



White paper

A Perspective on Fraud-Resilient Real-Time Payment (RTP) Hubs with Multiple Clearings

It's a moment of critical change for the payments industry, in which account-to-account (A2A) rails and Real-Time Payments (RTP) are gaining market share. While customers value the speed and convenience of RTP directly to other accounts, its unique character requires innovative implementations that are fraud-resilient. Here's how banks & other financial institutions (FIs) can formulate a strategy to securely orchestrate transactions with multiple new RTP clearings.

RTP addresses the shortcomings of both cash & EFT

Ever since money was invented in the 7th century BC, exchanges of paper, metal, and other forms of hard currency have been convenient ways to pay in real time for everyday purchases. Even with the introduction of checks and credit cards, cash is still used to conveniently exchange funds in an immediate fashion. However, cash's ease of use also has its challenges, such as printing, storage, and circulation. Additionally, consumers bear costs for check-cashing and ATM withdrawals. Further, cash also introduces societal risks, such as counterfeiting and tax evasion.

While electronic fund transfer (EFT) methods can address most of the burdens of cash, they're not helpful for immediate liquidity, which is one of the reasons RTP has ascended so dramatically (there are other factors as well, including modern-day smartphones' ability to enable consumers to conduct transactions anywhere). With RTP, consumers and businesses can immediately send and receive funds electronically through their financial accounts at any time—24/7/365.

Some of the key characteristics of RTP:

- **Availability:** Customer can send and receive payments anytime, including after hours and holidays.
- **Speed:** Fund is transferred from sender's account to recipient's account within seconds.
- **Irrevocability:** Once authorized, payments cannot be revoked by sender.
- **Standardized message format:** Most of the RTP systems have been implemented following the ISO 20022 message format. Some banks/FIs have yet to implement the format but most plan to migrate soon.
- **Cash flow control:** Immediate send and receive features gives customer better control over their cash flow and liquidity management.

The number of global RTP systems continues to grow

More and more countries are launching new RTP systems every year. Some countries, such as India, a leader in payments innovation, have more than one RTP Clearing and Settlement Mechanism (CSM), including IMPS & UPI. In July 2023, the U.S. Federal Reserve launched FedNow as an alternative to the existing CSM, known as the RTP Network of The Clearing House (TCH).

Global banks, regulators and governments are now providing even more sophisticated RTP options for businesses as well as individual payment consumers to fuel economic growth. Banks operating in RTP ecosystems with multiple CSMs typically have the option to integrate with more than one, although doing so incurs additional complexity and cost.

According to FICO's recent global survey:

