Fraud prevention and resolution in push payment systems

Comparative analysis

Prepared for the UK's Payment Systems Regulator (PSR)

May – September 2017

Lipis Advisors

Contents

Lipis Advisors

Executive summary

Executive summary

Key findings on centralized fraud prevention initiatives

- We looked at 12 markets' real-time push payment systems comparable to FPS and CHAPS in the UK, which were known to have a strong focus on consumer fraud protection. We consider what fraud processes are in place in these markets that could help prevent, mitigate, or respond to Authorised Push Payment (APP) scams.
- Most markets do not recognise APP scams as a separate type of fraud. Legislation and regulatory frameworks focus on fraud more generally (i.e., unauthorised fraud). Only two markets (Japan and South Korea) have implemented legislation targeted at APP scams, due to the prevalence of the issue.
- Most countries have fraud prevention processes in place, implemented either as a result of regulation or voluntarily for their value add. The role of Payment System Operators (PSOs) and Central Infrastructures (CIs) in these processes vary across countries - regulators and financial institutions often play significant roles in the overall fraud prevention strategy and its execution.
- Specific APP scam prevention processes were found in the withdrawal delay system in South Korea and a limit on ATM withdrawal in Japan. While the majority of fraud processes identified do not specifically and directly target APP scams, they can help indirectly. Examples of technical solutions in place include: addressing services and centralised fraud monitoring and scoring solutions. There are also examples of fraud information sharing processes.
- PSOs and CIs do not have a role in fraud resolution. In all markets, the financial liability of APP scams falls on the payer. In two markets - Japan and South Korea - legislation was implemented for APP scam resolution that allows for PSPs to freeze a scammers' accounts and redistribute funds to victims, and evidence suggests these are effective tools.
- Legislators and regulators are driven by the overarching policy goal of protecting the rights of consumers. In some cases, the policy aim is to increase confidence in electronic money, the coordination of payments fraud strategy, or improve consumer redress. There is also evidence of commercial drivers for clearing and settlement mechanisms (CSMs) to offer fraud prevention services to participants.
- None of the consumer fraud prevention processes were found in High-Value (wholesale) systems.

Scope and methodology

Project scope

APP fraud prevention in push payment systems

Background

In September 2016, the consumer group Which? submitted a super-complaint to the Payment Systems Regulator (PSR) concerning push payment fraud. Which? alleged consumers are not afforded an appropriate level of protection when tricked into transferring money to a fraudster via a 'push' payment as compared to other types of payment. In its response to the super-complaint, the PSR:

- Concluded that the UK's central infrastructure currently does not have any "rules, policies, or procedures in place related to consumer protection against fraud or scams."
- Pledged to investigate the potential for an expanded role of the payment system operators (PSOs) regarding authorized push payment (APP) fraud prevention for consumers. In support of this investigation the PSR would like to consider what the role of comparable payments systems in other markets are playing in combating APP fraud.

To that end, the PSR has requested a report that identifies comparable international push payment systems and reviews their respective fraud prevention and resolution practices.

Project scope

In support of its investigation into international APP fraud prevention practices, the PSR has engaged Lipis Advisors to provide research on prevention and resolution of authorized push payment fraud in 12 markets which were known to have a strong focus on consumer fraud protection:

- Australia
- Denmark
- SEPA (EU)
- India
- Japan
- Nigeria
- The Netherlands
- Singapore
- South Africa
- South Korea
- Sweden
- United States

The scope of the project is limited to:

- Payment system operators and central infrastructures of payment systems comparable to UK's:
  - Low-value real-time system, Faster Payments
  - High-value system, CHAPS
- Systems permitting consumer-initiated payments

Lipis Advisors

Project focus and methodology

APP fraud prevention in push payment systems

Focus topics

For this study we investigated the fraud prevention approach of payments systems used by consumers to initiate push payments. The research focuses on the following elements:

- Market-specific political, legislative, and regulatory context
- Payment fraud reporting and statistics
- Payment fraud prevention
- Payment fraud resolution
- Payment fraud prevention functionality and services
- Drivers of payment fraud prevention measures

Methodology

- In support of this research, we conducted extensive desk research and interviewed local experts familiar with push payment fraud prevention and resolution in each payment system in scope.
- We investigated which stakeholders have push payment fraud prevention responsibilities and what they are doing to prevent and resolve issues of fraud. Specifically, we examined rules and procedures as well as technology related to push payment fraud prevention capabilities.
- We paid particular attention to *authorized push payment* (APP) fraud – cases where the consumer is tricked into transferring money to a fraudster.

Definitions

- We defined the payments system as the interbank financial market infrastructure whose primary function is to facilitate the exchange of electronic payments for goods and services.
- Payment system stakeholders include the payment scheme rule makers and managers (comparable to FPSL and CHAPSCo), the technical infrastructure operators (comparable to VocaLink), and the regulators that together ensure the successful operation of the clearing and settlement of electronic payments.
- Payment System Operator is a company that operates one or more payment schemes – UK examples would be FPSL and CHAPS.
- Central Infrastructure (CI) is the hardware, software, connections, and operations that support the clearing and/or settlement of a payment or funds transfer request after it has been initiated. In some markets the CI is referred to as an Automated Clearing House (ACH)

