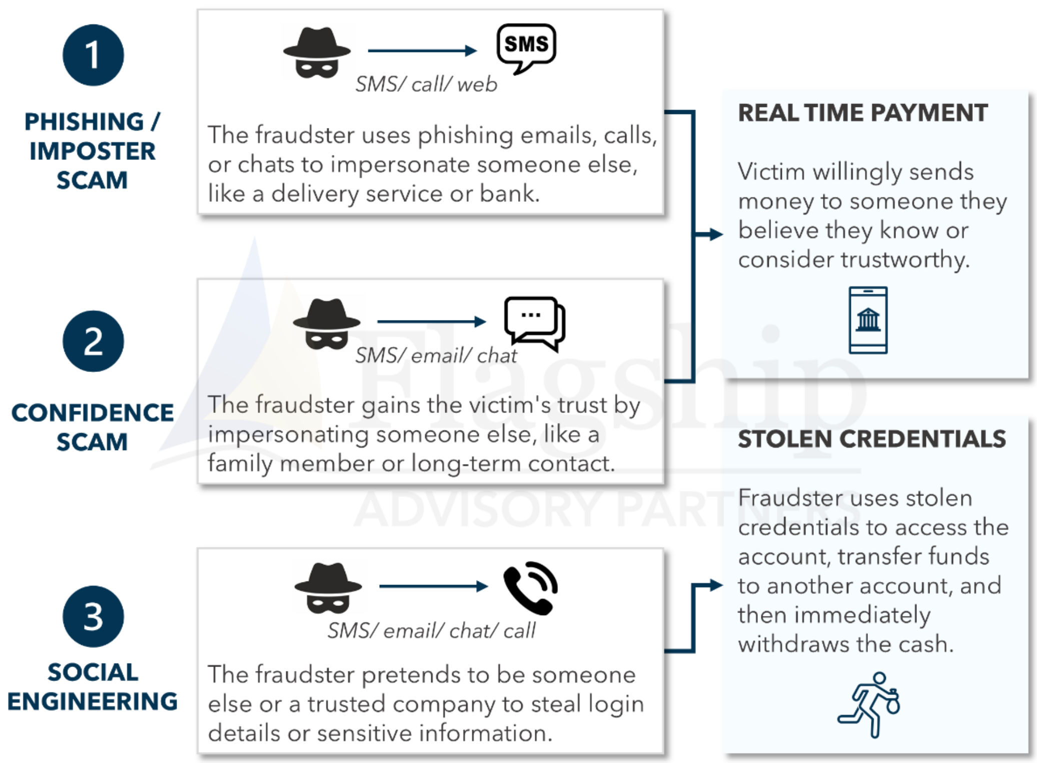
Anupam Majumdar and Stanislav Dubský, 11 November 2024

Authorized Push Payments (APP) Fraud: An Escalating Threat

In today's digital world, Authorized Push Payment (APP) fraud is becoming one of the most deceptive and dangerous scams. As these scams evolve and grow, understanding how they work and how to protect yourself is more important than ever. In this article we delve into APP fraud growth, use cases, solutions and ultimately how payments ecosystem providers can act to prevent this type of fraud.

APP fraud (see Figure 1) is a type of scam in which victims are tricked into authorizing bank payments to fraudsters, believing they are transferring money to legitimate entities. In the UK, APP fraud alone accounts for 80% of all fraud volumes in 2023, and we observe strong growth in fraud volumes across several geos (see Figure 2).

Figure 1: Common Use Cases of APP Fraud (non-exhaustive)



The fraudster uses phishing emails, calls, or chats to impersonate someone else, like a delivery service or bank.

The fraudster gains the victim's trust by impersonating someone else, like a family member or long-term contact.

The fraudster pretends to be someone else or a trusted company to steal login details or sensitive information.