90%

Of more than 14,000 consumers from 14 different countries polled have used RTP

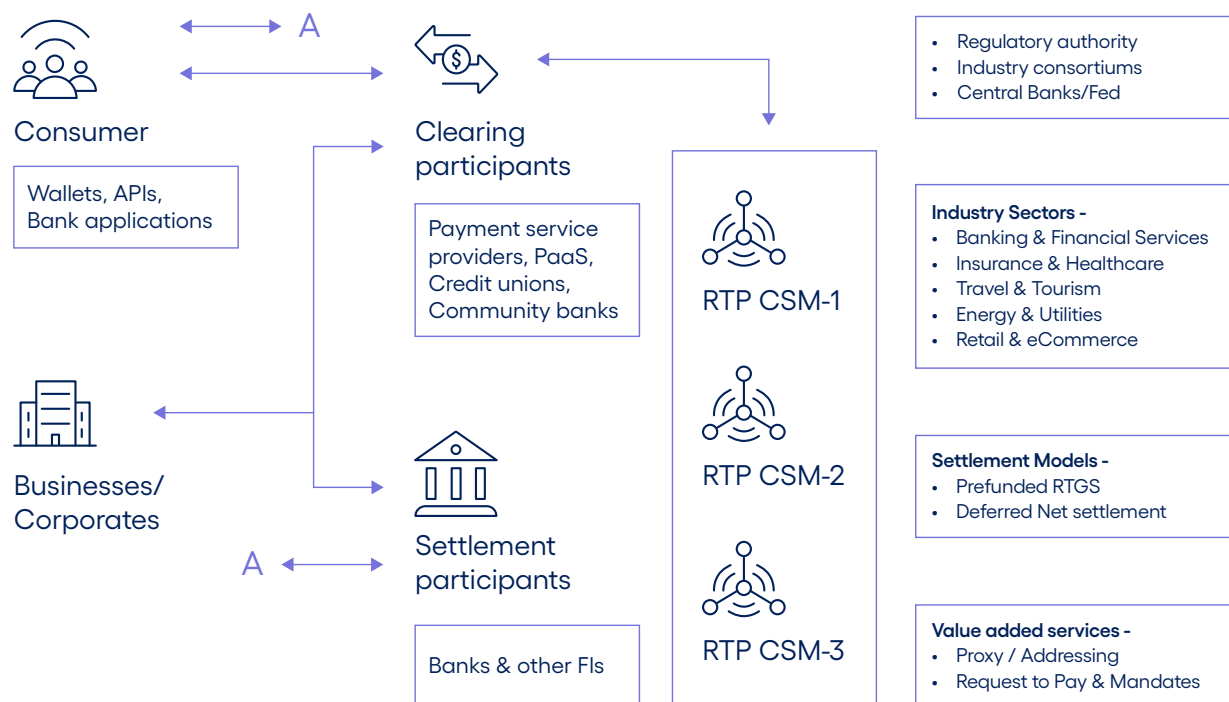
38%

Use RTP more than five times per month

88%

Plan to maintain or increase use of RTP in the coming year

Participants and stakeholders in advanced domestic RTP environments typically manage multiple CSMs.



Banks & Payment Service Providers (PSPs) have strong business cases for integrating with multiple RTP CSMs for both domestic & international payments

Participating in more than one RTP clearing grants the ability to transact with more counterparties, which invariably attracts a larger customer base.

More CSM integration means further reach

Integration with a single CSM opens doors for transactions with all other participating banks & PSPs. And each additional CSM integration multiplies the network, securing an even larger customer base.

Newer innovations like Request For Payment (RFP) have the potential to be a game-changer

FIs and customers can use RFPs to unlock additional value in a variety of use cases. Other evolutions, such as businesses being able to present bills through mobile banking apps, or customers transacting with single-step, prefilled payment forms, will provide more convenience.

RTPs are becoming the norm for corporations and institutional clients

As more consumers have grown accustomed to digital payments for sending and receiving money instantaneously, the trend is now attracting corporations and institutional clients as well. To meet this demand, FedNow has launched A2A and consumer-to-business bill pay services, and more offerings are in the works for the B2B, B2C & C2B sectors.

The promise of International RTP

Many FMs have begun enabling instant cross-border payments. For example, BIS Nexus is connecting Europe's TIPS with ASEAN-5. Elsewhere, Singapore and Indonesia have a cross-border QR code-based payment already in place. These regional networks bring additional opportunities for banks & PSPs to capture an international client base.



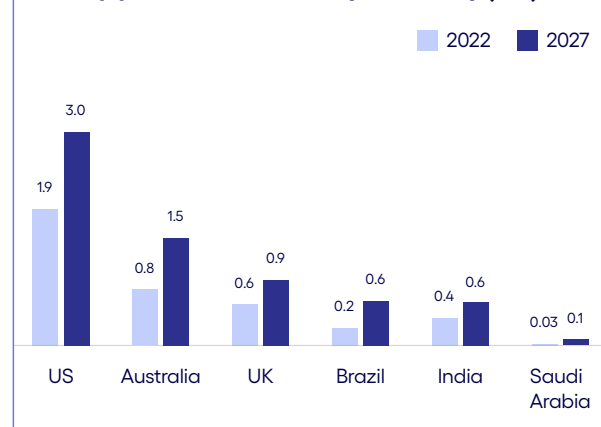
Multi-clearing RTP increases the chances of fraud exponentially

A global wave of scams has paralleled RTP's rapid adoption, resulting in more consumers suffering significant losses.

- Financial crime and fraud are projected to cost banks and financial institutions \$40.6B globally by 2027 on annual basis.
- In 2022, 20% of all consumers worldwide were victims of payment fraud, of which ~27% was [Authorized Push Payment \(APP\)](#) fraud.
- APP fraud losses are expected to climb to \$6.8B by 2026 at a CAGR of 11% (2022-27) across six major RTP markets (US, UK, India, Brazil, Australia and Saudi Arabia).

RTP fraud projections 2022-2027

App fraud losses by country(\$B)



Source: paymentscardsandmobile

A **fraud-resilient integrated solution approach** is required for creating instant payment hubs or enabling instant payment rails that process domestic RTGS, ACH or SWIFT transactions. Through RTP rails, money transfers arrive immediately and irrevocably, thereby necessitating powerful fraud prevention safeguards that stop suspicious transactions before they take place.



