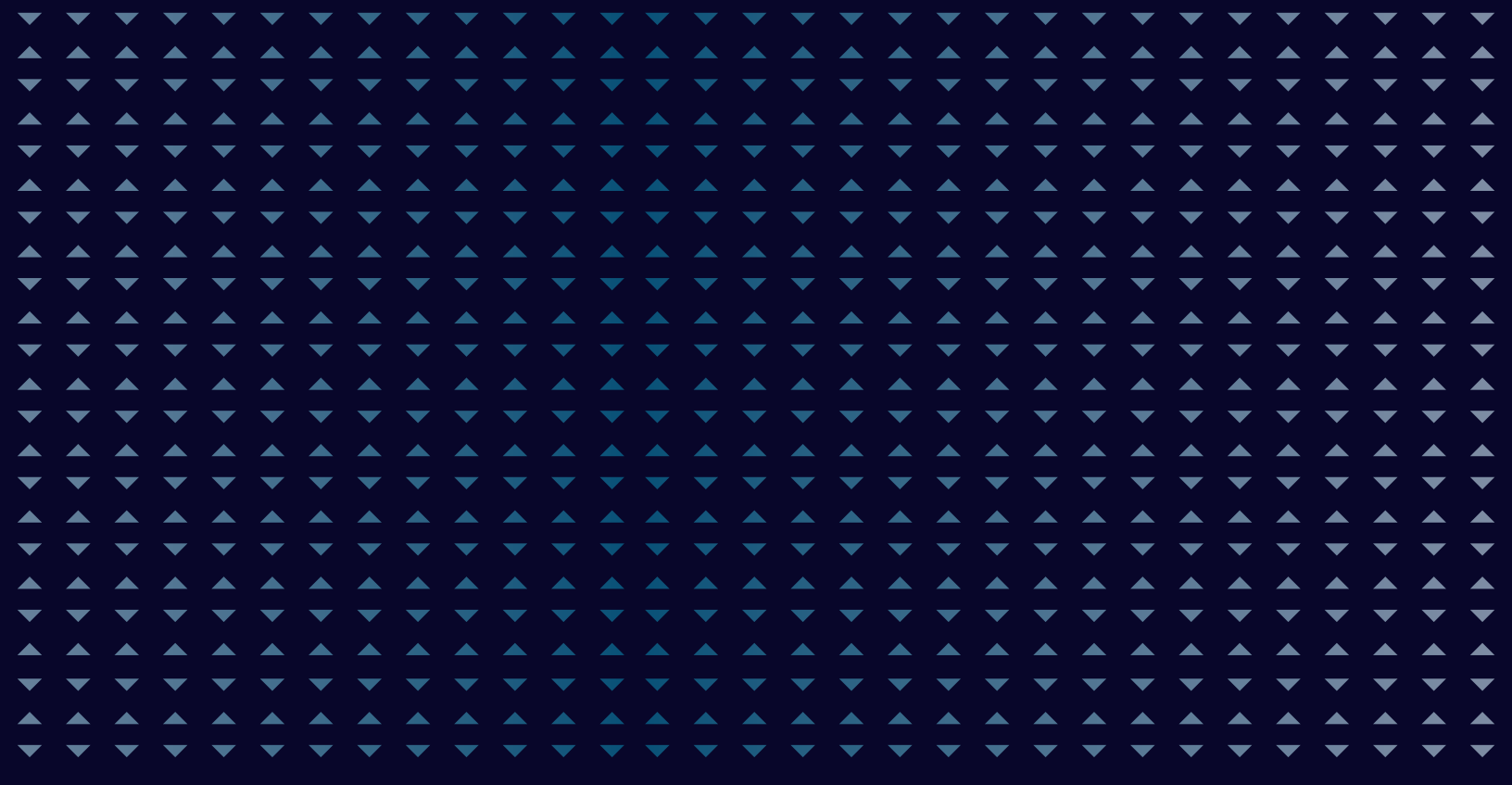
Nasdaq Verafin

Shifting Liability: Authorised Push Payment Reimbursement Models

Fighting Fraud in Global Real-Time Payment Systems

By Jonathan Frost,
Fraud and Cybercrime SME



Contents

$485.6B
in losses

Americas
$151B

Asia-Pacific
$221B

Europe, Middle East and Africa
$113B

Global Fraud Trends and Reactions

Fraud is a growing problem impacting economies around the world. As the race to incorporate new technologies into the financial system increases, financial institutions are left to balance the increasing expectations of their customers and the evolution of fraudsters exploiting gaps in the system.

As new fraud plays, led by authorised push payment (APP) scams, permeate online digital marketplaces and personal interactions, the consumer-focused aspects of payment platforms offering real-time transactions have become a significant vector for fraud.

As the financial system looks to self-correct through new regulations aimed at protecting the consumer good, the increase in liability placed upon financial institutions requires a more focused response to help mitigate fraud, while maintaining the customer experience.

Call and Response: The Case for Change

Recently, the Nasdaq Global Financial Crime Report uncovered that global fraud losses from individual and bank scams totalled $485.6 billion (USD) in 2023.[1]

With the continual growth of fraud year-over-year, the financial industry is responding through new regulations, enhanced prevention, and detection, while balancing increased customer expectations.