We looked at PSOs and CIs across 12 markets

12 Payment System Operators

1 Commercial Fraud Service

2 Scheme Managers

2 Payments Associations

5 Technology Vendors

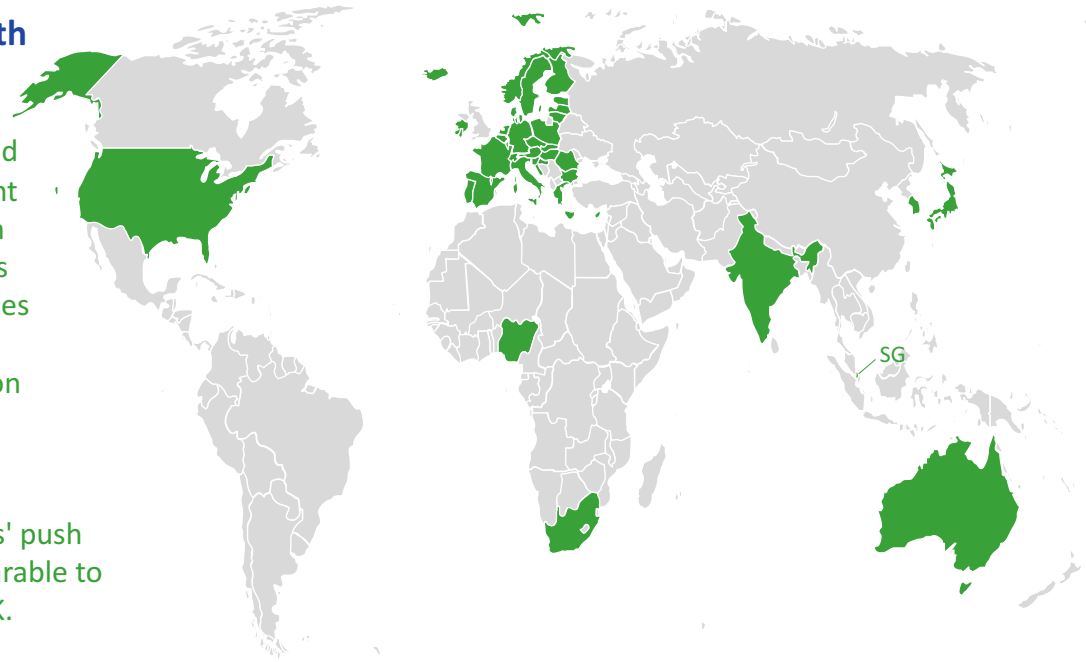
2 Government Bodies

Who we engaged with

We engaged with local stakeholders in payment systems around the world to understand the current state of fraud prevention in push payment systems and uncover best practices for authorized push payment fraud prevention and resolution.

What we focused on

We looked at 12 markets' push payment systems comparable to FPS and CHAPS in the UK.



What we found

- Most markets focus on unauthorized, not APP fraud.
- Only two markets (Japan and S. Korea) have legislation targeting APP scams.
- Most markets have fraud prevention processes in place. Only two (Japan & S. Korea) focus on APP scams.
- PSOs and CIs' role varies across markets – other stakeholders play significant roles as well.
- CI fraud prevention services are complementary and supplementary to the banks'.
- None of the consumer fraud prevention processes were found in High-Value (wholesale) systems.

Lipis Advisors

Comparing fraud prevention practices

Low value real-time system in scope

Market	System name	Rule maker	Infrastructure	Consumer initiation
Australia	New Payment Platform (NPP)	NPP Australia	SWIFT	Yes
Denmark	Straksclearing	Finans Danmark	NETS	Yes
India	Immediate Payment Service (IMPS)	National Payments Corporation of India	National Payments Corporation of India	Yes
Japan	ZENGIN	Japanese Bank's Payment Clearing Network	NTT Data	Yes
The Netherlands	iDEAL	De Nederlandsche Bank	Currence	Yes
Nigeria	NIBSS Instant Payment (NIP)	Nigerian Inter-Bank Settlement System	Nigerian Inter-Bank Settlement System	Yes
SEPA	Multiple	European Payments Council	Multiple	Yes
Singapore	Fast and Secure Transfers (FAST)	Singapore Clearing House Association	Banking Computer Services	Yes
South Africa	Real Time Clearing (RTC)	Payments Association of South Africa	BankservAfrica	Yes
South Korea	Electronic Banking System / HOFINET	Korean Financial Telecommunications & Clearing Institute	Korean Financial Telecommunications & Clearing Institute	Yes
Sweden	Betalingar i Realtid (BiR)	Bankgirot	Bankgirot	Yes
United States	The Clearing House's Real-time Payments System (RTP)	The Clearing House	The Clearing House	Yes

Comparing fraud prevention practices

High value payment systems in scope

Market	System name	Rule maker	Infrastructure	Consumer initiation
Australia	Reserve Bank Information and Transfers System (RITS)	Reserve Bank of Australia	Reserve Bank of Australia	Yes
Denmark	Kronos	Danmarks Nationalbank	Danmarks Nationalbank	Yes
India	RTGS	Reserve Bank of India	Reserve Bank of India	Yes
Japan	BOJ-NET	Central Bank of Japan	NTT Data	No
SEPA (EU)	TARGET2	European Central Bank	European Central Bank	No
Nigeria	Central Bank of Nigeria Interbank Fund Transfer System (CIFTS)	Central Bank of Nigeria	Central Bank of Nigeria	Yes
Singapore	MAS Electronic Payment System (MEPS+)	Monetary Authority of Singapore (MAS)	Monetary Authority of Singapore (MAS)	Yes
South Africa	South African Multiple Option Settlement (SAMOS)	South African Reserve Bank	South African Reserve Bank	Yes
South Korea	Bank of Korea Financial Wire Network (BOK -Wire+)	Bank of Korea	Bank of Korea	No
Sweden	RIX	Sveriges Riksbank	Sveriges Riksbank	No
United States	Fedwire	Federal Reserve	Federal Reserve	Yes
	CHIPS	The Clearing House	The Clearing House	Yes