REAL TIME PAYMENT

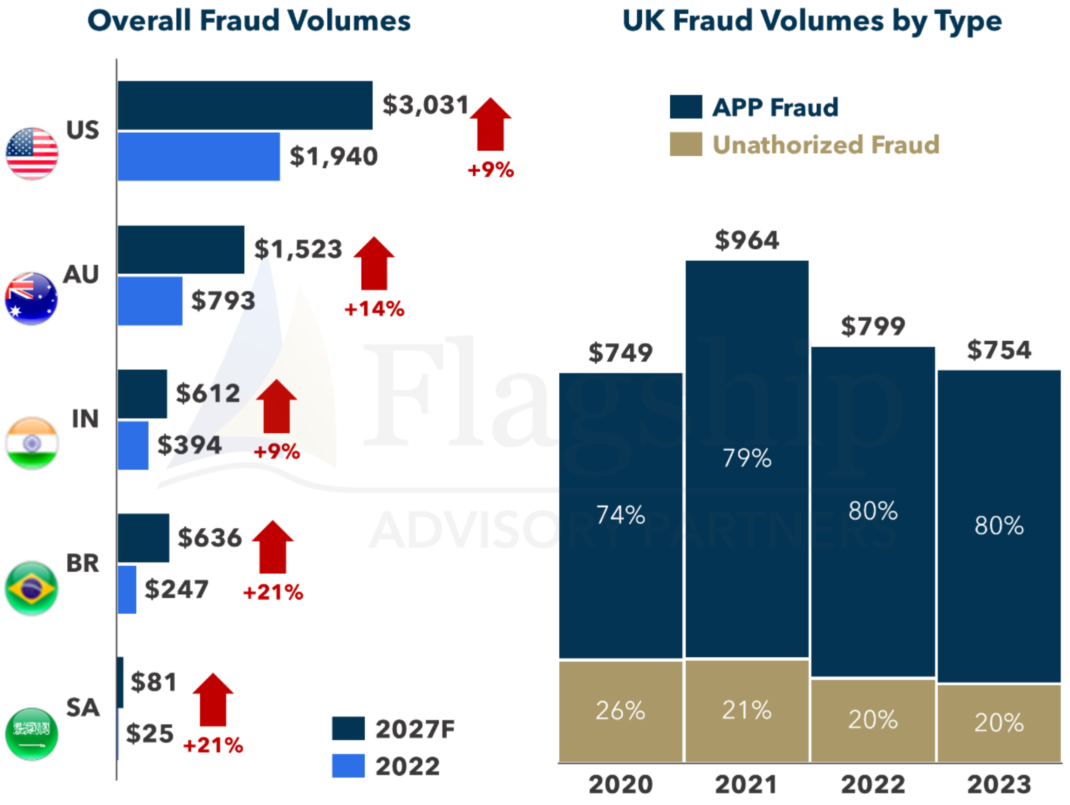
Victim willingly sends money to someone they believe they know or consider trustworthy.

STOLEN CREDENTIALS

Fraudster uses stolen credentials to access the account, transfer funds to another account, and then immediately withdraws the cash.