Typically, fraud is viewed through two lenses — unauthorised and authorised. While most jurisdictions have well-established regulations or laws to protect customers from unauthorised fraud linked to activities such as identity theft, stolen bank cards or account takeover scenarios, the United Kingdom (UK) is set to be the first

> "Authorised push payment scams happen when a person uses a fraudulent or dishonest course of conduct to manipulate, deceive or persuade someone into sending money to an account outside of their control."
>
> – Payment Systems Regulator

1 Nasdaq, Global Financial Crime Report, 2024

jurisdiction to address authorised fraud through regulations that compel financial institutions to reimburse their customers. This step places increased fraud prevention and detection on the shoulders of financial institutions, in addition to setting a global precedent in response to increased APP fraud.

The Rise of APP Fraud: Shifting Tactics

As financial institutions increased prevention and detection methods in remote channels, the volume of unauthorised fraud fell by 21% in the UK, leading to a corresponding fall of 7% in associated losses between 2023–2024.[2]

However, with that change in focus by financial institutions, criminals shifted their attention and focus away from the bank and placed it on their customers. This move unsurprisingly resulted in a growth in the volume and value of fraud involving the use of social engineering tactics that push consumers into authorising payments through numerous fraud and investment scams.

Consequently, many financial institutions adopted a more aggressive risk posture in their payment channels, with losses associated with APP fraud initially falling by 17% in the UK from 2021 to 2022.[3] However, in 2023 the reduction was a mere 5%,[4] demonstrating the need for continued vigilance on the part of customers and more innovative approaches to risk management in payment channels.

In the UK, this continued growth in APP fraud and external pressure from consumer advocates has ultimately resulted in a shift of liability away from consumers to the financial institutions.

Real-Time Payments: An APP Catalyst

Real-time payments (RTP) — also known as fast, instant, immediate, or rapid payments — allow account holders to transfer money 24/7/365, with the beneficiary generally receiving immediate access to the funds.

According to Grand View Research,

"the global real-time payments market size was valued at $17.57 billion in 2022 and is predicted to grow by 35.5% from 2023 to 2030."[5]

According to the World Bank,[6] more than 100 jurisdictions had live RTP solutions in place as of June 2022, with implementations either replacing existing payment systems or providing an entirely new standalone solution.

2 U.K Finance, 2024 Annual Fraud Report.

3 UK Finance, Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online, 2023.

4 U.K Finance, 2024 Annual Fraud Report.

5 Grand View Research, Real-Time Payments Market Size, Share & Trends Analysis Report By Enterprise Size (Large, SME), By Payment Type (P2B, P2P), By End-use Industry, By Component, By Deployment, And Segment Forecasts, 2023—2030, 2023.

6 The World Bank, Project Fast

RTP channels offer consumers and businesses significant convenience, speeding up commerce and contributing to economic growth. The positive attributes of RTP also make it equally as attractive to criminals, increasing the risk of fraud and money laundering.

The Payment Systems Regulator (PSR) in the UK noted that 0.1%[7] of the volume of payments in 2021 were fraudulent in nature, not a trivial amount when taken in the context of 3.4 billion payments made with a total value of GBP £2.6 trillion.[8]

The UK provides strong evidence that criminals have migrated to RTP systems, with statistics suggesting that over 90% of APP losses in the UK make use of RTP[9], a trend[10] that is also seen in losses linked to unauthorised fraud.

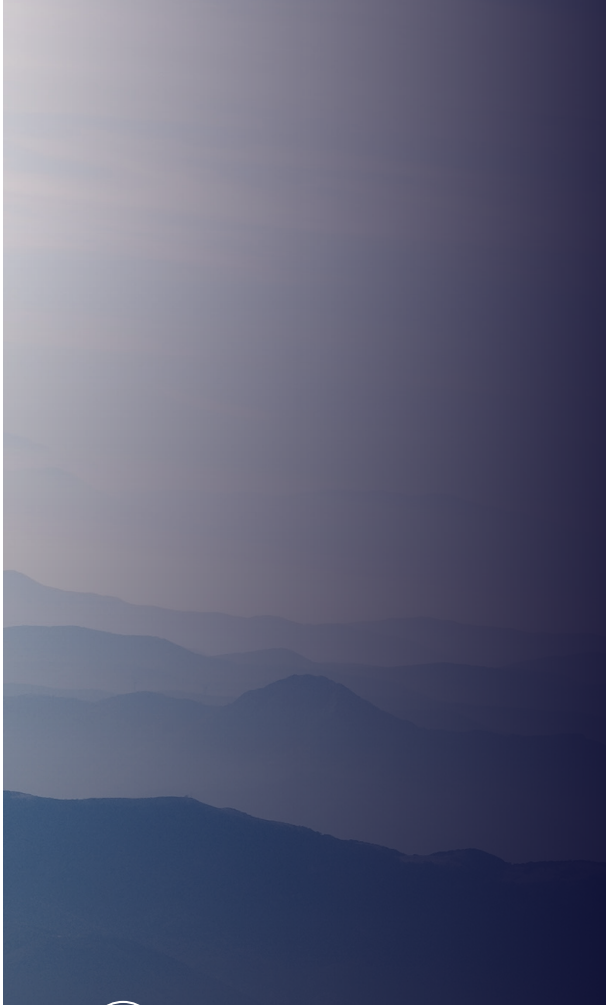
The UK's Real-Time Payment Journey

In the late 1990s, the UK began to lay the foundations for RTP with the aim of replacing the Bankers' Automated Clearing System (BACS) which typically made funds available after three days.