In a world of RTP and settlement, fraud prevention must be quicker than the fraudsters. Anti-fraud measures must be in sync with the latest consumer behaviors, which requires a holistic, AI/ML-based approach to detection and prevention.

How can fraud be detected even before the payment hits the payment hub?




































Network & counter-party collaboration is the key – sharing the data characteristics of fraudulent transactions through the Payment Market Infrastructure (PMI) service is essential for combating counter-party fraud and will provide better protection for end-customers.

Additional **AI/ML-based suppression layers of protection** against sophisticated threats would help detect and block [RTP fraud](#) with granular precision, reducing losses and improving approval rates. Detection of network decoding traffic and deploying firewalls to block suspicious transactions are some techniques for managing fraud early in the lifecycle.

APP fraud is the most prevalent type of RTP fraud

APP fraud, in which scammers pose as legitimate financial entities and trick consumers into authorizing credit transfers into fake accounts, has become the most prominent version of fraud in the world of real-time payments. But as you can see in the table below, there are many permutations of RTP scams.

Likelihood of various scams across RTP use-cases.

APP Scam/ Use-case segments	Use-case segment →	Account-to-Account credit transfer (A2A)	Consumer-to-Business bill pay (C2B)	Business-to-Business (B2B)	Consumer-to-Business (C2B)	Business-to-Consumer (B2C)
APP SCAM types ↓	Typical transaction types →	Me to Me prepaid card load wallet funding Cash Pooling	Pay bills E-invoicing	On-demand payment E-invoicing	Home service payment E-commerce	One-time payments immediate payroll
Purchase scam	Victim pays in advance for goods or services that are never received.					
Investment scam	Victim pays for a fake investment or fund.					
Romance scam	Victim pays a person with whom they believe they're in a relationship.					
Advance fee scam	Victim pays a fee in hopes of a larger return in cash or kind.					
Invoice & mandate scam	Victim pays for a legitimate invoice in a fraudulent account.					
CEO scam	Scammer impersonates a CEO or other high-ranking official.					
Impersonation scam	Scammer poses as the police, the IRS, the victim's bank, etc.					

Critical fraud resiliency considerations for a multi-CSM RTP solution



Modernized scam detection techniques for RTP fraud

Although scams have existed for decades, RTP gives fraudsters a new way to get money immediately and irrevocably from their victims. Average RTP transaction values are relatively small, which makes them easier to go undetected. And due to their instantaneous nature, fraudsters can quickly move the stolen money through multiple account “hops,” adding to the difficulty of tracking and recovering the funds. Moreover, RTP fraud doesn’t require an account takeover the way many prior-generation scams did, leaving fewer suspicious indicators to detect. Thus, RTP scams have rendered many of the traditional fraud prevention models obsolete.

As a result, customized real-time ML techniques are necessary to build features that help confirm the identity and intentions of the sender. Ultra-modern ML techniques, such as specialized behavior-sorted lists (B-lists) can determine the probability that the debit party is the authentic originator of the payment. B-lists also monitor key attributes of the originator’s payment history and isolate similar repeated behaviors (i.e., “favorites”), thus learning what constitutes normal behavior for an originator (and, conversely, what are suspicious anomalies).



Payment Command Centers guided by customized rule sets

Given the immediate nature of RTP, the major challenge for banks and PSPs is finding a way to act instantly after detecting a scam. First, the right interdiction support must be baked into the payment flow for all RTP CSMs. Classifying detected fraudulent transactions against a pre-defined and agreed upon taxonomy for each participating RTP network is difficult for any risk scoring engine. Thus, it’s crucial for PMIs to separate authorized transactions from push-payments in order to apply the appropriate rule set. In fact, not only does the entire process of interdiction and regulatory reporting & compliance depend upon the classification rules defined by the PMIs for the CSMs and participating banks and PSPs, but those rules usually evolve over time. Therefore, any fraud detection and command action software needs to be easily customizable in order to support rule updates.

Setting up a separate RTP command center that can employ automated responses based on the appropriate (and easily updatable) scenario-driven rule sets should be a critical consideration for banks & PSPs that process a large volume of RTP transactions.

Critical fraud resiliency considerations for a multi-CSM RTP solution (cont'd)



Stakeholder collaboration strengthens data modeling

Stakeholders should share their enhanced data and intelligence, as well as collaborate in order to reduce fraud more effectively. Solution design can also foster collaboration by allowing easy API access to third-party providers, making data source modification easier.