Lipis Advisors

APP fraud prevention in payment systems

High value/RTGS system vs. Low value real-time systems

All of the markets in scope have multiple clearing and settlement mechanisms for electronic payments. In most markets, distinctions are made between low value real-time payment systems (retail payment systems) whose primarily function is to transfer funds between consumers and sometimes businesses, and high-value payment systems (wholesale payment systems) that facilitate the exchange of payments for settling obligations between financial institutions. The interaction of consumers with the high-value system varies by market. In some systems, consumers do not have access. In others, consumers can initiate a payment over the high-value system in certain circumstances. However, access to high-value systems is almost exclusively limited to payment initiation in person at the bank branch.

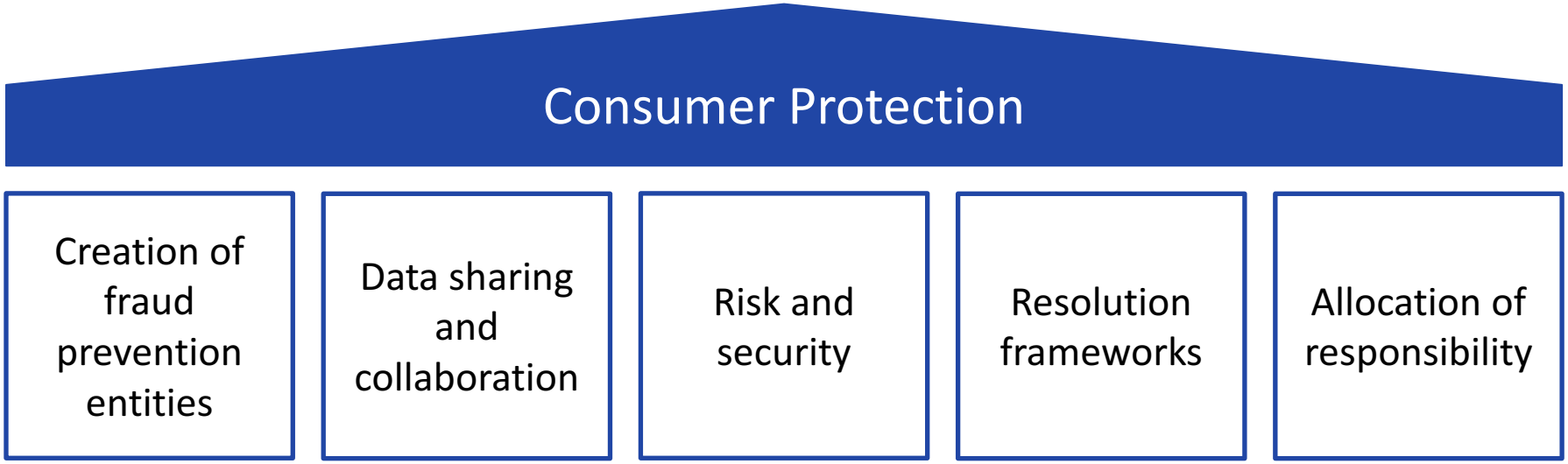
Due to the wholesale focus of high-value systems there is limited access for consumers. In general, these payments are settled in gross and real-time (RTGS) or in some cases via high-speed netting. Payments are final and irrevocable, which is important to limit risk for financial institutions managing liquidity across multiple counterparties and settlement systems. For some types of payments, consumers do use the high-value system. Consumer may use the high-value system if their payment exceeds the retail payment system's value limit, or if other payment options are too slow, or for certain use cases where finality of the payment is important. Examples include home purchases, or other high-value purchases where a counterparty needs to transfer ownership on receipt of payment. Financial institutions tend to protect their consumers by limiting access and providing disclaimers to customers who need to initiate a high-value payment. However, in our study, no high-value system contained rules or procedures to protect consumers from fraud, including authorized push payment fraud. Therefore, we focus on retail payment systems in the remainder of the report.

Political, legislative, and regulatory context

Payment fraud prevention and resolution

One overarching theme; five broad legal and regulatory areas

We investigated each markets' legal and regulatory frameworks to understand how the ecosystem approached fraud prevention, and to better understand the context for the fraud measures that have been implemented. We discovered that the legal and regulatory frameworks in most markets are constructed around payment fraud more generally. Only two markets - Japan and South Korea - have frameworks specific to APP fraud. The study revealed one overarching theme and five legal and regulatory areas, through which markets are working to establish the legal and regulatory framework necessary to effectively combat fraud in consumer push payments. Collectively, these five legal and regulatory areas establish a framework conducive to coordination between stakeholders, the sharing of information, mandated levels of security, rules around freezing and transferring fraudulently obtained assets, and defining liability for fraud prevention.



Lipis Advisors

Payments fraud prevention and resolution

Consumer protection is the overarching driver in fraud prevention

Legislators and regulators are motivated by a combination of factors to strengthen payments fraud frameworks. Consumer protection is a cross-cutting factor behind nearly every measure to reduce consumer payments fraud. However, other factors, such as the policy goal to decrease cash usage and instill confidence in electronic payments, drive the need to improve fraud measures. Special circumstances, such as the prominence of payments fraud (as in Nigeria), or the vulnerability of certain segments of society (such as the aging population in both Japan and South Korea), can also play a role. In some cases regulators have responded by specifically creating financial services-related consumer protection frameworks to ensure that consumers are adequately protected and treated fairly, including the prevention of payments fraud. While not the sole focus, in some cases this extends to protecting consumers from authorized push payment fraud as well.