In May 2008, the Faster Payments System was launched, a solution that guaranteed available funds within hours and typically took mere seconds. It is widely believed to be the first truly 24/7/365, real-time payment system in the world.

Today the Faster Payments System facilitates payments of up to GBP£1 million (where permitted by the financial institution) and has become a ubiquitous fully embedded RTP solution. Following efforts by regulators and the industry, the number of participating institutions has increased, with the first non-bank participant[11] joining in 2018.

In 2023, Faster Payments processed more than 4.5 billion payments worth GBP£3.7 trillion[12] — by any measure Faster Payments has proven to be a significant success. Most UK consumers take for granted that payments are posted in seconds, that the service is available 24/7/265, is final and offers them the flexibility to send large payments.



Unfortunately, Faster Payments has also proven equally attractive to criminals with APP fraud resulting in losses averaging GBP£492 million per annum since 2019 when measurement commenced. It is a significant part of the £1.17 billion loss incurred by the industry when you also factor in unauthorised fraud.[13]

7 Payment Systems Regulator, Fighting authorised push payment fraud: a new reimbursement requirement, 2023.

8 Pay.UK, Faster Payment System statistics.

9 Payment Systems Regulator, Authorised push payment (APP) fraud performance report, 2022.

10 UK Finance, Annual Fraud Report 2023, 2023.

11 UK Finance, Unlocking the future of faster payments.

12 Pay.UK, Faster Payment System statistics.

13 UK Finance, 2024 Annual Fraud Report.

Advantages and Disadvantages of RTP Channels

Speed of Posting: Funds are typically available to beneficiaries in seconds, creating a very small window in which a sending financial institution can undertake fraud or money laundering checks. If a transaction is allowed to proceed, the likelihood of repatriation is also significantly degraded with criminals utilising the speed of RTP to layer the proceeds of their crime.

24/7/365 Availability: While offering customers the convenience of availability, criminals operating outside the waking hours of your customers will likely reduce the opportunity to spot and report fraud. This creates additional operational challenges for financial institutions that will need to manage fraud and money laundering alerts in real-time 24-hours a day.

Payment Finality: Most RTP systems do not support the reversal of payments, providing consumers with a sense of security when compared to traditional methods of payment such as cheques. The other side of this finality is that it can often be difficult for fraud or errors to be addressed. Payment Systems Providers (PSP) that attempt to engage with the recipient institution inevitably take on operational costs and, in the event of the funds being repatriated, a liability by way of an indemnity.

High Transaction Limits: Many RTP systems support high transaction limits, enabling them to meet the needs of consumers and businesses. The ability to send large-value transactions also makes them attractive to fraudsters.

Geographic Scope: While the majority of RTP systems are currently national in scope, 2024 will mark the arrival of the cross-border Single Euro Payments Area (SEPA) Instant Credit Transfer within the eurozone with non-eurozone markets to follow in 2026. This increases the opportunity for fraud on instant payment channels across a broader geographic area.

APP Reimbursement: Shifting Liabilities

While becoming a victim of any form of fraud can cause distress, most unauthorised fraud in the UK is promptly reimbursed. Historically customers who incurred a loss because of a transaction they authorised were not reimbursed, but in 2019 this changed with the introduction of the Contingent Reimbursement Model Code for Authorised Push Payment Scams which required 10 institutions (which covered 21 UK banking brands) to reimburse victims of APP fraud.

The UK's APP commitment to implementing full reimbursement will come into force in October 2024 when provisions in the Financial Services and Markets Act 2023 require all in-scope PSPs to reimburse their customers who become victims of APP fraud.

The Journey to Reimbursement

So how did the UK become an outlier in the world of APP reimbursement regulations? The answer is simple, customer demand and the use of a provision within the Enterprise Act 2002 that enabled Which? (also known as the Consumer Association) to launch a super-complaint in 2016 against the banking sector.

Which? Super-complaint

In their submission Which? stated:

> "UK consumers and businesses rely on using payments services and payment systems every day. Consumers' confidence in payments is important for the economy and consumer welfare.
>
> Yet when consumers are subject to sophisticated scams and are tricked into transferring money to fraudsters via 'push' payments (such as Faster Payments) banks do not provide the levels of protection that they could — and that they typically do provide for other types of payment.
>
> The sums involved are often large and can be life-changing for the victims. The use of push payments is growing and likely to grow further as new push payment services are introduced, increasing the risk of such scams."[15]

"A Super-complaint, as defined by section 11(1) of the Enterprise Act 2002 (EA02), is a complaint submitted by a designated consumer body that 'any feature, or combination of features, of a market in the U.K. for goods or services, is or appears to be significantly harming the interests of consumers."

