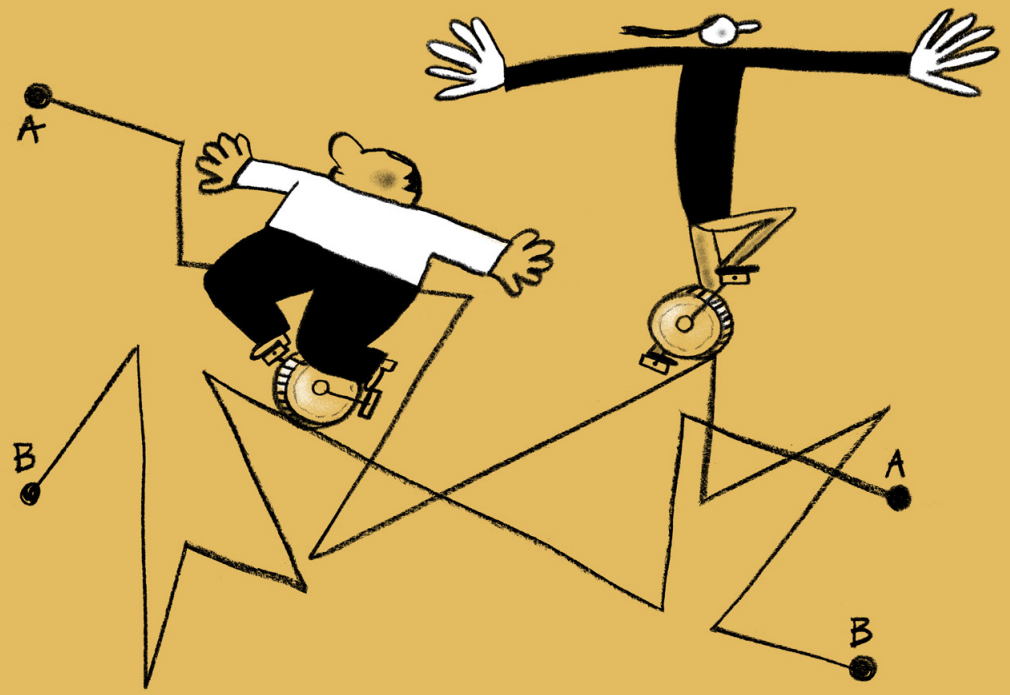
the paypers

fintech market insights

Report 2025



Account-to-Account Payments Report 2025

Unlocking Potential: Insights into Global Trends, Key Players, and Partnerships

Supporting and Key Media Partners

mpe

PCMI

AI-Powered Risk and Fraud Prevention Solutions for Account-to-Account Payments

Roy Prayikulam
SVP Risk and Fraud Division
INFORM

Roy Prayikulam is SVP Risk and Fraud Division at INFORM, a pioneer in AI-powered business process optimisation and intelligent decision-making. For over two decades, INFORM has delivered intelligent, customer-centric solutions for fraud prevention and AML compliance, offering proven, fast, and reliable fraud detection.

With the proliferation of Open Banking and Pay by Bank solutions, how has fraud evolved in the instant payments space?

At the heart of Pay by Bank and Open Banking is a growing reliance on instant payment networks such as Faster Payments (the UK), SEPA Instant Credit Transfer (EU), FedNow and RTP (the US), Pix (Brazil), or UPI (India). These systems allow funds to be settled within seconds, 24/7, even on weekends and holidays. While this delivers unmatched convenience, it also eliminates the traditional 'buffer' that fraud prevention teams relied on to intervene in suspicious transactions.

The faster money moves, the easier fraudsters win, unless detection and decision-making are just as fast. Moreover, we now see that fraud is more psychological than technical. Rather than bypassing security controls, fraudsters manipulate the victim's behaviour. Looking at recent trends, we observe a rise in social engineering attacks such as phishing and identity theft, where criminals impersonate trusted entities to access accounts or initiate transactions.

Which fraud types are most prevalent in instant payments, and how can businesses best address these threats?