Integration with credit bureaus is crucial for sourcing individual and corporate credit history, eligibility scores, credit types, interest rates, and more. Access to PMI data—including fraudulent transaction history, watchlists, compliance metadata, and settlement reports for both domestic and cross-border transactions—is also of utmost importance. Finally, several third-party firms and organizations can source know-your-customer (KYC) information, aggregated transaction data, channel data, financial information data, and ratings. Banks and PSPs should always seek out ways to make their intelligence more comprehensive, and they should be supported by a solution that facilitates connectivity to these data sources.



Leverage both internal and RTP network data & controls

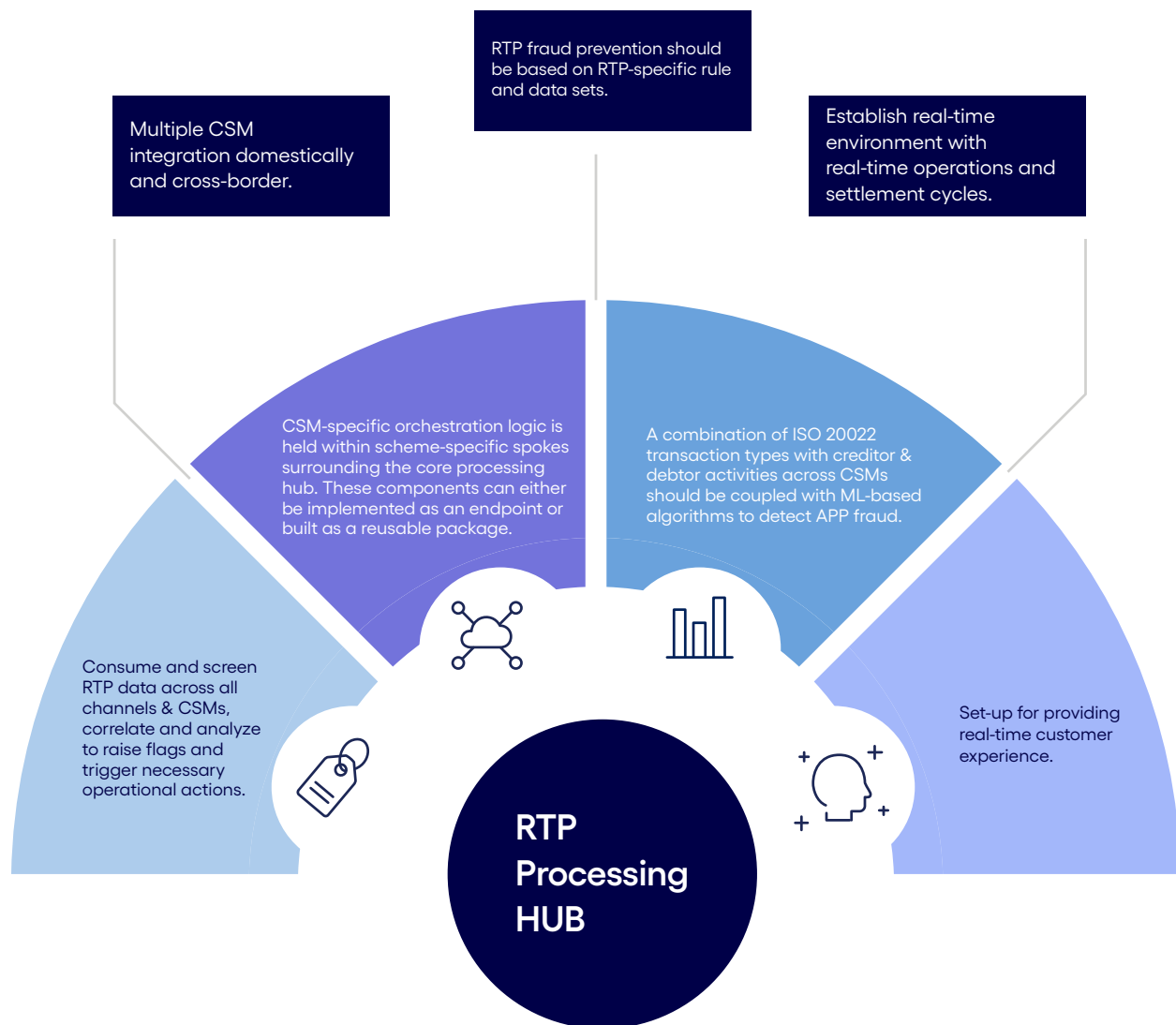
Instant PMIs like FedNow provide certain capabilities for preventing fraud through various transaction limits (network- and participant-level) and through participant-defined negative lists. Typically, network-level limits are defined by the PMI, whereas participant-level limits are set by banks and PSPs. Participating banks & PSPs need to fully leverage these capabilities to fight RTP fraud.