– GOV.UK[14]

15 Which?, super-complaint: Consumer safeguards in the market for push payments, 2016.

14 GOV.UK, What are super-complaints?, 2015

Payment Systems Regulator Response

Acting on the super-complaint, the PSR put in motion a response that addressed the concerns raised by Which? based on the following key findings:

- The way banks worked together to respond to scams needed to improve.
- There was evidence to suggest more could be done to identify fraudulent incoming payments and prevent accounts from being under the influence of scammers.
- The data available on the type and scale of scams is of poor quality.[16]

The 2023 Financial Services and Markets Act will require all in-scope PSPs to reimburse APP losses. Effective October 2024 the new mandatory regime states:

- Reimbursement applies to individuals and micro enterprises.
- APP losses of up to GBP£415K to be reimbursed promptly, with PSPs allowed to place an excess of GBP£100 on claims*.[17]
- The cost of reimbursement is to be split 50/50 between the sending and receiving PSPs, encouraging both parties to risk assess outbound and inbound payments.
- Customers must adhere to the customer standard of caution (gross negligence), heeding warnings, reporting promptly (to the bank and police where appropriate), and providing requested information to support their claim.
- Customers who are specifically told that their payment is a scam will not be covered, unless they are deemed vulnerable,[18] in which case they will be reimbursed and not subject to an excess.
- In May 2024 the PSR launched a consultation that indicated the inclusion of CHAPS payments in the post October 7th rules; international payments remain out of scope for reimbursement.
- Transfers within a financial institution are also excluded, but banks are encouraged to treat these as an APP.

As with jurisdictions such as Australia and Singapore, the UK Government has also emphasised a response to APP which extends beyond the banks.

Voluntary arrangements include "Charters" which set out how various sectors should address fraud risk, the most recent of which was the Online Fraud Charter. This follows similar undertakings in conjunction with the telco, banking, and legal/accountancy sectors.

Uniquely the UK has also gone further, seeking to address a wide range of online harms through legislation. The Online Safety Act creates requirements for online platforms to remove harmful content from their search, paid and unpaid services. The Act is complimented by the introduction of the Online Advertising Programme which aims to ensure that ad networks do not cause harm.

It remains to be seen what impact this multi-layered approach will have on APP fraud, but the PSR has mandated three metrics which will provide significant transparency.

- Metric A – Reported APP fraud losses reimbursed.
- Metric B – APP transactions sent.
- Metric C – APP transactions received.

PSPs are required to report both the volume and value of each metric with a percentage per million transactions used to contextualise Metric C.

These will be reported annually with the first report covering 2022.[19]

16 Payment Systems Regulator, Which? super-complaint on payment scams, 2016.

17 *In 2022 the volume of purchase scams was 117K with a cumulative value of GBP£67M were reported to banks, of these 90% were under GBP£1K. Provision of an excess enables PSPs to exclude high-volume, low-value claims.

18 Financial Conduct Authority, Finalised guidance: FG21/1 Guidance for firms on the fair treatment of vulnerable customers, 2021.

19 Payment Systems Regulator, Authorized push payment (APP) fraud performance report, 2023.

Industry Precedent: Jurisdictional Overview

Regardless of the volume of fraud and money laundering found in each RTP system, the continued growth of fraud via RTP and the emergence of cross-border solutions necessitates that financial institutions across multiple jurisdictions adopt a change in their risk posture.

Reimbursement Models

Given that APP is a relatively new fraud phenomenon, most jurisdictions have a regulatory lag. This is true of those that have ubiquitous RTP and those who are proposing it.

Except for the UK, reimbursement is likely to be on a "goodwill" basis. Consequently, it is difficult to identify what proportion of APP victims are reimbursed as there is unlikely to be a regulatory obligation to report a goodwill payment.

APP fraud is a growing topic of discussion between the industry and regulators on a global scale, with many consumer protection groups expressing a desire to see movement towards a position akin to that of the UK.

United States

The Consumer and Financial Protection Board (CFPB) in the US only addresses unauthorised payments via Regulation E of the Electronic Fund Transfer Act (EFTA).

While APP fraud has been identified as a risk and is expected to grow within the US[20], regulatory bodies have yet to provide guidance on APP liability for financial institutions.

The US is a late adopter of RTP payment platforms. With the launch of instant payment rails RTP from The Clearing House and the Federal Reserve's FedNow Service, it can be expected that APP fraud scams and tactics already well established among other payment options will migrate into these RTP channels, taking advantage of fast, large-value transfers and the irrevocable nature of the platform.

Growth of RTP in the US is also occurring alongside increased political interest in the management of wire fraud, with the US Senate Banking Committee calling on banks to do more to protect consumers. US Senator Sherrod Brown and Jack Reed, recently wrote to the CEOs of JPMorgan Chase, Bank of America, Wells Fargo, and Citi, calling on them to "proactively monitor and prevent unauthorized and fraudulently induced transactions."[21]

20 Federal Trade Commission, The top scams of 2022, 2023

21 United States Senate Committee, Brown, Reed Push Big Banks to Protect Consumers from Wire Fraud, 2024.

Reference to fraudulently induced transactions could be seen as a signal that Senators are potentially ready to press US banks to offer customers similar protection to those seen in the UK.

Australia

There has been significant focus in Australia on the need to address the causes of APP, with the launch of a new National Anti-Scams Centre (NASC). Alongside this, the Australian Government has sought to coordinate an improved response from the public and private sectors, to prevent scams before they result in an APP.

