entersekt

The Financial Authentication Company.

Preventing emerging payment scams: A strategic guide for issuers

As payment scams become more sophisticated, issuers must remain vigilant, keeping pace with advances in payment authentication, legislation, and standards like 3-D Secure.

entersekt.com
info@entersekt.com

In this white paper

Introduction

Detecting and preventing advanced payment scams requires evolved authentication

Fraudsters have access to the same cutting-edge technologies that financial institutions use to protect their customers — and they're using them to continuously refine their tactics and bypass security measures. As payment scams become more sophisticated, issuers must remain vigilant, keeping pace with advances in payment authentication, legislation, and standards like 3-D Secure. Otherwise, they risk losses that extend beyond financial damage, affecting brand reputation and customer trust.

The rise of faster, instant payment systems around the world has intensified this challenge. Funds can be irrevocably moved — and stolen — in seconds, leaving little room for error or delayed detection. To prevent losses, issuers need the tools to not only recognize the mechanisms behind today's scams but also anticipate how they evolve. Equipped with the right technology and risk intelligence, banks can shift from a reactive stance to a proactive defense, detecting and preventing scams before they impact customers.

At Entersekt, we believe true resilience lies in evolved authentication — the seamless integration of strong authentication and real-time fraud detection across every banking and payment channel to deliver strong security and a frictionless user experience.

In this white paper, we aim to shed light on this evolving scam landscape and how innovative fraud prevention solutions can protect institutions — and their customers at the coalface of risk.

Section 1

Understanding the evolving scam and fraud threat landscape

Scammers are now operating like sophisticated businesses, rapidly adopting the latest AI tools — from agentic AI commerce to open-source large language models, voice-cloning and deepfake video software — alongside 'fraud-as-a-service' offerings such as phishing kits and bot networks. What began at a level of simple caller ID spoofing has evolved into capabilities that can clone a victim's voice in under five seconds. These tactics are deceiving even the most digitally literate consumers.

According to GASA's Global State of Scams 2025 report, 70% of adults worldwide encountered a scam in the past year. Essentially, fraudsters are leveraging technology to automate and scale their operations globally, giving rise to new forms of exploitation such as virtual kidnapping scams using voice cloning and sextortion powered by deepfake videos. The result is a staggering escalation in harm — with global scam losses reaching $442 billion in 2024.

> "70% of adults globally have had a scam experience in the last year, with scam exposure most common in Oceania, South America and Africa. Of those who have encountered a scam, 70% have reported it at least once, with over a third claiming that no action was taken by the platform after reporting it."

– Jorij Abraham, Managing Director, GASA.

While financial institutions (FIs) strengthen controls, regulatory and governance frameworks often struggle to keep pace. In the UK, for example, Authorized Push Payment (APP) fraud losses and cases declined between 2023 and 2024 following the rollout of the Confirmation of Payee (CoP) service. Yet, a new wave of hybrid scams subsequently emerged — combining multiple attack vectors and exploiting international payment channels to bypass traditional APP fraud prevention measures.

The current lay of the land can likely be attributed to five main drivers:

1. **Fraudsters increased use of advanced AI tools:**
   Generative AI is lowering the barrier to entry for complex scams. Tools like FraudGPT, WormGPT, and text-to-video engines such as Sora 2 enable hyper-personalized phishing, impersonation, and romance scams at scale.

2. **Faster payment systems:**
   With 78% of U.S. businesses now viewing instant payments as essential, and nine in 10 FIs offering or planning to utilize FedNow®, RTP®, or Zelle®, criminals exploit the speed and irrevocability of real-time transactions to cash out before being detected.

3. **Expansion of professional scam enterprises:**
   The fraud ecosystem is maturing. Smaller, local operations are being absorbed into larger, organized 'scam-as-a-service' networks that use AI and data analytics to industrialize their schemes.

4. **Proliferation of exposed and stolen data:**
   Mass data breaches and dark-web data markets fuel more convincing social engineering. Fraudsters combine leaked personal, biometric, and behavioral data to create realistic synthetic identities that can bypass traditional identity checks.

5. **Regulatory fragmentation across markets:**
   While some regions, such as the UK and EU, enforce reimbursement and APP fraud prevention regulations, there are others that lag behind. Fraudsters exploit these inconsistencies to move funds across borders and jurisdictions with minimal traceability.

The impact of authorized and unauthorized fraud

Modern scams have moved beyond simply gaining unauthorized access to a cardholder's account through an account takeover. While banks can safeguard against unauthorized fraud by verifying the identity of the person making the payment, the same does not apply to authorized payment fraud.

> Learn more about the dangers of authorized push payment (APP) fraud and five tactics to help protect your cardholders.

Today, scammers turn consumers into 'criminals' by tricking them into initiating fraudulent payments themselves. In 2019 in the UK, for instance, authorized fraud losses increased while unauthorized fraud losses dropped.