Case study: The Consumer Protection Framework (Nigeria)

The Central Bank of Nigeria (CBN) has interpreted its statutory responsibility to promote confidence in the financial system to include the implementation of consumer protection measures. Furthermore, an overarching policy to promote electronic payments and reduce cash usage, known as the Cashless Policy, along with high rates of payments fraud has driven the CBN to enact a series of fraud measures. Initially, these measures were mainly in the form of customer complaint management. While this arrangement helped to protect the rights of consumers of financial products and services, it was limited in scope and did not address other key issues. A main concern being the poor level of financial literacy in the use of banking products and services in Nigeria. While a limited consumer protection framework did exist in the banking industry, it was deemed inadequate and in 2016 Nigeria created a new Consumer Protection Framework. The framework laid out a strategy to create comprehensive consumer protections within the payments system, including enabling new regulation where necessary.

Drivers of fraud prevention measures

Consumer protection is the overarching driver of fraud prevention

Consumer protection is the overarching driver of fraud prevention measures. However, several additional and specific policy drivers were discovered. In addition to protecting the rights of consumers, legislators and regulators have given special focus to protecting specific demographics of societies. In Japan and South Korea it was found that elderly persons are more susceptible to certain types of fraud due to a lack of understanding of technology, and can be more easily tricked into authorizing push payments. Other policy drivers include increasing confidence in the electronic money and reducing cash usage. Drivers of specific regulation on fraud are also practical measures to create the legal framework necessary to fight fraudsters. These include the coordination of payments fraud strategy, for example, creating a forum for discussion and strategy input, clarifying issues of liability, enabling the sharing of fraud related personal data that would otherwise violate data protection rules, and the sequestering and distributing fraudulently obtained funds.

In addition, commercially operated clearing and settlement mechanisms (CSMs) are also driven to offer fraud services to support their clients - who may be held liable for payments fraud - and to increase their own revenue streams by selling additional value-added services. One CSM we interviewed stated that fraud services were the easiest value-added service to sell to banks, as it more than pays for itself through the reduction in fraud.

Consumer fraud prevention and resolution

Five legal and regulatory areas

Creation of fraud prevention entities	Law makers and regulators use their authority to create and assemble public bodies and other types of governmental and quasi-governmental organizations, tasked with fraud prevention and resolution. In some cases, these organizations are given specific legal powers (Nigeria), in others they act as a forum for policy making and industry coordination (The Netherlands). Coordination is a necessity in the process of crafting an industry strategy across multiple stakeholders, who are often competing, and in establishing the foundation for cooperation on non-competitive areas of security.
Data sharing and collaboration	The ability for stakeholders to share fraud data varies by jurisdiction. Some stakeholders expressed frustration at being constrained by rules designed to protect consumer data, that in effect prevented information sharing of fraudulent activity. In some markets, law makers have mandated rules around protecting and sharing of fraud related information to realize the benefits of shared data to create a wider view, sharing knowledge of known fraudsters and their methods, and prevent fraudsters that are black-listed at one bank from moving to target victims at another.
Risk and security	Law makers and regulators have mandated security and risk management standards for the financial services industry. These include increased or minimum standards for data protection, Know Your Customer (KYC) practices, risk reduction, and fraud prevention measures. In rare cases, such as in Nigeria, this includes the use of specific fraud technology. It is also worth noting that in some cases industry has voluntarily adopted standards such as Australia's ePayment Code of Conduct which, although voluntary, sets minimum standards that have become de facto industry regulation.
Resolution frameworks	We have found cases where markets have codified the rules and procedures around vetting and freezing assets suspected of fraud, and in some cases such as Japan and South Korea, stipulated schemes for victim compensation. This is important for not only stopping further fraudulent activity, but also establishing the rules for resolving fraudulent cases and compensating victims according to a transparent scheme.
Allocation of responsibility	All markets have some legislation that places financial liability on financial institutions if they are at fault for unauthorised transactions. None of the markets in scope have legislation that holds the financial institution or PSO financially liable for authorised transactions. However, in some markets, notably South Korea and Japan, legislation requires banks to follow specific processes to help customers investigate fraud claims and recover funds lost due to APP scams.

Lipis Advisors

Legal and regulatory areas covered

Overview of where specific legislation has been enacted

Market	Creation of Fraud entities	Data sharing and collaboration	Risk and security	App fraud resolution	Allocation of responsibility
Australia	■	■	■		■
Denmark		■			
India		■	■		■
Japan		■	■	■	■
The Netherlands	■	■	■		
Nigeria	■	■	■		
SEPA		■	■		
Singapore			■		
South Africa		■			■
South Korea	■	■	■	■	■
United States	■	■	■		

Legend

■ Legislation/regulation in place

■ De facto regulation / governmental initiative

Lipis Advisors

Regulators convene fraud prevention entities

Case studies

Nigerian Electronic Fraud Forum (Nigeria)

The Central Bank of Nigeria (CNB), in a quasi-regulatory role, created the Nigerian Electronic Fraud Forum (NeFF), which comprises the CNB and the Nigerian banks, to enable information sharing and knowledge exchange among key industry stakeholders in order to find a proactive approach to limit electronic fraud. The NeFF is working to protect the integrity of the banking industry from criminal threat, and at the same time boost public confidence in the use of electronic payments. Decisions made in the NeFF are mandated by CBN and are issued to industry participants in the form of a circular.