Source: Flagship Advisory Partners
© Flagship Advisory Partners, November 2024

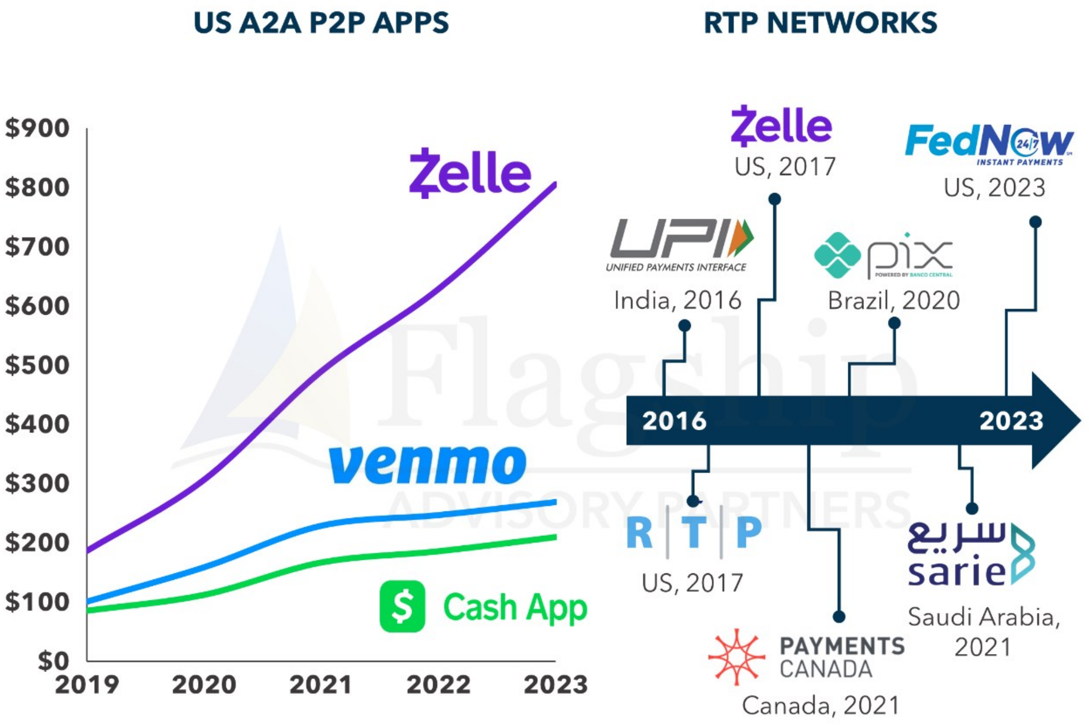
Figure 2 : Fraud Volumes in Select Geos & UK
(select markets; in $ million)



Sources: ACI Worldwide & Global Data Scamscope Fraud Report 2023, UK Finance Annual Report 2024

The rapid growth of instant bank payment networks and the widespread adoption of P2P apps have significantly increased the prevalence of Authorized Push Payment (APP) fraud (see Figure 3). These apps have become a favored tool for fraudsters, who exploit the speed of instant transfers to quickly move stolen funds, making it more difficult for authorities to trace the transactions. To further complicate investigations, fraudsters often convert the stolen money into cryptocurrency, further hindering detection and recovery efforts.

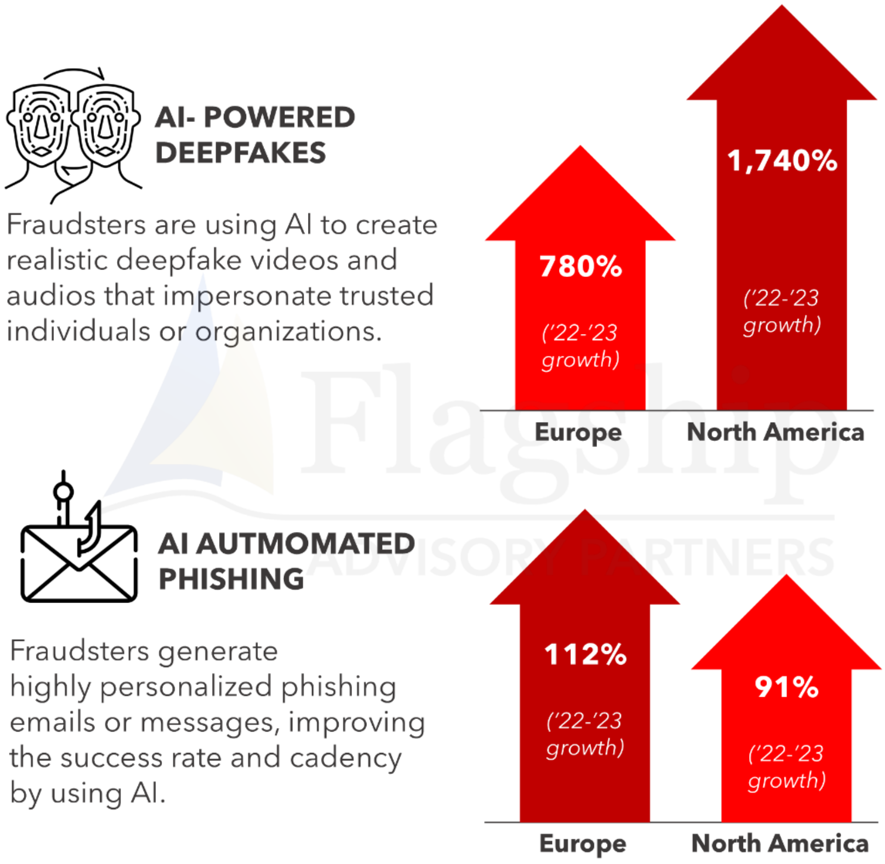
Figure 3 : Popularity of P2P Apps & Real Time Payments Networks
(annual payment volumes in $ billion, RTP networks are non-exhaustive)