With this growth in authorized payment fraud, traditional prevention measures have become less effective. What does remain the same is the impact of these crimes.

For cardholders, this can include:

- Financial loss
- Mental and emotional trauma
- Loss of trust in their bank, and sometimes digital banking services in general

For banks, scam fraud often results in:

- Reimbursement liability, which may be mandatory
- Reputational damages
- Increased operational and compliance costs

How to combat prevalent scams: Authorized vs unauthorized payment fraud

Authorized payment fraud

Occurs when a customer is tricked into initiating or approving a transaction to a scammer — typically following a social engineering or impersonation attack.

Example 1: Social engineering attacks

Often a precursor to Authorized Push Payment (APP) fraud, a social engineering attack deceives victims into revealing information or sending money through manipulation and a false sense of trust.

What is social engineering? Learn more

Examples:

- OTP phishing and SIM-swap fraud
- Vishing (voice phishing)
- Smishing (SMS phishing)
- Social media scams (e.g., fake investment or 'discounted goods' offers)

Characteristics:

- Exploits trust through impersonation of banks, family members, or authorities
- Delivered via phone, SMS, email, or social platforms
- Frequently leads to APP fraud or account takeover

Strategic levers:

- Behavioral analytics to flag abnormal behavior patterns
- Risk-based and contextual authentication
- Consumer and employee education
- Real-time scam alerts and customer warnings

Relevant regulations:

- Strong Customer Authentication (SCA) under PSD2 / upcoming PSD3 (EU)
- Australian Scams Prevention Framework (effective since early 2025)

Example 2: Authorized Push Payment (APP) fraud

A type of fraud where victims willingly initiate payments to scammers, believing them to be legitimate recipients.

What is APP fraud? Learn more

Examples:

- Investment scams (including crypto-related)
- Romance scams
- Tech support or refund scams
- Impersonation or fake recruitment scams
- Business email compromise (BEC) / CEO fraud
- Fake charity donation scams

Characteristics:

- Users approve payments under false pretenses
- Common in real-time payment systems (e.g., RTP®, FedNow®, SEPA Instant, Pix)
- Increasing regulatory pressure for reimbursement liability on FIs

Strategic levers:

- Payee name-matching tools like Confirmation of Payee (CoP) and Verification of Payee (VoP)
- Real-time transaction risk assessment
- Contextual, in-app authentication (e.g., matching device, behavior, and location)

Relevant regulations:

- Mandatory reimbursement rules under the Payment Systems Regulator (UK) (effective since Oct 2024)
- Proposed PSD3 fraud prevention mandates (EU)
- National scam protection frameworks or bodies (e.g., Australia, Canada)

Unauthorized payment fraud

Occurs when a fraudster initiates or manipulates a transaction without the customer's knowledge or consent.

Example 1: Account takeover (ATO)

The attacker gains control of a legitimate account to conduct fraudulent transactions.

What is ATO? Learn more

Examples:

- Credential stuffing and phishing
- Man-in-the-middle (MitM) or reverse proxy attacks
- SIM-swap fraud
- Deepfake or synthetic identity impersonation

Characteristics:

- Criminals hijack access via stolen credentials or compromised devices
- Often involves adding beneficiaries or changing account settings
- Commonly overlaps with phishing and malware attacks

Strategic levers:

- Passwordless or biometric authentication
- Adaptive multi-factor authentication (MFA)
- Silent authentication using behavioral analytics
- Device, network, and location intelligence
- QR scan authentication for proximity proof

Relevant regulations:

- PSD2 (SCA) / upcoming PSD3 (EU)

Example 2: Third-party chargebacks

Fraud involving unauthorized purchases made using someone else's saved card or digital wallet credentials.

What are third-party chargebacks?
Learn more

Examples:

- ATO leading to e-commerce or ride-hailing purchases
- Card-not-present (CNP) transactions with stolen credentials
- Fraudulent in-app or digital wallet purchases

Characteristics:

- Often tied to digital wallet or tokenization vulnerabilities
- Commonly part of larger ATO or mule account networks
- Drives higher operational costs through chargebacks

Strategic levers:

- Behavioral analytics and silent authentication
- 3-D Secure 2.0 for richer data and frictionless verification
- Risk-based authentication measures across channels

Relevant regulations:

- PSD3 (EU, 2025)

Section 2

Navigating global payment regulatory trends

As fraud tactics, technology, and consumer expectations continue to evolve, so too must the global regulatory landscape. Issuers need to comply with shifting regional and international requirements, while recognizing that measures effective in one market may not translate seamlessly to another.