Australian Financial Crimes Exchange (Australia)

The Australian Financial Crimes Exchange (AFCX) was established in 2015 through a partnership between Australia's four major banks and the Australian Government to create mechanisms to share information and strengthen the financial and banking industry response to fraud and financial crimes. Although the government served as the impetus for the creation of the AFCX, it does not fall under the purview of any government agency. Instead, it is organized as a not for profit entity and will operate on a cost recovery basis offering members multiple fraud prevention and resolution services through a subscription model.

National Forum for Payment Systems (NL)

The Netherlands have developed a solid framework for information sharing and collaboration across multiple stakeholders. The main initiative is the National Forum of Payment Systems, which takes place twice a year to discuss various issues surrounding Dutch payment systems. The stakeholders have agreed on several key points such as that there is no competition on security matters and cooperation is encouraged. Furthermore, they agree that transparency is key in the fight against payment fraud, hence there is a culture in the banking community to share information between financial institutions and also with the public.

Lipis Advisors

Regulators mandate security standards

Case studies

Mandating implementing of a fraud monitoring system (Nigeria)

In 2015, the Central Bank of Nigeria issued a circular mandating NIBSS (PSO & CI) to implement a centralized fraud monitoring system, and for banks to implement across all electronic channels an enterprise fraud monitoring system, for behavioral monitoring, patterns, and hold/block controls on transaction suspected to be fraudulent. Banks are permitted to build this solution themselves, or outsource this function. NIBSS offers an enterprise anti-fraud solution for this purpose, in addition to the central monitoring service.

Establishing minimum security standards for FIs (India)

In mid-2016, the Reserve Bank of India issued a circular putting the onus on banks to put in place robust and dynamic fraud detection and prevention mechanisms, to mitigate unauthorized payments and to make customers feel safe about carrying out electronic banking transactions. Previously, in 2010, the RBI issued recommendations for banks to address information security, electronic banking, technology risk management, and cyber crime. The recommendations included the implementation of risk-based transaction-monitoring which may use dynamic scoring models and related processes to detect abnormal transactions.

Lipis Advisors

Data protection and sharing are vital

Case studies

Nigeria

Section 33 of the Central Bank of Nigeria Act empowers the CBN to collect and share "information relating to or touching or concerning matters affecting the economy of Nigeria", and to "issue guidelines to any person and any institution under its supervision". The CBN interprets this clause as the basis for its mandate for the sharing of fraud data within the industry. The CBN has, for example, mandated that NIBSS collect bank records of fraudulent transactions, providing monthly reports to the CBN. Furthermore, NIBSS provides several fraud data services to its participants that, from a data security perspective, operate under CBN's remit.

SEPA

Article 94 of the new Payment Service Directive (PSD2) states that "Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud". However, sharing of personal data in SEPA is governed by the EU's Data Protection Directive (Directive 95/46/EC) as well as local legislation. The current data protection legislation is an obstacle to cross-border data sharing and cooperation because there is no uniform definition of personal data. The General Data Protection Regulation (GDPR), to be implemented in 2018, intends to strengthen and unify data protection for all individuals within the EU. It might provide some clarification around the interpretation of private data and contribute to the ease of data sharing.

Australia

Due to growing concerns of cyber and financial crime, the Department of Treasury and the Attorney-General's Department commissioned a comparative study to evaluate Australia against other countries in relation to information and intelligence sharing for the purpose of collaboration. The study was conducted around 2011/2012 and looked at the regulatory and legislative regimes in different markets, and out of this identified a gap in Australia's capabilities. Since the completion of the study around 2014, there have been legislative changes to the Privacy Act. These changes have enabled information sharing to occur, provided a party believes that illegal activity or serious misconduct is being or may be engaged in.

Lipis Advisors

APP fraud resolution schemes

Case studies

Japan

In the mid-2000s there was growing public awareness of APP scams and the financial damage it was causing, especially among Japan's elderly population. In response to this, the 'Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes' was enacted in 2008. The law set out a processes for damage recovery in the case of APP fraud. The objective of the scheme is to compensate APP fraud victims for their losses by fairly distributing the remaining balance on the fraudster's account. It also lays the legal foundation and creates the administrative process for banks to, first, freeze accounts suspected of fraudulent activity and, second, to redistribute assets obtained illegally.

South Korea

The 'Special Act on the Prevention of Loss Caused by Telecommunications-based Financial Fraud and Refund for Loss' was enacted in 2011 to relieve financial consumers' losses from increasing instances of voice phishing fraud. The law enables victims to recover their damages up to the balance remaining in the fraudster's account, without proceeding with a formal lawsuit. As in Japan, the law lays the legal foundation and creates the administrative process for banks to freeze accounts suspected of fraudulent activity and redistribute assets obtained illegally. In 2011, the Financial Supervisory Service (FSS), South Korea's integrated financial regulator, established a new team, whose responsibility is damage recovery, educating the public on phishing fraud prevention, and promoting the damage refund system.

Lipis Advisors

Sharing fraud responsibility between stakeholders

Case studies

South Korea

Financial institutions share some responsibility with the consumer for certain types of payment fraud. However, this does not extend to financial liability for APP fraud. In 2007 the Electronic Funds Transfer Act (EFTA) was enacted and shifted responsibility to financial institutions, making them responsible for redress when consumers suffer losses as a result of unauthorized transactions, forgery, and unfulfilled orders. In brief, this law states that financial institutions have to indemnify their customers for the losses when they fall victim of fraud, unless they can prove that the customer acted with intention or gross negligence. This law does not specifically apply to APP fraud.

