7 Things You Need to Know About …

Digital Fraud

A quick guide to understanding Digital Fraud from the Association of Payment Professionals

01 | WHAT IS IT?

Digital fraud spans a broad spectrum of schemes designed to deceive, manipulate, or steal through online channels. Criminals are increasingly using advanced technologies to sharpen their tactics and expand their reach. As digital tools become more powerful and woven into everyday life, digital fraud is evolving just as quickly, growing more sophisticated and harder to detect.

02 | HOW DOES IT WORK

Digital fraud operates by exploiting vulnerabilities in technology, human behavior, and financial systems to deceive individuals or organizations for financial gain. Some fraudsters rely on simple tactics, such as sending deceptive emails or making phone calls to trick people into revealing sensitive information. Others employ more advanced methods like creating fake websites, malicious apps, or hacking payment systems to steal data, gain unauthorized account access, or facilitate illegitimate transactions.

Fraudsters typically use one of the following methods:

Identity Theft and Synthetic Identity Fraud:

- Criminals use stolen personal information, or fabricate entirely new identities, to open fraudulent accounts or make unauthorized purchases.

Account Takeover (ATO):

- Fraudsters gain control of legitimate user accounts through phishing attacks, malware, or stolen credentials, enabling them to conduct transactions or change account details.

Association of Payment Professionals

02 | HOW DOES IT WORK (continued)

Payment Fraud:

- Nefarious actors use stolen or fake payment information, such as credit or debit card numbers, to purchase goods and services.

Friendly Fraud / Chargeback Fraud:

- Real customers dispute a valid transaction to obtain a refund, often after having already received and used the goods or services.

Phishing:

- Fraudsters impersonate trusted organizations such as banks or merchants to deceive individuals into divulging personal or financial information.

03 | WHO IS DOING IT?

a. Synthetic-identity and fraud-kit providers
Service operators sell polished identity packages and merchant application kits containing AI-generated IDs, machine-curated social profiles and websites, and end-to-end application bundles designed to pass KYB/KYC checks.

b. Coordinated fraud rings build "clean" merchant shells
Criminal networks deliberately age domains, add a small amount of test activity to check that a system works before scaling up, and use AI to model underwriting thresholds so they remain below detection, shifting from rapid "attack and exit" to slow "groom and exploit."

c. Merchants who intentionally misrepresent
Legitimate-appearing businesses may obfuscate prohibited products or services, rephrase descriptors to evade keyword filters, fabricate fulfillment evidence, or produce AI-polished chargeback rebuttals.

d. Third-party "compliance packagers"
Application preparers and consultants optimize ownership disclosures, draft policies, and train merchants on underwriting responses. Some entities use generative AI to create highly consistent, industry-standard documentation that blurs the line between legitimate preparation and fraud facilitation.

e. Money-movement networks and mule coordinators
Scammers provide payout destinations, laundering rails, or coaching on maintaining a "clean" profile. AI is used to model flow-of-funds patterns that minimize anomaly flags.

04 | WHY IS IT SIGNIFICANT?

Digital fraud in payments is a critical concern due to its financial impact, reputational consequences, and erosion of merchant trust. Rising demand for frictionless boarding is creating more opportunities for fraudsters to exploit gaps in controls. Some concerns are:

Operational Costs	Fraud detection requires additional costs and resources such as systems and staff.
Financial Losses	Businesses and customers lose billions due to fraudulent transactions, chargebacks, and identity theft.
Reputational Damage	A single scam or account takeover can leak online and cause brand-damaging risks to card networks and their partners.
Compliance and Regulatory Risks	When fraudulent merchants slip into portfolios, acquirers may face card network assessments and regulatory penalties.

05 | WHAT IS THE DOWNSIDE?

When digital fraud succeeds in creating a new merchant account by passing traditional underwriting controls, the consequences for the payments ecosystem can be immediate and severe. What makes this emerging threat so dangerous is its ability to impact every layer of the risk framework, from financial exposure to compliance obligations.

The most direct impact is financial. Fraudulent merchants leave the liable entity exposed to chargebacks, refunds, and potential card network assessments. Because these merchant profiles often appear authentic, fraud may not be detected until substantial volumes have already been settled.

Once fraudulent activity is detected, the operational fallout can be significant. Internal investigations, chargeback management, and remediation efforts consume substantial time and resources. Fraud incidents can also disrupt underwriting workflows, prompting heightened scrutiny of medium- and high-risk merchant types and delaying approvals. The need to re-underwrite or intensify monitoring across existing portfolios adds further cost and complexity. In short, every missed fraudulent account amplifies the burden on underwriting, risk, and compliance teams. This impacts efficiency and profitability.