Here are five current trends to bear in mind as the market continues to shift:

1. **Tightening scam and fraud prevention regulations**
   As global scam losses continue to rise, regulators are strengthening mandates on fraud prevention and liability. In the UK, the PSR shifted APP fraud reimbursement from consumers to a shared responsibility between sending and receiving banks from October 2024. Similar consumer-protection measures are under review in the EU under PSD3 and being explored elsewhere, including Canada's Real-Time Rail (RTR) system. In Australia, the launch of the National Anti-Scam Centre (NASC) in 2023 coincided with a 25.9% drop in reported scam losses to AUD 2 billion in 2024.

2. **Global adoption of Strong Customer Authentication (SCA) measures like MFA**
   In the EU, card-not-present (CNP) fraud rates declined by 12% following the rollout of SCA. Consequently, markets like the U.S., India, Brazil, and others have recommended or adopted similar MFA requirements to better protect digital transactions.

3. **Expansion of instant payment regulations**
   Along with the EU and UK, more recent faster payment systems like FedNow® in the U.S., India's Unified Payments Interface (UPI), and Brazil's Pix are also accelerating real-time payments. In the EU, for instance, FIs must comply with the SEPA Instant Credit Transfer regulation, mandating that instant payments be received, available to the payee, and that confirmation is received by the payer within 10 seconds.

4. **Increased adoption of AI-driven fraud prevention tools**
   In many regions, regulators are encouraging the adoption of modern fraud prevention tools — like behavioral analytics, AI-driven transaction monitoring, and name-matching services, like CoP. In the U.S., while there's no overarching federal mandate, FedNow® provides fraud management features (such as negative lists, account activity thresholds, and risk-intelligence sharing capabilities) to help secure real-time payments.

5. **Global convergence vs local divergence**
   While cross-border regulatory alignment is vital in areas like authentication and instant payments, institutions must also adapt strategies to their local compliance landscape and regional frameworks. An example of this is the post-Brexit divergence between the EU and UK banking regulations.

Let's examine a few of the core payment regulations on a geographical basis.

A snapshot of the current payment regulatory landscape

Strong Customer Authentication (SCA) and PSD2/PSD3
(Europe, UK, global influence)

- Introduced in the EU and UK to reduce fraud through MFA (SCA was mandated under PSD2 in 2019).
- Beyond the UK and EU regions, many countries have SCA requirements, including Brazil, India, Australia, and South Africa.
- Friction in e-commerce flows, especially under OTP-based 3-D Secure (3DS), remains a global issue.
- PSD3, scheduled for kickoff between 2026-2028, proposes broader fraud liability reforms and stricter real-time payment controls.

Discover the key differences between PSD2 and PSD3 — and what they mean for your organization in this free ebook: From PSD2 to PSD3: Turning a compliance challenge into business success.

3-D Secure 2.0 (3DS2)
(EU, UK, APAC, North America, and other regions)

- 3DS2 is widely used to comply with SCA requirements, and its implementation by issuers and merchants continues to grow worldwide, including countries like India, Brazil and South Africa.
- Biometrics and in-app approvals are improving user experience across mobile wallets and e-commerce platforms.
- Leading banks around the globe are enhancing their 3DS programs with behavioral analytics to counter advanced social engineering attacks.

Know what to look for in your next 3-D Secure ACS purchase? Download this free buyer's guide to support your decision and futureproof your payment fraud prevention.

Instant payment regulations and fraud prevention

(U.S., EU, UK, India, Brazil)

- **U.S.:** FedNow® and RTP® promote best practices but currently lack federal liability mandates.
- **EU:** The Instant Payments Regulation, adopted in March 2024, will help accelerate instant payments rollout and, from October 2025, will require a verification of payee service for EU member states.
- **UK:** The Faster Payments System enforced mandatory scam reimbursement rules from October 2024.
- **Brazil and India:** Pix (Brazil) and UPI (India) have built-in risk-based safeguards and consumer reimbursement processes. UPI will phase out peer-to-peer collect requests starting October 2025, further strengthening fraud prevention.

Need a smarter, more dynamic approach to fraud and scam prevention, especially for irrevocable payments? Watch this webinar to learn how to get started.

Liability shifts and consumer protections

(Canada, UK, EU, and emerging markets)

- **Canada:** Real-Time Rail (RTR) is developing fraud accountability frameworks; details are still under development.
- **UK:** PSR mandates £85,000 reimbursement for APP scams, with costs shared equally between sending and receiving banks.
- **EU:** PSD3 draft proposes consumer-first reimbursement for impersonation fraud, with potentially greater liability for the sending bank.
- **Global:** Regulators increasingly advocate for banks to detect and prevent fraud before funds leave a customer's account.

Learn more about the downside of real-time payments and how to overcome growing industry-wide digital payment fraud here.