The 'Special Act on the Prevention of Loss Caused by Telecommunications-based Financial Fraud and Refund for Loss' was enacted in 2011, strengthening consumer protection in response to increased cases of APP fraud. In 2014, the law was amended to enhance the responsibilities of financial institutions and regulatory authorities for the prevention of phishing fraud (a type of APP fraud). The current law mandates South Korea's top financial regulator, the Financial Services Commission (FSC), and financial services companies to take necessary measures to prevent APP fraud. These measures include cooperating with the police and banks on public awareness campaigns in print, on TV, and online. The law also enables victims to recover their damages up to the balance remaining in the fraudster's account without proceeding with a formal lawsuit, thus removing the financial barrier for victims to pursue compensation.

Further legislation related to APP fraud

Increased security standards in Japan

Japan

The 'Law Concerning the Identification of Customers by Financial Institutions and the Prevention of the Unlawful Use of Bank Accounts' (2004) established measures concerning the identification of customers and the preservation of transaction records by financial institutions. This has tightened the control on client onboarding and KYC procedures at financial institutions. The 'Act on Prevention of Transfer of Criminal Proceeds' (2007) superseded the law and strengthens measures to prevent criminals from using bank accounts for criminal activities, and mitigate the transfer of criminal proceeds.

Crimes targeted at older people has increased in line with the rapid aging of Japan's population. Many older people have fallen victim to a particular ATM transfer scam – the case where a person is deceived into using an ATM to transfer money to a fraudster. The government has taken legislative measures to tackle this challenge. In accordance with the enactment of the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds people are unable to make ATM-initiated credit transfers that exceed JPY100,000 (<GBP700). This has contributed to a reduction of APP fraud, as ATMs are frequently used in APP scams targeted at elderly people.

Lipis Advisors

Payment fraud reporting and statistics

Lipis Advisors

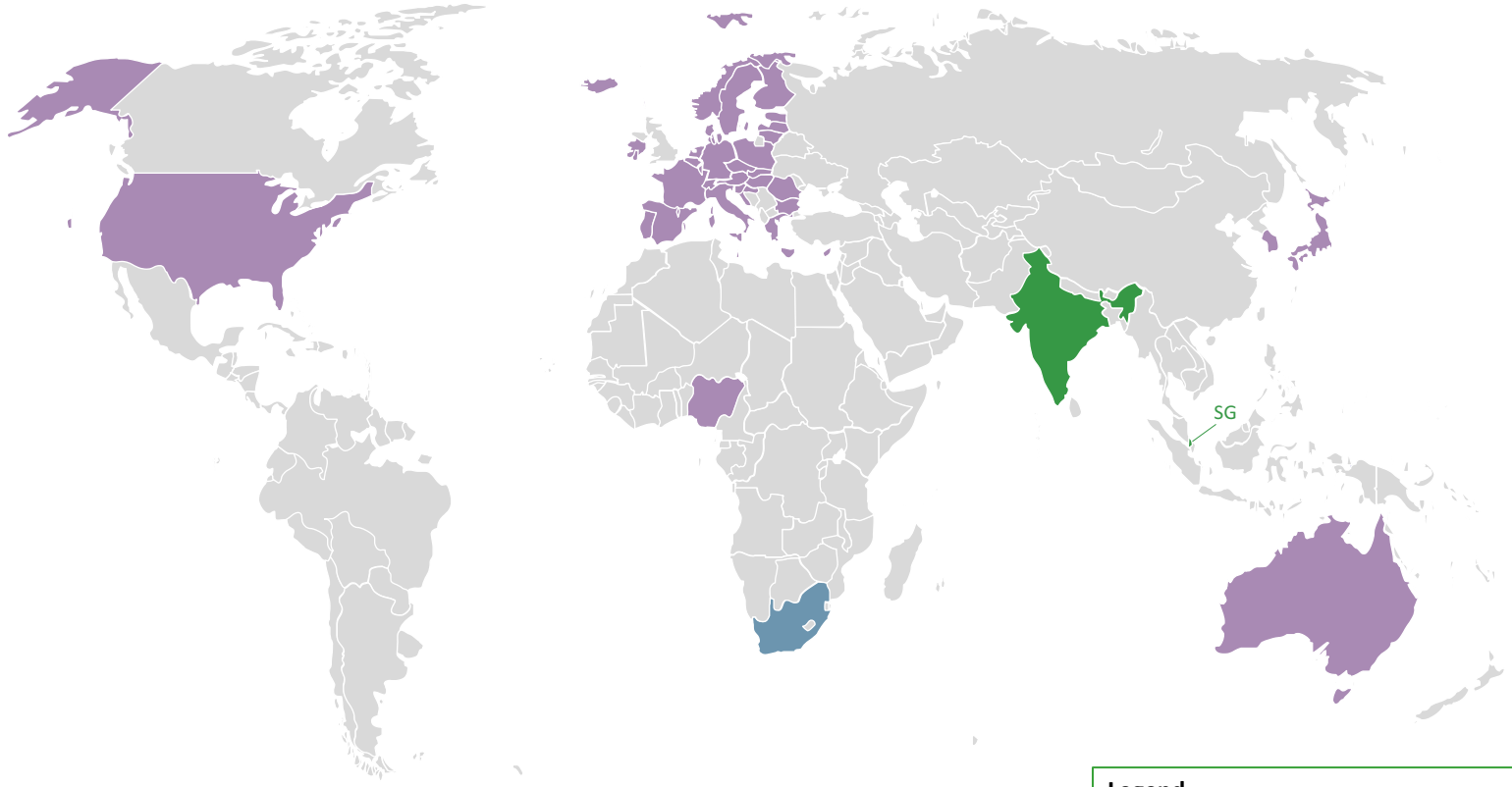
Payment fraud reporting and statistics

Most markets collect and publish payments fraud data

The majority of markets in scope mandate the collection of fraud data, with more than half making some fraud data available to the public. Only Japan and South Korea publish APP fraud data. Out of the 10 markets where we received feedback, 8 have some form of centralized fraud collection. In most markets, data on the rates of fraud at individual banks is considered to be competitive information. In other cases, notably in the Netherlands and in Nigeria, the payments community has explicitly decided that combating fraud is a non-competitive area and that sharing fraud data is important in instilling confidence in the payments system.