In a move which echoes the UK's Fraud Sector Charters, the Australian Government has proposed a Scams Code Framework. While this is still in consultation, it is intended to ensure that regulated businesses prevent, detect, disrupt, and respond to scams.

The ePayments Code (Code) is a voluntary code of practice that regulates electronic payments including automatic teller machine (ATM) transactions, online payments, EFTPOS transactions, credit/debit card transactions and internet and mobile banking.

Administered by the Australian Securities & Investments Commission (ASIC) the ePayments Code explicitly does not address APP losses. While ASIC is not currently proposing to replicate the UK approach, it has emphasised the need for banks to address scams via Report 761, entitled "Scam prevention, detection and response by the four major banks." This highlighted that the banks detected and stopped a low proportion of scam payments (13%).

Looking toward the future, ASIC has also noted it "is supportive, in principle, of the suggestion to explore a model similar to the United Kingdom's Contingent Reimbursement Model Code."[22]

Brazil

As with Australia, banks in Brazil will generally reimburse for unauthorised transactions. The nature of crime in Brazil complicates matters with violent crime presenting the potential for transactions to be executed under duress.

Brazilian banks do not reimburse customers for losses arising from APP, nor do any of the insurance policies, with their focus being purely on losses that arise from incidents of violent crime.

The Instituto Brasileiro de Defesa do Consumidor (IDEC) has demonstrated a desire to focus on banking scams, especially those which involve the criminal impersonating a financial institution.

In a recent report[23] concerning the use of bank impersonation fraud, which was facilitated via remote access, IDEC noted that only one of three banks could detect and mitigate its use.

The report noted that Article 14 of the Consumer Protection Code and Summary 479 of the Superior Court of Justice require the other two banks to recognise that proven security flaws can cause consumer detriment. It also noted that there was a duty to repair such damage, by cancelling any loans and refunding any purchases or payments.

> "It is their duty to return the victim's money, cancel the loans and purchases made by scammers and restore the customer's good name."[24]
>
> – IDEC

While IDEC have not sought to address other forms of APP, it would seem likely that Article 14 could extend beyond bank impersonation, provided it could be demonstrated that the bank had an opportunity to prevent the loss.

22 Australian Securities & Investments Commission, REP 718 Response to submissions on CP 341 Review of the ePayments Code: Further consultation, 2022.
23 Instituto Brasileiro de Defesa do Consumidor, Golpe Do Celular Invadido: A Responsabilidade Dos Bancos E O Direito Dos Consumidores (Portuguese), 2023
24 Instituto Brasileiro de Defes a do Consumidor, Golpe Do Celular Invadido (Portuguese) Translated: "é dever delas devolver o dinheiro da vítima, cancelar os empréstimos e compras feitas pelos golpistas e retirar o nome sujo da vítima," 2023.

Canada

In Canada, the industry has committed to utilising guidance contained within the Canadian Code of Practice for Consumer Debit Card Services.

The Code provides scope for customers who are not at fault to receive reimbursement but does apply some expectations on customers with those not meeting them more likely to not be reimbursed. The sharing of one-time passcodes and the use of weak personal identification numbers are potential reasons why a customer might not be reimbursed.

The Code does not refer to APP scams or fraud, reflecting the environment in which it was authored. Canadian bank customers who are unhappy with a reimbursement decision can seek recourse via the Ombudsman for Banking Services and Investments (OBSI).

As an ombudsman, OBSI responds to complaints from customers. In 2023, it addressed a complaint from a consumer who was seeking redress on the basis that the receiving bank had contributed to the detriment. While the OBSI did not find against the bank it does indicate the potential for it to address authorised losses in the future.

European Union (EU)

In 2016, the EU saw the introduction of Payment Services Directive 2[25] (PSD2) which required the reimbursement of unauthorised payments and the introduction of strong customer authentication (SCA).

In 2022, the European Banking Authority published a Discussion Paper[26] outlining its preliminary observations on fraud data under the PSD2. This yielded some interesting points around "Credit Transfer Fraud" a category which is broadly equivalent to the concept of an APP:

- The total volume of credit transfer fraud is 29 times lower than card fraud.
- The value of credit transfer fraud is significantly higher than card fraud.
- Cross-border credit transfers make up a third of fraudulent transactions, but 2% of the volume.
- Fraud is higher for electronic payments than for non-electronic payments.
- 48% of credit transfer fraud involves the manipulation of the payer.

The last statistic, "48% of credit transfer fraud involves the manipulation of the payer," brings us neatly to the provisions within Payment Services Directive 3[27](PSD3), which for the first time includes limited reimbursement of authorised payments.

PSD3 does not propose universal reimbursement akin to that of the UK, but does put forward two situations in which reimbursement should occur:

1. If the payer requests verification of the payee, via IBAN Name Check, also known as Confirmation of Payee, and either the payer or payees' institution fails to do this correctly then the institution that failed will be liable.
2. If the payer has been socially engineered into authorising a payment by a third party who purports to be an employee of the payer's institution (Bank Impersonation Fraud) then the payer's institution will be liable for the loss.