In terms of internal tooling, transactional fraud models have been very effective in fighting account takeovers, CNP fraud, etc. However, RTP transaction fraud requires more sophisticated tools to detect scams that fall in a more ambiguous area that will often look like authentic transactions. The best approach to tackling this problem is a consortium-based model that detects anomalies in the consumer's behavior and fed by the data sources we've discussed.

The hub-and-spoke approach to fraud-resilient RTP solutions

A centralized RTP Hub houses the business logic for payment processing, while RTP scheme-specific orchestration and transformation occurs at the spokes.

Many PMIs have launched RTP CSMs with basic credit transfer solutions that include push- and pull-type scenarios for C2C, B2B, B2C & C2B sectors, as well as value-added services (e.g., credit transfer initiation through proxy/addressing-based payments, request-to-pay-initiated transactions using QR code and mandate-based RTP). Banks and PSPs should review all value-added services and strongly consider supporting them in addition to their core RTP-processing engine.



Capability anatomy of a futuristic fraud-resilient RTP processing solution

Payment ordering

Payment receipt

Debulking of files

Bulking of files

Message switching & routing

Payment object generation

Translation services

Data capture

Parsing & transformation

Orchestration

Structural validation

Qualification

Protocol conversion

RTP processing & orchestration

Data transformation

Duplication checking

Functional validation

Authentication

FX handling

BPO & Workflow manager

Workflow optimization

Prioritization

Liquidity & risk check

Exception handling & reporting

Enrichment (Personalization)

Automated & manual repairs

Routing to CSMs

Release scheduler

Booking & posting

Advising (Pricing)

Pricing & billing

Audit Logs

Returns matching

Reporting & reconciliation

RTP fraud solution

Real-time behavioral profiling

Adaptive analytics

Identity resolution

ML execution

Contextual processing

External data access

Connectivity & integration (Adapters)

To enterprise/ common services

To payment networks

Rule management

Case creation

Automated decision

Hotlists & queues

User management

Reports & audits

To core banking systems

Payment interfaces for channels



Bank payment hub capability



RTP scheme orchestration capability



RTP fraud solution capability

Design considerations for an RTP processing hub supporting multiple CSMs

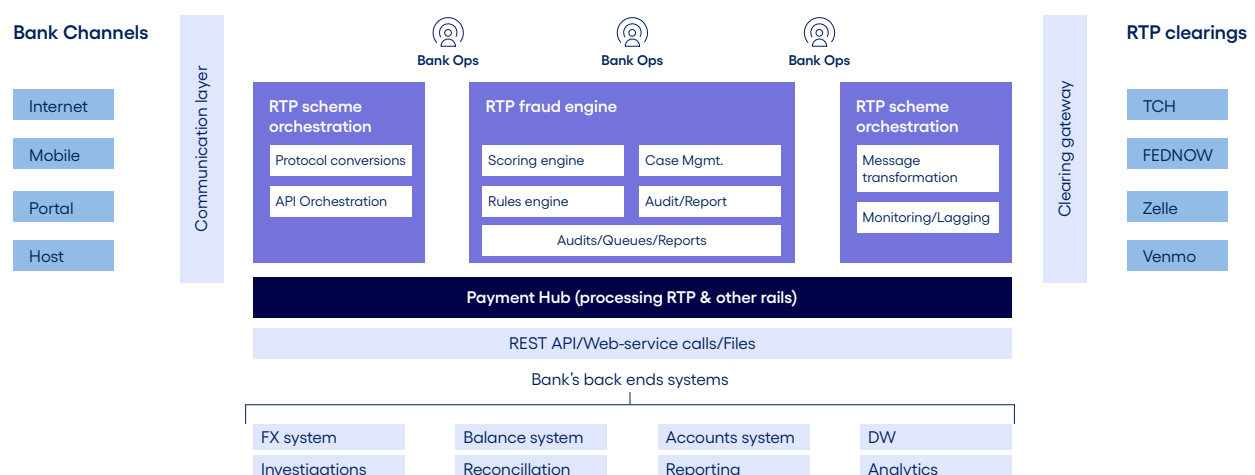
Architectural and Transition/Migration Considerations:

- **Managing all RTP transactions through a hub solution** should be the default approach for integrating new RTP CSMs and new protocols issued by existing CSMs.
- **ISO 20022** should be adopted as the internal message formatting of the RTP hub—it's what most organizations are on or will likely adopt.
- **Translation and orchestration** solutions need to be configurable and easy to scale. This allows legacy systems to coexist with the new messaging standard and aid in gradual transition from a fragmented ecosystem to a standardized target architecture.
- **Employ a sound framework** for selecting your solution – ensure you prioritize considerations such as the supporting RTP CSMs, geographical coverage, NFR requirements, etc.
- **Develop a detailed data transition plan and prepare for contingencies.** The process of data mapping from existing channels to a new RTP CSM transaction processing hub can lead to data truncation and other snags—test rigorously during the transition and be ready to troubleshoot.
- **Take an iterative approach to your RTP transformation.** You will want to roll out your RTP hub in phases, especially if you're participating in multiple CSMs. This is primarily to ensure you maintain interoperability with your back-end systems and third-party services.

Integration priorities

1. **Seamless integration** – analyze the modernization needs for your back-office transaction processing systems and design a solution with easy access to FinTech services, including AML and compliance.
2. **Modernized payments orchestration** – the objective is an independent, well-bounded capability set that leverages reusable microservices across multiple clearings, both in-country and cross-border.
3. **Connected case management** – ensure your solution links each component (payment flow orchestration, translation, transformation & fraud management) to gain a complete, 360° customer view.

A sample logical system components view of a fraud-resilient, multi-CSM-orchestrating RTP hub



Implementation considerations

At this point, it should be clear that transforming to a fraud-resilient RTP processing system that supports multiple CSMs is complex. We've covered several key considerations, including modernizing your fraud detection protocol, integrating your existing CSMs with new ones, designing the optimal target architecture, and more. Before executing your transformation, there are four implementation factors that you'll need to consider, and they're just as crucial to your transformation as everything else we've discussed.

1. Choose between managed cloud vs on-prem

Typically, on-prem solutions for RTP fraud management are highly customized for each CSM in the network. These CSMs typically require frequent regulatory updates and new feature launches to keep up with changing customer expectations. Rolling out changes on a custom solution can quickly become an application value management nightmare. Managed cloud solutions, by contrast, require less customization and can update simultaneously.

2. Work with experts

Many critical factors (e.g., data protection during information exchanges in financial messaging) need adequate planning and execution by industry experts. Robust data protection and privacy policy compliance with regulatory standards such as GDPR, PCI DSS and SWIFT CSP require global program management, all of which can be facilitated by an experienced implementation partner.

3. Focus on ISO 20022 native models

Almost all new RTP systems follow ISO 20022-based message types or similar. This promotes routing interoperability with other instant payment services, domestically and cross-border. ISO20022 is highly structured, data-rich, and offers a standardized set of rules and practices. Its structured payment methodology helps increase interoperability and its rich payload increases routing and fraud decisioning accuracy. Consider canonicalizing the payment solution based on an ISO 20022 native format.

4. Consider proven market-leading vendor products rather than building from scratch

Implementing an enterprise-grade payment hub & fraud risk management platform with advanced ML-based RTP scam detection and workflow capability could have severe consequences if mismanaged. There are already solutions available with the ability to engage and confirm with payment debtor and creditor in real time for both push- and pull-RTP flows. Seek to minimize customizations with out-of-the-box solutions already have the appropriate scheme-specific rule sets defined.

Authors



Krishanu De

Sr. Director – Head of Payments
Risk & Compliance Industry Solutions
Cognizant

Krishanu.De@cognizant.com

<https://www.linkedin.com/in/krishanude/>



Manan Gauba

AVP - Head of Strategy and Partnerships
Banking and Capital Markets
Cognizant

Manan.Gauba@cognizant.com

<https://www.linkedin.com/in/manangauba>



Fabricio Ikeda

Sr. Director – Partner Solutions
FICO

FabricioIkeda@FICO.com

<https://www.linkedin.com/in/fabricioikeda/>

Learn more about FICO at www.fico.com



Cognizant helps engineer modern businesses by helping to modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. To see how Cognizant is improving everyday life, visit them at www.cognizant.com or across their socials @cognizant.

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB
England
Tel: +44 (0) 20 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraiakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (0) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Tel: +65 6812 4000

© Copyright 2024, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission of Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned here in are the property of their respective owners.