Sources: Flagship Advisory Partners market observation, Zelle & PayPal Company websites, Federal Trade Commission report, SumSub Identity Fraud Report 2023, Abnormal Email Security Threats Report, Ark Invest, eMarketer
© Flagship Advisory Partners, November 2024

The rise of AI-powered deepfakes has introduced a new and rapidly growing tool for fraudsters. The growth in detected AI-powered deepfakes has increased by 780% in Europe and 1,740% in North America between 2022 and 2023 (see Figure 4). These AI-driven manipulations—whether videos or images—are becoming increasingly realistic and harder to detect, with their quality improving at an exponential rate. Fraudsters use deepfakes to enhance phishing campaigns, creating personalized messages and tailored schemes that target a broader range of victims. This technology makes their efforts more efficient, significantly increasing their chances of success.

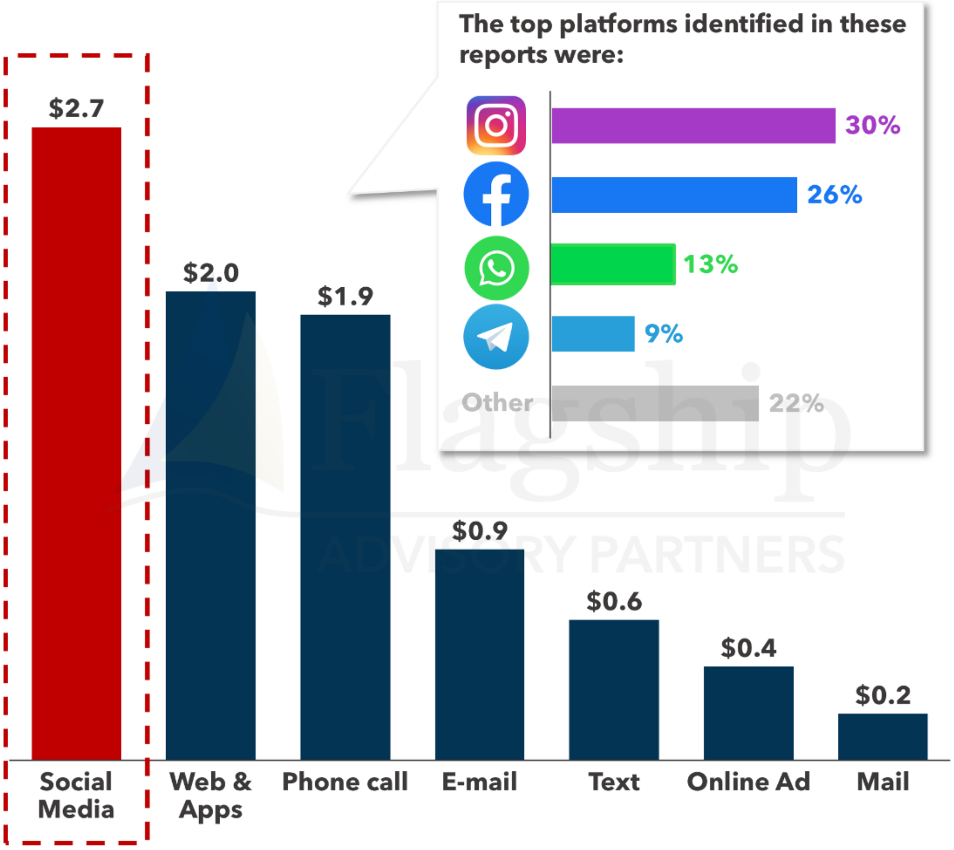
Figure 4 : Sophisticated Social Engineering Using AI
(% growth of number of deepfakes detected)