These two scenarios came about following a consultation in which the EU considered and rejected reimbursement for other forms of APP. It is notable that the second scenario closely mirrors the provisions made in the Netherlands for bank help desk fraud — bank impersonation fraud — to be reimbursed on a "coulance" (goodwill) basis.

The reimbursement provisions within PSD3 should be of concern especially given the proposed arrival of SEPA Instant in 2024. A combination of speed and the opportunity for cross border transactions will make the blocking and repatriation of funds inherently more complex.[28]

25 European Central Bank. The revised Payment Services Directive (PSD2) and the transition to stronger payments security, 2018.

26 European Banking Authority, EBA publishes a Discussion Paper on its preliminary observations on selected payment fraud data under the Payment Services Directive, 2022.

27 Adyen, PSD3: What you need to know, 2023.

(Translated) "If a transaction contested by the user has been the subject of strong authentication, then it is up to the account holding establishment to determine whether this transaction can be considered authorized by the user. This analysis must be based on the various parameters associated with the transaction (origin of the transaction, strong authentication parameters, interactions with the payer, etc.), the existence of strong authentication not being sufficient in yourself to consider that the transaction has been authorized."[29]

– Banque de France

29 Banque De France, L'Observatoire de la sécurité des moyens de paiement émet des recommandations sur le remboursement des victimes de fraude, 2023

Inside the EU – France

While PSD3 seeks to address authentication and liability within the EU, it would be remiss not to acknowledge the role of regulators and the courts in parts of the single European payment area.

Regulators such as the Banque De France are already signalling that PSPs cannot solely rely on strong customer authentication to determine if a transaction was authorised, calling on PSPs to consider the customer's transactional behaviour.

Inside the EU – Nordic Region

In the Nordic region the Swedish Supreme Court has similarly signalled that consumers should expect greater protection.[30] The court determined that while a consumer may be negligent in disclosing authentication codes, the onus was on the bank to demonstrate that they "intentionally" gave the codes to a criminal.

This ruling creates scope for thousands of Swedish victims of bank impersonation fraud to see reimbursement and will likely result in an ongoing liability shift from the consumer to their bank.

Swish (RTP) and BankID are actively exploited by criminals with the Sveriges Riksbank noting in its 2024 Payments Report that, "there are also serious problems of fraud that risk undermining trust in the payments system."[31]

The trend for a shift in liability isn't limited to Sweden, with the Supreme Court of Norway[32] arriving at a similar conclusion. In a 2022 case the court concluded that a customer who was tricked into sharing their BankID password and codes was only liable for the first NOK 12,000 (USD $1090) of a NOK 153,240 (USD $13,930) bank impersonation fraud.

28 European Payments Council, Yearly update of the "Payment Threats and Fraud Trends Report", 2023
30 Högsta Domstolen, Konsument får ersättning av bank för obehöriga transaktioner som gjorts från konsumentens konto, 2022
31 Sveriges Riksbank, Payments Report 2024.
32 Supreme Court of Norway, A bank customer was not liable for the entire loss after BankID fraud, 2022
33 Credit Agricole, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, 2017

India

The Reserve Bank of India (RBI) introduced measures to limit customer liability in 2017. Entitled "Limiting Liability for Customers in Unauthorized Electronic Banking Transactions," the regulations required banks to reimburse customers for fraudulent transactions.[33]

It also placed expectations upon customers, requiring them to report the fraud within three days and demonstrate that they were not grossly negligent.

While there is currently no immediate indication that India intends to look at the reimbursement of authorised losses, the size and nature of the country have proven to make it a target for scammers.

The scope for losses within India's RTP system was highlighted in late 2023 when a group of cybercriminals set their sights on India's financial ecosystem and started advertising a malicious APP impersonating a bank headquartered in Tamil Nadu.

Between July and September 2023, the criminals accumulated INR 37 lakhs (USD $45K) using over 55 malicious Android apps.

To receive the loan, victims are asked to share personal information, including bank details and phone numbers and even to upload their national identity cards known as Aadhaar and tax-related Permanent Account Number (PAN) cards.

Once the fee is paid, the loan never materializes, and the fee is laundered through mules with funds flowing from India to China. Chinese payment gateways ensure the authorities cannot pursue the scammers.

Mules who have legitimate existing bank accounts in small banks — those without too much investigative structure — are paid a 1 to 2 per cent cut of the transaction in exchange for their service. The mules change their phone numbers associated with the receiving, thus giving the scammers control over the account and the ability to launder the money.

The scam impacted over 40,000 individuals, given the size of the Indian market, it seems inevitable that this attack is likely to remain an attractive target.

Singapore

As with other markets the Monetary Authority of Singapore (MAS) has sought to ensure that customers are reimbursed for unauthorised fraud. To encourage the correct customer behaviours, victims are required to demonstrate that they did not share their credentials or one-time passcodes.

MAS also require the customer to ensure that their device is patched and is using an up-to-date version of the operating system, and this includes the browser. Account holders are also required to utilise anti-virus software and must use strong passwords.

While there is currently no provision for victims of APP to be reimbursed, MAS has emphasised bank controls, resulting in one bank being required to add 330 million Singaporean dollars (USD $235M) to its capital base because its online controls were judged deficient.