Section 3

Blocking scammers with multi-layered, real-time defense strategies

Fraudsters continually look for new vulnerabilities in banking and payment systems, with global e-commerce fraud projected to more than double from $44 billion in 2024 to $100 billion by 2029 (Statista). Emerging technologies like agentic e-commerce payments, where AI agents can make purchases or authorize transactions autonomously, introduce new risks and attack surfaces that fraudsters will be quick to exploit.

As attacks have evolved, so have defenses — from basic credentials and OTPs to endpoint signals and biometrics for multi-factor authentication. Each additional layer makes it harder for scammers to succeed.

Equally critical is real-time fraud monitoring, especially as faster payments accelerate the speed of fraud. McKinsey notes that financial institutions must invest in real-time or near-real-time fraud detection and prevention to stay compliant and secure. Modern, risk-based authentication systems use dynamic risk scoring to assess each transaction and apply only the friction needed to match the threat level.

Simplifying scam prevention with evolved authentication

Legacy systems often stand in the way of rapid modernization and effective protection against today's complex scam and fraud threats. Many banks rely on multiple, disconnected fraud prevention tools across their different channels to keep fraudsters out. However, this fragmented approach creates data silos and vulnerabilities that fraudsters can exploit.

> "The fact that your fraud system and your challenge system and your identity proofing system are not linked together, that's a problem. If you want evolved authentication, they need to be tied together."
>
> – Gerhard Oosthuizen, CTO, Entersekt

A unified fraud prevention approach allows issuers to share risk intelligence across channels for faster, stronger, and more consistent safeguards. To prevent these safeguards from mistakenly blocking legitimate payments, issuers should also consider moving beyond traditional risk-based authentication (RBA) models that rely on static, rule-based logic.

By investing in a 3-D Secure ACS that dynamically adjusts the authentication method based on real-time risk scoring and dynamic risk conditions, banks can increase transaction success rates while providing advanced scam detection. Unlike static signals that flag all "high-risk" merchants, for instance, dynamic RBA can identify suspicious activity at the individual level, recognizing when a user's behavior is legitimate. The individualized analysis delivers effective fraud mitigation, and balances security with a seamless user experience.

Learn more about how to deliver robust security without compromising customer convenience through adaptive risk-based intelligence here.

To counter modern-day fraud threats such as AI-enhanced social engineering and APP fraud, and align with fraud prevention standards, banks should consider an evolved authentication strategy built on:

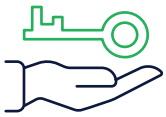
Cross-silo protection: Strong, unified fraud prevention across all channels.

Strong authentication: Dynamic authentication using silent and active authentication measures, enabling frictionless experiences.

Risk intelligence: Collecting and analyzing risk conditions to detect suspicious patterns in real-time.

ID proofing: Collecting and analyzing endpoint signals on originating and authentication channels.

Consortium data: Integrating with global networks and consortiums to collate and enrich fraud risk signals.



Biometrics or passkeys: To better align with modern fraud prevention technology standards and CX.

Conclusion

How to build financial security for the payments ecosystem

McKinsey predicts that by the end of 2028, global payments revenue will reach $3.1 trillion. Taken in parallel with major payment shifts, like the U.S. Federal government phasing out checks for dispersal payments, the opportunities for scammers are rife.

To reduce the inevitable rise in payment threats that will follow, the industry can still create a win-win situation for all proponents — by viewing scam prevention as a collective responsibility. Sharing scam and risk data across the ecosystem will help amplify risk analysis and mitigate threats faster.

In addition, the use of frameworks like SCA and standards like 3DS 2.0 can support improved regulatory alignment. In this regard, regulators should also support innovation that balances security and user experience. In their report, McKinsey reiterates "the importance of banks investing in payment technologies to stay ahead of specialist players."

To leverage future growth, banks should invest in scam prevention solutions that employ real-time risk data, are scalable, and use risk intelligence to detect and prevent fraud. Their ROI will not only be realized directly, but also indirectly by building trust with cardholders and the broader ecosystem.

Ready to learn more? Request your personalized demo from an Entersekt expert, here.

About Entersekt

Entersekt, The Financial Authentication Company, provides financial institutions with digital banking fraud prevention and payment security solutions through its cross-channel, Context Aware™ Authentication platform that secures digital transactions and optimizes user experiences. Founded in 2008, Entersekt serves financial institutions around the world, and holds 120+ patents for its security innovations. In 2023, Entersekt acquired the Modirum 3-D Secure software business from Modirum, a security technology firm based in Helsinki, Finland, positioning Entersekt as a global industry leader in authentication solutions for financial services. Entersekt processes 7.5bn+ transactions for 250m+ cardholders and 450,000+ merchants from nearly 900 banks in 70+ countries. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions.

For more information about Entersekt, or to speak to an expert, please visit **www.entersekt.com** or email **info@entersekt.com**.

/Entersekt

@Entersekt

/Entersekt

V01_202511MKT7858