Standardized procedures for reporting fraud data have been implemented in several markets. This includes, for example, coordinating the various stakeholders and their respective roles, and creating standardized submission formats. The result has been an increase in both the quantity and quality of fraud data. In the following case studies we explore where fraud data is collected and shared, and, when possible, what the discernable trends in payments fraud are.

Payment fraud data collection and publication



Legend

- Market that does not collect fraud data
- Market that collects but does not published fraud data
- Market that collects and publishes fraud data

Note: Publication of fraud data varies across SEPA markets.

Lipis Advisors

Payment fraud data collection and publication

Overview

Market	Fraud data collected	APP fraud data available	Centralized collection	Data publically available	Collector(s)
Australia	Yes	No	No	Yes	Industry body, Government agency
Denmark	Yes	No	Yes	Yes	Industry body
India	No	No	No	No	n/a
Japan	Yes	Yes	Yes	Yes	Government agency
The Netherlands	Yes	No	Yes	Yes	Industry bodies
Nigeria	Yes	No	Yes	Yes	Industry body/PSO
SEPA	Yes	Varies	Yes	Varies	Government agencies
Singapore	Yes	Yes	No	Yes	Industry body
South Africa	Yes	No	Yes	No	Government agency, Industry body
South Korea	Yes	No	Yes	Yes	Government agency
Sweden	Yes	No	Yes	Yes	Government agency
United States	Yes	No	No	Yes	Industry bodies, Government agencies

Legend

Yes | No | Varies

Lipis Advisors

Payment fraud data collection and publication

Case studies

Nigeria

NIBSS, the PSO & CI for retail payment systems in Nigeria, is mandated to collect records of fraudulent transactions from the banks and to provide monthly reports to the CBN. In addition, it publishes an annual report on the the prevalence of fraud in Nigeria.

The Nigerian banking industry reported 19,531 instances of fraud in 2016, an 82% increase in the volume of reported fraud cases compared to 2015, and more than 1200% compared to 2014. Despite the increase in fraud volume, there was a decrease of 2.5% in actual loss of value.

SEPA

There are significant geographical differences across Europe; some markets publish fraud data, others do not. The aspect of fraud reporting is currently under review due to new reporting requirements under Payment Services Directive (PSD2). In accordance with Article 96(1) of the PSD2, payment service providers must send their competent authorities statistical data on fraud affecting different types of payments. The competent authority must then provide this data in an aggregated format to the European Banking Authority (EBA) and the European Central Bank (ECB).

South Africa

Banks report fraudulent transaction to the South African Reserve Bank. However, banks tend to do no more than the required minimum when it comes to fraud reporting, and this poses challenges regarding granularity of data. All fraudulent transactions are lumped together regardless of the type of fraud, and consumer transactions are not differentiated from commercial transactions. In addition, the South African Banking Risk Information Centre (SABRIC), a financial crime information centre, collects fraud-related information from banks, and track statistics on card fraud.

Japan

The National Police Agency (NPA) collects and publishes data on APP fraud. In accordance with the Japanese APP fraud resolution scheme, codified in the 'Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes', fraud victims must report instances of fraud to the police. This provides data to track the entire process; from the initial report until resolution.

Payment industry stakeholders are finding it difficult to crack down on increasingly more sophisticated frauds, and the number of reported cases has been growing since 2009.

PSO and CI roles in fraud prevention and resolution

Lipis Advisors

Fraud prevention

The role and responsibilities of PSO and CI stakeholders

Most payment systems have centralized fraud solutions, and most of these were implemented to address unauthorized fraud, or generally to enhance security and stop fraudulent and malicious behavior. While not specifically targeting APP fraud, they help mitigate fraud indirectly by providing consumers with additional information to make informed decisions, and preventing fraudsters from repeat attacks. The extent to which the PSOs and CIs have fraud prevention responsibilities also varies widely by market. In general, the financial institutions that participate in the payments system have primary responsibility for protecting their customers against fraud. Our research shows that all tier-one and tier-two banks maintain sophisticated fraud platforms, while smaller banks invest less. From a systemic point of view, where centralized fraud prevention services exist, it is to extend and augment the banks systems, not to replace them.

One area of fraud prevention responsibility in particular has emerged for the central infrastructure (CI). The CI, by its nature of sitting between the counterparties in a transaction, has a broader view of transactions than any one participating party. Therefore, the CI is often tasked with collecting network wide information and providing this information back to the participants in the form of transaction monitoring service and scoring. What information is collected, how it is processed and how the information is shared back to the participants is unique to each market. Services are mandated in about half of the markets. In other markets, they are offered as value-added services. Factors determining the structure and content of fraud services that are delivered include the legal framework, and the commercial relationship between the participants and the CI. The majority of these services focus on unauthorized fraud. However, other services, such as addressing services, national bank IDs, proxy services, and verification of beneficiary, may help to reduce APP scams. One instance where a solution has been implemented to help address APP scams specifically is the withdrawal delay feature introduced by South Korean regulator FSS. The above-mentioned fraud prevention functionalities and services are discussed in more detail on page 34 onwards.