Unique to Singapore is the Infocomm Media Development Authority of Singapore (IMDA) Proposed Shared Responsibility for Fraud Loss. While focused on phishing scams, it sets out to create a tripartite position making financial institutions, telecommunications operators, and consumers jointly responsible.

The approach in Singapore is the first time another sector (telecommunications) has been required to participate in a government-mandated process of the reimbursement of bank customers.

Phase one of the shared responsibility model focuses on phishing scams which target Singaporean customers and relate to a consumer clicking on a phishing link and entering credentials on a fake digital platform.

The question of which of the three parties the losses fall on has also been addressed by MAS, with financial institutions placed first in line, if it has fulfilled all its duties the telco is expected to meet the cost of reimbursement. If both the financial institutions and telco are considered to have fulfilled their duties the loss falls on the consumer.

Mitigating APP Fraud Risk in Real-time Payments

Management of fraud risk should involve a multifaceted strategy, some elements of which are likely to be outside the direct control of sending and receiving institutions.

As the UK demonstrates, there is scope for regulation to be brought to bear, addressing the detriment that APP has caused, primarily through RTP channels. This can be achieved through the implementation of a shared liability for senders and receivers, while encouraging and incentivizing increased detection and prevention across the industry.

Education

Providing staff and customers with materials which allow them to identify fraud risk is an essential starting point for any strategy which sets out to reduce the risk of fraud.

Much of the fraud that now leverages RTP is not new, with threat actors using a range of techniques — cyber-attacks, insiders and social engineering — to execute multiple forms of authorised and unauthorised fraud.

Techniques	Typologies	Unauthorised	Authorised
Cyberattacks	Account Takeover (inc. SIM Swop)	•	
Social Engineering	Identity Theft	•	
Insiders	Remote Banking Fraud	•	
Social Engineering	Impersonation Fraud		•
Social Engineering	Romance Fraud		•
Social Engineering	Advance Fee Fraud		•
Social Engineering	Purchase Fraud		•
Social Engineering	Business Email Compromise & CEO Fraud		•

Cyberattacks
institutions are best served by highlighting broader cybersecurity campaigns which encourage the use of suitable passwords and multifactor authentication across the totality of the customer's digital presence.

Insider Threats
Strong regulation and control/risk management models, such as the Three Lines of Defence (3LOD) that splits responsibility across three functions — front-line operations, risk management and compliance, and internal audits.

Social Engineering
The greatest risk in the RTP space is social engineering, with customers falling victim to APP frauds and scams. An example of an industry-wide campaign is "Take Five — To Stop Fraud" a UK-based campaign that encourages people to defeat social engineering attacks by taking time to think about what they're being asked to do.

Regulation

Regulators have a key role to play in the management of APP fraud risk in RTP channels, setting standards and ensuring that the payment system rules reflect the interests of consumers.

For instance, PSD2 mandated the use of Strong Customer Authentication (SCA) throughout the EU, leading to significant reductions in the losses associated with remote banking channels and cardholder-not-present transactions.

Regulators have also played a part in empowering customers to avoid errors and identify potential APP by mandating services which enable them to compare the expected recipient name with the name of the account holder.

Confirmation of Payee (CoP) in the UK and IBAN Name Check are examples of this service, in the case of CoP the user is provided with an indication that the payee's name they have provided is a match, partial match or not a match.

There is also evidence that regulators are increasingly seeking to encourage data sharing, with the Monetary Authority of Singapore providing a platform and an enabling regulatory framework. COSMIC, which stands for "Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases" will enable six major commercial banks in Singapore to share potential financial crime risks such as the misuse of trade finance.

Payment System Rules

The rules set by an RTP enterprise are integral to the management of fraud risk, supporting participating financial institutions to better manage risk.

Transactional Limits

The most obvious rule relates to the transactional limits within the payment system, typically these will focus on the volume and value of payments. For instance, Transfiya, a provider of RTP in Columbia limits users to 15 transfers a day with a cumulative maximum value of $280.

Transactional Holds

The opportunity for a participant in a payment system to hold a transaction for additional checks is another key opportunity for the management of fraud risk. While this would typically be focused on the outbound risk, due in part to the cost associated with unauthorised payments, it is increasingly becoming an essential tactic for receiving institutions.

Holding transactions either as they leave or are received by an institution is a key customer experience risk and requires close management. With both sending and receiving parties seeking to minimise the number of transactions they place on hold, there is a need to balance risk management with the potential of undermining customer confidence in the institution and RTP system.

One way to manage the scope for unnecessary transactional holds (false positives) is through the provision of additional context. Pay.UK which operates the UK's retail payments operations (including Faster Payments) undertook a proof of concept which provided sending and receiving institutions with an extended range of data points.

Those additional data points enabled the participants to identify high-risk payments more accurately, improving detection while also reducing the scope for unnecessary transactional holds.

Reporting

Requiring sending and receiving institutions in an RTP system to report fraud enables the operator to potentially offer the detection and mitigation of fraud risk. This approach is akin to that of the card channels, which monitor fraud and chargeback rates to manage the risk associated with acquirers, processors, and merchants.

Machine learning is an effective way of managing fraud risk and while the operators of RTP channels have access to transactional data, in the absence of reporting they have a reduced opportunity to determine which transactions were fraudulent.