Sources: Flagship Advisory Partners market observation, Zelle & PayPal Company websites, Federal Trade Commission report, SumSub Identity Fraud Report 2023, Abnormal Email Security Threats Report, Ark Invest, eMarketer
© Flagship Advisory Partners, November 2024

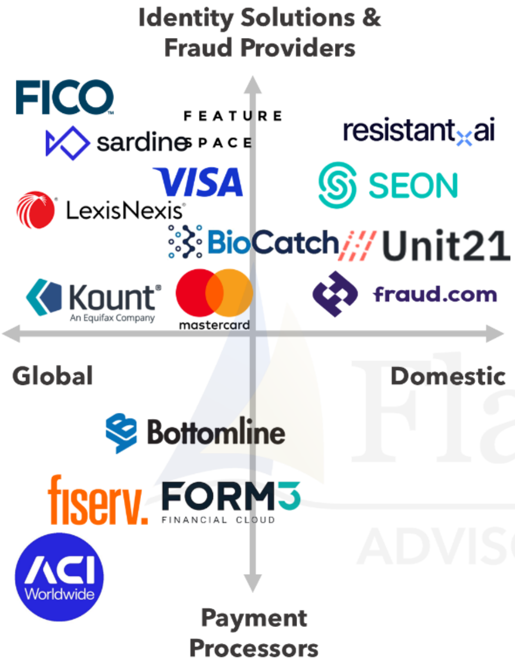
Fraudsters are increasingly using social media platforms to target potential victims, exploiting the widespread use of sites like Facebook, Instagram, and WhatsApp (see Figure 5). By creating fake accounts and sending AI-generated messages, scammers are able to reach individuals more effectively than ever before. According to the US Federal Trade Commission, nearly 70% of scams in the country originate on Meta platforms. A similar trend is seen in the UK, where social media and other online channels accounted for 70% of Authorized Push Payment (APP) fraud cases in 2023. The growing use of these platforms for financial scams highlights the rising risks associated with online communication.

Figure 5 : Reported Fraud Losses by Contact Method in the US
(total aggregate value for 2021, 2022 and 2023; in $ billion)



Sources: Flagship Advisory Partners market observation, Zelle & PayPal Company websites, Federal Trade Commission report, SumSub Identity Fraud Report 2023, Abnormal Email Security Threats Report, Ark Invest, eMarketer
© Flagship Advisory Partners, November 2024

Figure 6 : Anti-Fraud Product Providers & Solutions (non-exhaustive)



Fraud fintechs and payment service processors are **expanding their product sets to include new propositions to fight against APP fraud**

BEHAVIORAL ANALYSIS & DEVICE INTELLIGENCE
AI solutions to detect behavioral patterns using additional signals (e.g., behavioral usage, device geo-location, etc.)

MULE ACCOUNT DETECTION
AI solutions to detect and monitor transaction to potential mule accounts before funds are moved

REAL TIME TRANSACTION MONITORING
AI-powered products that can monitor transactions in real time and prevent fraud

FRAUD PREVENTION ACROSS TRAN. LIFECYCLE
Tools to detect scams across the account lifecycle (during customer on-boarding, account takeover and transaction initiation)

Sources: Flagship Advisory Partners market observation, Company websites

Fighting APP Fraud: List of Key Regulations & Initiatives

Payments ecosystem providers must step up efforts to address the rising threat of APP fraud. Several key regulations and initiatives have been introduced to protect consumers and hold fraudsters accountable. Here we summarize some of the most important regulations and initiatives currently shaping the fight against APP fraud.

PSR Regulation in the UK (effective as of 7 October 2024)

- Consumers, microenterprises, and charities are entitled to mandatory reimbursement within five working days for APP fraud incidents.
- The costs associated with these reimbursements will be shared equally between the sending and receiving Payment Service Providers (PSPs). Both Faster Payments and retail CHAPS payments will be included under this reimbursement policy.
- The maximum reimbursement limit for Faster Payments is set at £85,000.

PSD3 Regulation in the European Union

- PSD3 proposes to introduce reimbursement policies for APP and Phishing fraud. The specific amounts and procedures yet to be determined.
- Banks will be required to implement a confirmation of payee system to ensure the account name matches the International Bank Account Number (IBAN) during transfers.
- PSPs will be enabled to share fraud-related information, and PSD2's TRA, including device analysis checks, will be mandatory for all PSPs.