The most common fraud types exploit the human factor. Authorised push payment (APP) fraud remains the most prevalent, with criminals deceiving customers or employees so that payments are made voluntarily, for example, by creating a false sense of urgency or impersonating a bank or business partner. Account takeovers are another major concern, where criminals obtain login credentials or bypass security checks to access accounts and transfer funds to mule accounts. ➔

A multi-layered approach is essential to counter these threats. Firstly, companies – especially banks and payment providers – need strong authentication processes. With PSD2, Strong Customer Authentication (SCA) is already standard in Europe, which helps reduce unauthorised access.

Secondly, modern fraud detection systems are crucial. These are solutions that analyse transactions in real time and detect suspicious patterns immediately. Ideally, these are AI-powered systems that continuously learn user and payment behaviour and flag anomalies.

Thirdly, technical measures should be complemented by education and awareness, both internally and for customers. Staff and users should be trained to recognise current fraud methods like phishing and vishing. Procedural controls such as transaction limits, delayed execution for unusual transfers, or dual authorisation for high-value payments further strengthen defences.

Finally, collaboration within the industry pays off. Sharing information about fraud trends and known fraudsters – in compliance with data protection regulations – can help detect and prevent fraud earlier. In the end, a combination of technology, processes, and human vigilance is key to protecting instant payments and building digital trust.

How is industry regulation trying to mitigate the risk of A2A payments, and which factors should companies prioritise to ensure compliance and effective safeguards?

The new EU Instant Payments Regulation is a strong signal: account-to-account (A2A) payments must not only be fast, but also secure. The obligation to verify the payee by matching the account holder's name with the IBAN is an effective tool to prevent misdirected payments and fraud. The UK has gone even further. Since 2024, banks have been required to reimburse victims of APP fraud in most cases. This liability shift forces providers to take proactive action.

Companies should go beyond basic compliance and prioritise proactive measures like real-time risk analysis, transparent AI-based decisions, clear incident processes, or strong customer education. In A2A payments, protecting the end-user experience – the 'last mile' – is especially critical.

How can hybrid AI help prevent fraud in A2A payments, and which approaches have proven most successful?

Hybrid AI combines data-driven models with knowledge-based decision logics – a particularly effective approach in the A2A context, where new fraud patterns often lack sufficient historical data. While machine learning identifies known patterns, knowledge-based logic analyses behaviour in real time, such as unusual transaction flows or recipient profiles. In A2A systems, where transactions are final and there's no time for post-processing, this combination is essential. It also improves precision. Hybrid AI reduces false positives and enables instant decisions in high-risk situations, without unnecessarily blocking legitimate payments. →

INFORM

“ We now see that fraud is more psychological than technical. Rather than bypassing security controls, fraudsters manipulate the victim’s behaviour.

“ Hybrid AI reduces false positives and enables instant decisions in high-risk situations, without unnecessarily blocking legitimate payments.

Click here for the company profile

For A2A payments, which increasingly occur across channels and borders, real-time intelligence is a core safeguard.

What are your expectations for the evolution of the instant payment industry, and how does INFORM support financial institutions in securing A2A payments at scale?

The instant payment market continues to evolve, and user expectations do too. New features such as Request to Pay or embedded payments also contribute to making instant payments an integral part of everyday digital commerce. To support this, INFORM offers purpose-built solutions for real-time fraud prevention in A2A payments. Our RiskShield platform provides hybrid AI-powered decision intelligence that analyses A2A transactions across channels within milliseconds.

RiskShield is especially effective in combating APP fraud. Even when a user authorises a payment, the system can flag when something feels off based on behavioural profiling and dynamic risk signals so that unusual payments to unknown or high-risk recipients can be stopped before funds are released. Scalable for millions of transactions and operable without long training cycles, RiskShield also comes with expert consulting to align security strategies with A2A processes and regulatory requirements. INFORM sees itself as a trusted partner in secure digital transformation and in strengthening long-term trust in A2A payments.

the paypers

Don’t Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

The Paypers releases annual reports covering the latest trends, developments, disruptive innovations, and challenges that define the global payments and fintech industry – B2B and B2C payments, cross-border ecommerce payments, Embedded Finance, A2A payments, BNPL, consumer preferences, fraud prevention, payments regulation, marketplaces and online platforms, and many others. In these reports, consultants, policy makers, service providers, merchants and marketplaces, banks, and fintechs from all over the world share their views and expertise on key industry topics. Listings and advertorial options are also part of the reports to ensure effective company exposure at a global level.

For the latest editions, please check the **Reports section**