Increasingly the same outcome can be achieved without the involvement of the RTP operator, with participant institutions making use of consortia that utilise the infrastructure of third-party vendors.

Dispute Resolution

As with payment cards, the provision of dispute resolution mechanisms also provides opportunities for fraud prevention. The forthcoming UK framework for APP reimbursement sets an expectation that victims of APP will make a timely report to their financial institution, and where appropriate, law enforcement, helping ensure that the scope for moral hazard (first-party or friendly fraud) and unintended disincentives for victims and financial institutions are minimised.

As with reporting, ensuring that an RTP system has a clear understanding of which transactions resulted in a dispute also empowers the payment system or third parties to use machine learning proactively.

Technology

As observed in the Transactional Holds, Reporting and Dispute Resolution elements of this section, there is significant scope for technology to assist with the management of fraud risk.

Technology, such as machine learning, can be deployed at a payment system level and within the infrastructure of participating institutions. In the latter, the deployed solution may operate independently or can increasingly be part of a consortium model.

At a system level, Pay.UK has actively considered how they might provide fraud and risk scoring within their New Payments Architecture (NPA) which will replace Faster Payments. Identifying and alerting sending and receiving institutions to transactional risk is easier when you have a complete view of a given transaction and the associated parties.

This is a trend seen elsewhere with RTP operators in India, Nigeria and South Africa already leveraging centralised solutions to improve the management of fraud risk.

Data sharing should be seen as distinct but complementary to risk scoring, with RTP channels providing participants with the opportunity to report suspected money laundering and fraud. As observed in the Reporting and Dispute Resolution elements of this section, data sharing, within the parameters of regulatory direction or anonymization of data, is an essential input to the successful utilisation of machine learning.

Many of the institutions that participate in RTP channels have deployed fraud detection systems, with channels such as PIX in Brazil mandating the use of such technologies. While such solutions can derive a great deal of insight from transactional data there is an intrinsic asymmetry, with institutions lacking insight as to the nature of third-party senders and receivers. To address this, some channels provide centralised fraud prevention solutions and extended data on senders and receivers.

While such additional insight is undoubtedly valuable it does not address the broader asymmetry that exists beyond an RTP solution. Given the likelihood of displacement from RTP to other payment channels, such as international payment systems, it would seem likely that institutions will need to seek out services that provide consortium analytics which go beyond a single jurisdiction.

Consortia Infrastructure

Consortia technologies provide financial institutions the benefit of industry-wide and jurisdictional insights that uncover threats across the totality of the financial system, without compromising the integrity of Personal Identifiable Information (PII).

Understanding the risk on the receiving end of a transaction in real-time helps institutions streamline fraud prevention, reduce customer friction, and ensure timely access to funds to entities that are considered low risk. With infrastructure supporting a consortia network, institutions have the increased ability to uncover money mules, and benefit from early detection of new and emerging fraud schemes.

When incorporated with machine learning technologies that can identify fraud typologies across a collective network of financial institutions, the ability to detect and prevent fraud benefits the entire landscape of the global financial system. This culminates in ultimately reducing exposure to customers and banks in the UK who will, as of October 2024, now have the added liability of responding to the unrestrained growth of APP fraud.

Taking Action: An Industry Under Pressure

Financial institutions are being met with several external pressures that impact the operations and efficiency of their day-to-day business. As fraud grows, largely driven by socially engineered APP scams, compounded by increasingly sophisticated technology, customer expectations, and new regulations, financial institutions are left trying to foster a way forward that protects their financial environment and stakeholders.

Approaching this problem on their own, financial institutions have limited options that do not impact their customer base or increase the level of internal resources required. Fraud is an industry-wide occurrence that must be met with an equal response. While the greater machinations of the financial system have not evolved to co-operatively address fraud at this scale, a collaborative approach to financial crime has become a necessity.

As technology has enhanced day-to-day life globally, it has also allowed bad actors to thrive and employ scams that are quick, effective and ever evolving.

Through enhanced fraud detection and prevention methods that combine education, regulations, trans-action rules and infrastructure that supports consortia investigations, financial institutions can collectively work as an industry to reduce fraud and the impact it has locally, regionally, and on a global scale.

About Jonathan Frost

During his tenure at the City of London Police, Jonathan led the development of the UK National Fraud and Cybercrime Reporting system. He also contributed to the evidential workstream of the Contingent Reimbursement Scheme (CRM), the voluntary scheme for Authorised Push Payment (APP) fraud reimbursement.

Recently, he served as the Director of Technical Collaborations at Stop Scams UK, working with companies like Meta, Google, and BT to combat fraud at source. Jonathan also worked on several data science projects for the Foreign, Commonwealth and Development Office and Home Office during his time with Faculty.ai.

Jonathan currently sits on the board of the Stop Scams Alliance (US 501(c)(3) nonprofit). He acts as an indepen-dent consultant to several organisations, assisting them to reduce fraud and cybersecurity risks.

Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing. More than 2,500 financial institutions globally, representing more than $8T in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts. Leveraging our unique consortium data approach in targeted analytics with artificial intelligence and machine learning, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

To learn how Nasdaq Verafin can help your institution fight fraud and money laundering visit www.verafin.com or call 1-877-368-9986.

Nasdaq
Verafin