Amendment to EFTA Legislations in the US

- According to an investigation by the US Senate in 2023, EWS (owner of Zelle) and participating banks rarely reimbursed customers who fall victim to scammers on Zelle.
- Proposed legislation to amend the EFTA (Electronic Fund Transfer Act) to offer protection to consumers and reimburse them for APP fraud.

Meta (Social Network) Partnering with UK Banks

- In Q3 2024, Meta partnered with NatWest, Metro Bank, and Stop Scams UK to share data and combat app scams. leading to the removal of 20,000 scammer accounts across 185 URLs in a pilot phase to combat against ticket fraud.
- Several more banks are expected to join the initiative aimed at protecting social media users from scams.

Key Recommendations to Fight App Fraud

As APP fraud grows, it's essential for financial institutions, fintechs, regulators, and consumers to find effective solutions to fight against it. Along with existing regulations, proactive strategies are needed to counter evolving fraud tactics. The following recommendations outline key actions to strengthen defenses and reduce APP fraud's impact.

Banks & Financial Institutions

- Embrace new technologies such as AI/ML based transaction monitoring capabilities and detect fraud in real time (moving away from more traditional rules-based engines).
- Adopt additional transaction monitoring capabilities, e.g., monitoring of 'payees' via new tools/ AI based models.
- Add additional risk signals to monitor transaction activity, beyond just looking at historical spend patterns.
- Expanding the risk monitoring models to additional signals such as:
  - → Behavioral data (e.g., click speed, pressure on screen).
  - → Device intelligence (e.g., if device far away from payments form factor)
  - → Adopt dynamic risk assessments to reduce false positives.
- Embrace additional authentication methods against suspicious transactions (e.g., a biometric challenge to authenticate payers during a potential scam).
- Continue to educate customers to be wary of APP fraud patterns; regular consumer notification services in online banking apps to prevent scams.

Fraud Fintechs & Other Service Providers

- Be on the forefront of innovation and product development to fight against APP fraud, e.g., utilizing new technologies such as gen AI tech to authenticate genuine users from scammers, behavioral analysis.
- Have solutions in place that can offer an end-to-end approach for banks/FIs to attack APP fraud (e.g., having a unified view of the customer identity across the customer lifecycle / touch-points).
- Innovate in creating data sharing networks to share anonymized fraud data across banks (e.g., consortiums with data providers such as Falcon, Alloy, Sardine).

Regulators

- Provide for balanced regulations that fairly allocate risk and responsibilities to consumers, FIs and 3rd parties (e.g., social media channels).
- Ensure the purview of regulations is extended to all push payment Apps and use cases (e.g., when using APMs, beyond online banking).
- Create regulations to foster information sharing across banks/FIs around suspicious behavior, anonymized data signals, fraud patterns in a quest to make banks remain more informed on potential scams, fraud patterns.

Consumers

- Always double-check unexpected requests for money or sensitive information, even if they appear to come from a trusted source.
- Use multi-factor authentication (MFA) for account access and keep one's software and devices updated to protect against security vulnerabilities.
- Regularly educate oneself on common fraud tactics and warning signs, as fraudsters often use new, sophisticated methods to deceive consumers.

Conclusions

As APP fraud grows with the rise of instant payment networks, P2P apps, and AI-driven tools, both financial institutions and consumers face increasing risks. Fraudsters are exploiting these technologies to quickly move stolen funds and evade detection. However, new regulations like the UK's PSR and the EU's PSD3, alongside proposed US legislation, offer hope for better consumer protection. To combat APP fraud, banks must adopt advanced fraud detection systems, while fintechs and regulators can support data-sharing efforts. Consumers also play a key role by staying informed, using strong security practices, and being cautious of emerging fraud tactics. With collaboration across all parties, the fight against APP fraud can be more effective, though ongoing vigilance is essential.

Please do not hesitate to contact Anupam Majumdar at Anupam@FlagshipAP.com or Stanislav Dubský at Stanislav@FlagshipAP.com with comments or questions.