fraud into a Competitive Business, Not Just a Threat

AI does not merely increase fraud volume – it changes the underlying mechanics of it. AI lowers marginal cost, increases success rates, and enables constant experimentation. Fraud tools are now sold, rented, and refined like SaaS products. Identity compromise is no longer a prerequisite hurdle; it is an input that can be bought, generated, or simulated. When combined with the economic draw of personal data monetization, the incentives for ongoing collection and exploitation grow stronger over time.

Monetizing personal data is such a powerful commercial driver because it sits at the intersection of economics, technology, and human behavior in a way few other assets do. Unlike physical resources, personal data is non-rivalrous (it can be reused infinitely), constantly replenishing, and becomes more valuable as it is aggregated, linked, and analyzed. Personal data also compounds in value over time. As data about identity, behavior, relationships, and transactions accumulates, it allows for more accurate predictive capabilities – aided by AI.

Machine learning systems can turn personal data into long-lived strategic capital rather than a one-time asset, which incentivizes institutions to retain data indefinitely, repurpose it beyond its original context, and combine it with Third-Party sources. While these practices materially boost enterprise valuation and competitive advantage, they also directly threaten privacy and increase the blast radius of breaches.

This is why losses are rising faster than incident counts, why synthetic identity fraud persists undetected for years, and why traditional detective controls struggle to keep up. **As long as identity remains static, centralized, and easily reusable, fraud-as-a-service will continue to scale faster than defense.**

Catching Up: Modern Digital Identity as Anti-Fraud Infrastructure

Addressing fraud at scale requires a shift from reactive detection to preventive trust infrastructure. This requires modernized digital identity – specifically, a form of identity that is user-owned, privacy-preserving, and based in root-of-trust forms. When combined with biometrics, higher levels of assurance can be obtained, and identity can become both "persistent" (continually re-used/verified) and enabled in both physical and digital environments. This is no longer optional – it is foundational.

Verifiable digital credentials (VDCs) replace photocopied IDs, screenshots, and database lookups with cryptographically signed claims issued by trusted authorities and held by the user. Rather than transmitting full identity records, individuals can prove specific attributes – such as "is employed," "is a student," "is not sanctioned," or "is eligible (e.g. old enough)" – without exposing unnecessary personal data. This dramatically reduces the value of stolen data and removes the incentive for mass identity harvesting.

Paired with advanced biometrics – including liveness detection and behavioral analysis – these credentials are bound to a real, present human being. Even in agentic activities, verifiable digital credentials can provide an affirmed proof of person (or entity) whose identity has been affirmed *and* whose authorization to the agent has been authenticated. This combination directly counters AI-driven impersonation, synthetic identities, and automated abuse by reintroducing a cost that software attacks struggle to overcome: physical presence and continuous proof of control.

Privacy, User Control, and Fraud Reduction are Mutually Reinforcing

Critically, this model increases assurance while preserving privacy. Because credentials are user-controlled and permissioned, individuals decide what to share and with whom. Selective disclosure and zero-knowledge proofs (proving truth/facts without revealing sensitive information) allow organizations to verify legitimacy without centralizing identity data. This helps reduce breach impact while improving trust.

At scale, this approach benefits all sectors:

- **Financial services:** Reduces account takeover, synthetic identities, and onboarding fraud, improving KYC/CIP and client and transaction monitoring
- **Education:** Prevents ghost students, AI-forged enrollment abuse, false testing and backgrounds, and student aid/tuition fraud.
- **Workforce & Employment:** Secures workforce access and payroll without intrusive surveillance, and ensures employee engagement (at work, transfer/mobility, etc.) is secure, frictionless, and privacy preserving.

By shifting from static identifiers to verified, consent-based trust, fraud becomes harder, slower, and more expensive – exactly the opposite of the features that make AI-boosted fraud-as-a-service so appealing.

Conclusion: Identity Modernization as Anti-Fraud Infrastructure

Fraud is no longer a series of isolated attacks – it is a digitally enabled business ecosystem fueled by identity exposure and amplified by AI. Continuing to rely on legacy identity verification mechanisms is as absurd as trying to protect a modern Cloud service with a physical lock.

Modern, user-owned digital identity – grounded in verifiable credentials and advanced biometrics – offers a path forward that aligns security, privacy, and scale. In the AI era, who we trust, how we prove it, and how we share that proof will determine whether fraud remains a growth industry – or becomes economically unviable. A healthy benefit is a heightened assurance that our most sensitive data – our identities – are safe and secure and belong to their rightful owners: ourselves.

For more information, contact us at
smart-biometrics@idemia.com