

In the Time It Takes to Blink



Abhishek Jhunjunwala
Associate Partner, Forensic
Services
KPMG in India

Real-time domestic and cross-border payment systems are increasingly becoming real and rapidly evolving as critical financial infrastructure. The race towards speed and inter-operability shall be equally matched with robust governance and safeguards to win customer trust and build confidence.

As cross-border instant payments become increasingly widespread, they are reshaping the global payments ecosystem and driving a new era of digital financial services. The rapid advancement of digital banking has elevated real-time payment infrastructure to a critical component of modern financial systems. Apart from banking, the cross-border real-time payments (RTPs) would be a game changer for capital markets and FX markets as it enables real-time cross border inflows and improves liquidity, collateral management and faster settlement cycles, thereby improving transparency and traceability.

However, the accelerating adoption of real-time payments also brings heightened regulatory and compliance challenges, requiring financial institutions to navigate an increasingly dynamic and complex regulatory landscape. Rising fraud and scam incidents, coupled with increasing transaction volumes, have become major challenges for RTP systems, requiring robust fraud prevention, financial crime compliance management, scalable infrastructure, strong cybersecurity, and continuous 24x7 monitoring capability to ensure secure and resilient operations.

As transaction volumes continue to surge, the industry is increasingly focused on interoperability, enabling cross-border real-time payment corridors that reduce settlement times from days to seconds while lowering costs. Global real-time payment transactions reached USD 266.2 billion in 2023, growing 42.2% YoY, and are projected to rise to USD 575.10 billion by 2028 at a 16.7% CAGR¹.

Across the globe, multiple cross-border interoperable RTP systems are making significant progress. As an example, multiple ASEAN countries have linked their domestic instant payment systems to build cross-border RTPs. Similarly, in GCC region, Buna is cross border payment platform connecting various Arab Nations. SEPA Instant Credit Transfer (SCT Inst) is a pan-European payment scheme designed to deliver near-instant euro transfers across participating countries within the Single Euro Payments Area (SEPA).

Similarly on domestic payment rails, Canada's Real-Time Rail (RTR)² built on the ISO 20022 messaging standard, scheduled for launch in Q4 2026, is a new nationwide instant payment system. In India, India's Unified Payments Interface (UPI)³, operated by the National Payments Corporation of India (NPCI) operates the domestic instant real-time payment system and is also currently connected with payment systems in five other geographies, namely, Singapore, UAE, Nepal, Bhutan and France.

Global initiatives such as Project Agorá⁴ and Project Nexus⁵ by BIS (Bank of International Settlements) is set to improve operational efficiency, bring transparency and improve settlement speed to RTPs.

The expansion of cross-border instant payment systems has attracted significant attention from regulators, who aim to foster innovation and faster transactions without compromising financial security, consumer safeguards, fraud prevention, and compliance standards.

As RTPs become national critical infrastructure, Fraud, Scam and financial crime risks represent the most visible challenge within instant payment ecosystems as funds are transferred and settled within seconds, fraudsters can move stolen funds quickly before financial institutions have an opportunity to intervene.

Some of the most common challenges include Authorized Push Payment (APP) Frauds, social media enabled scams, account takeover and mule accounts. Incrementally organized crime syndicates have increasingly used sophisticated digital attacks to undermine instant payment systems through cyber-attacks.

Similarly, RTPs also can be exploited by money launderers to layer illicit funds rapidly, move proceeds through multiple accounts, obscure transaction trails and conduct structuring activities.

Sanctions compliance post significant challenges in RTPs and the U.S. Office of Foreign Assets Control (OFAC)⁶ has specifically issued guidance encouraging financial institutions operating instant payment systems to adopt risk-based sanctions screening frameworks that match the pace of real-time transactions.

A case can also be made that while payment systems are under threat, it may necessitate relooking at the entire digital ecosystem and shall not be limited to financial institutions in isolation as the above risks are often spread using social media that allows reach, anonymity and virality of deceptive content and exploitation of personal information. Hence, financial Institutions, telecom companies, internet service providers and social media should have shared responsibilities to manage and mitigate frauds and scams. Some initiative such as "scam signals"⁷ in UK, "Shared responsibility Framework"⁸ in Singapore, "Scam prevention framework – anti-scam intel loop"⁹ in Australia are steps in the right direction.

With the objective of building and retaining customer trust in evolving payment landscape, the need of the hours is to build cross-industry collaboration, data sharing, cross-regulatory interface and public-private forums that may support managing fraud and financial crime risks.

Some notable measures that can be assessed by organizations to manage and mitigate frauds and scams in RTPs include:

Preventive Measures:

1. Payee Verification that allows payer to confirm the intended recipient before initiating a transfer.
2. Utilize real-time transaction monitoring systems to identify suspicious transactions and delay or block them when necessary.
3. Invest in AI-enabled fraud detection tools that identify scams in real time and help customers recognize warning signs before losses occur.
4. Establish real-time alert mechanisms for payment mandate changes to enable rapid detection, assessment, and resolution of suspicious activity.
5. Conduct regular sanctions screening of customers against lists of individuals and entities subject to targeted financial sanctions. These checks must be conducted at least once per day.

Detective Measures:

1. Establish customer behavior baselines using - Typical transaction values, Device usage patterns and Payment timings.
2. Identify excessive activity within a short period through velocity monitoring - Multiple transactions per minute/hour, Repeated authentication attempts and Rapid account-to-account transfers.
3. Assign a dynamic risk score based on - Customer behavior, Beneficiary risk and Geographic risk.
4. Geolocation and IP Monitoring - High-risk IP addresses and Geographic anomalies

Responsive Measures:

1. Implement Multi-Factor Authentication (MFA).
2. Block Suspicious Transactions.
3. Contact receiving banks/payment providers to request fund recall or account freeze.
4. Add transaction limits for high-risk transfers.
5. Reimbursements for fraud victims to improve consumer confidence and create incentives to strengthen fraud controls.
6. Regulatory reporting to assess institutional effectiveness and support in building private-public coalition to counter abuse of payment systems.

Supported by Viren Gupta – Manager, Forensic Services, KPMG in India

All views, opinions, and ideas presented are solely the author's own and do not necessarily reflect those of any organization or employer

¹ Global Real-Time Payments Growth “Sustainable” As New Use Cases Push Transactions to Record Highs – ACI Worldwide Report | ACI Worldwide

² Retail payments supervision and access to Real-Time Rail - Bank of Canada

³ Press Note Details: Press Information Bureau

⁴ Project Agorá: exploring tokenisation of wholesale cross-border payments

⁵ Project Nexus: enabling instant cross-border payments

⁶ Sanctions Compliance Guidance for Instant Payment Systems

⁷ Mobile and Banking Industries Join Forces to Fight Fraud - Connected Fintech

⁸ Implementation of Shared Responsibility Framework | IMDA

⁹ New Australian anti-scam sharing technology unveiled