05 | WHAT IS THE DOWNSIDE? (continued)

Regulators, card networks, and sponsor banks hold liable entities fully accountable for knowing their merchants. Onboarding fabricated or shell businesses can trigger violations of regulatory obligations. As fraudsters adopt increasingly sophisticated synthetic identities and falsified documentation, acquirers face heightened scrutiny from the networks and sponsor banks and may be subject to penalties or mandatory remediation programs.

Every undetected fraudulent merchant erodes an acquirer's reputation for underwriting, risk management, and trustworthiness. Card networks, sponsor banks, and regulators increasingly expect the industry to uphold stringent merchant-vetting standards. If an acquirer becomes known as a "soft target," it risks not only reputational harm but also the loss of valuable partnerships and referral relationships. Restoring market confidence after a major incident can take years, far longer than the brief window in which the fraud occurred.

06 | WHERE IS IT GOING?

Digital payment fraud is quickly evolving as criminals weaponize emerging technologies to outpace traditional controls. AI now enables the creation of convincing synthetic identities, deepfakes, and forged business documents, which allow fraudsters to impersonate legitimate merchants at scale. In 2023 alone, synthetic identity fraud was estimated to cause over $35 billion in losses, and that number is rising.

Next-generation fraud will go further. Criminals are beginning to deploy autonomous AI agents that generate fake documents, mimic human behavior, and adapt in real time. Deepfake voice and video will challenge merchant onboarding and customer support verification, while behavioral mimicry threatens to defeat even advanced risk models. As instant payments, open banking, and embedded finance accelerate money movement, fraud will propagate faster across borders and between platforms.

Regulators are responding with new frameworks for AI disclosure, transparency, and human oversight, and are expected to introduce model certification and real-time incident reporting standards. Payment providers are investing in document forensics, device and IP intelligence, behavioral analytics, and self-learning fraud models that evolve as fast as the threats they face.

The future of fraud prevention will rely on a layered defense that combines automation with human judgment to safeguard compliance, reputation, and trust in an increasingly technologically savvy fraud landscape.

07 | WHAT ARE THE IMPLICATIONS FOR PAYMENTS?

Digital fraud is growing more sophisticated as technology advances, enabling perpetrators to feign legitimacy with minimal effort. For payments, the consequences range from misplaced confidence during initial KYC to significant financial exposure and reputational harm.

Financial institutions also face heightened regulatory and compliance scrutiny. Regulators continue to require human oversight of automated processes, including approvals, identity verification, and chargeback-risk mitigation. In cases where fraud appears systemic or widespread, a bank's ability to sponsor acquiring services could be revoked entirely.

A significant portion of fraud can be traced back to insufficient or poorly executed merchant onboarding. When fraud is knowingly or negligently facilitated, merchants may face termination by upstream processors, placement on the MATCH list, and other potential adverse actions.

Advanced technology is essential for detecting complex fraud schemes and identifying falsified documents. Human oversight remains a core regulatory expectation and now a necessity. Transaction monitoring can highlight unusual processing patterns, while IP analysis, device location tracking, and strengthened identity verification can reveal linked accounts and suspicious activity. At scale, behavioral analytics and machine learning algorithms can detect unusual patterns and validate applicant information through KYC checks against global watchlists.

This Seven Things publication was produced with contributions from members of APP's Strategic Interest Group on Fraud Trends.

Contributors

- Christine Harper: Director of Investigations, Global Payments
- Eric Knapp: President, Electronic Verification Systems LLC
- James Filomena: Vice President, Commercial Risk- Sponsorship & Third Party Payments, Citizens Bank
- Jonathan Corona: COO, MobiusPay
- Kevin Lambrix: Payments Leader, Hoyne Bank
- Marlena Hubley, Principal, Rebeta Consultants LLC
- Mark Creizman: Director of Risk & Compliance Advisory, Material Connections LLC
- Niamh Lewis: Vice President, G2 Risk Solutions
- Noelle Parise: Senior Fraud & Risk Investigator, North
- Shari Savlick: Vice President, Merchant Compliance, Merrick Bank

About APP

The Association of Payment Professionals (APP) is a volunteer-driven, nonprofit, membership organization committed to safeguarding the payments ecosystem through education, collaboration, and leadership.