The role of PSO and CI stakeholders

Case studies

Market	Role and responsibility of PSO/CI
Nigeria	NIBSS has specific responsibility delegated from the CBN for the provision of multiple anti-fraud solutions and related services. The CBN takes an active role in fraud prevention and uses NIBSS as the technical provider for these solutions.
South Africa	BankservAfrica is the official clearing house for electronic payments, appointed by the Payments Association of South Africa (PASA). PASA derives its authority to manage the payment system from the South African Reserve Bank (SARB), under the National Payment System Act. BankservAfrica has been working closely with SARB and PASA to figure out ways in which they, on a national level, can assist the financial community in mitigating fraud. This includes the operation of a centralized transactional fraud mitigation system as well as an account verification service.
India	The Reserve Bank of India (RBI) has encouraged payment system operators (PSOs) to adopt best practices for protecting customer interest by putting in place robust fraud and risk monitoring systems. In response the national clearing house, NPCI, has designed and implemented a real-time transaction monitoring tool for fraud detection and prevention and offers this free of charge to its participants.
South Korea	South Korea has a holistic approach to payments fraud prevention and resolution, where the South Korea regulator, the Financial Supervisory Service (FSS), plays a large role in payments fraud prevention and resolution.

The role of PSO and CI stakeholders

Case studies

Market	Role and responsibility of PSO/CI
SEPA: STET	SEPA rules do not stipulate that CSMs must provide fraud services. However, most major CSMs offer, or will offer fraud services that cover SCT and SCTinst payments. STET is one of the largest ACHs in Europe; it operates the CORE platform, which clears low-value payments for consumers and corporate clients in its home market of France and neighboring Belgium. STET offers fraud scoring as a value-added service for all payment types it processes.
SEPA: EquensWorldline	Similar to STET, EquensWorldline clears low-value payments for consumers and corporate clients. It has extensive experience in centralized fraud services for its card switching products. A new solution, which is envisioned to screen both SCTs and SCTinst payments, is still under development, and is scheduled to go live at the end of 2017.
United States: TCH	Under US legislation, the legal and financial liability for authorised push payments fall on the consumer. Payment systems are not mandated to offer fraud services or resolution mechanisms for consumer disputes. However, TCH is instituting several features in its real-time system that should help to reduce misdirected and fraudulent payments including a centralized transaction monitoring and scoring service.
Australia	PSOs do not provide fraud services, nor are they mandated to. However, a separate entity, the Australian Financial Crimes Exchange (AFCX), was established in 2015 to facilitate the exchange of fraud data between the banks.

PSO and CI role in APP fraud resolution

Only two markets in scope have APP resolution schemes

In all countries, no central payment system stakeholder - PSO or CI - plays a role in APP fraud resolution. Japan and South Korea are the only two countries in scope that have established official schemes for the recovery of funds from APP fraud, performed by the banks. Statistics from both countries show that the schemes have increased the amount of money returned to victims. In South Africa, an effort has been made to shift responsibility for fraud prevention from solely that of the consumer, to a joint responsibility with the banks. However, the effectiveness of these policies is still undetermined and most fraud resolution is focused on unauthorized fraud. In Japan, the Netherlands, South Korea, and Singapore there are active campaigns to raise consumer awareness of APP scams.

Japan

The mid-2000s saw a growing public awareness and will to put in place a resolution scheme for fraud victims. In response to this, the 'Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes' was enacted in 2008. The law set out the processes for damage recovery in the case of fraud.

The APP fraud resolution scheme is codified in the 'Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes'. The Police Agency, Japanese Bank's Payment Clearing Network, the Deposit Insurance Corporation of Japan (DICJ), the Japanese Bankers Association (JBA), and banks have committed to follow the resolution scheme. The objective is to compensate APP fraud victims for their losses by fairly distributing the remaining balance on the fraudster's account.

South Korea

The 'Special Act on the Prevention of Loss Caused by Telecommunications-based Financial Fraud and Refund for Loss' was enacted in 2011 to relieve financial consumers' losses from increasing instances of phishing fraud.

In 2014, the law was amended to enhance the responsibilities of financial institutions and regulatory authorities for the prevention of phishing fraud. The law enables victims to recover their damages up to the balance remaining in the fraudster's account without proceeding with a formal lawsuit. In 2011, the FSS established a new team within the Micro-Finance Support Department, whose sole responsibility is damage recovery, educating the public on phishing fraud prevention, and promoting the damage refund system.

Fraud prevention functionality and services

Lipis Advisors

Fraud prevention functionality and services

Lessons learned from card processing

The majority of markets in scope have established fraud services or functionality at the central infrastructure level. The majority of these services are aimed at unauthorized payments. Others, such as directory services, focus on improving the customer experience, but have resulted in reducing misdirected or fraudulent payments. Fraud transaction monitoring, scoring and analytics services have been widely used in the cards processing industry for decades. Although the technologies used continue to evolve to take advantage of new developments in hardware and software, we can describe the technical capability as well developed and mature. We have also observed that PSOs with a history of processing card transactions are more likely to have existing fraud solution expertise and technology that can be applied to other payment streams, such as ACH products. We have seen, for example, that Euro CSMs that process cards are now moving to offer transaction monitoring services for their ACH services as well.

Fraud prevention functionality and services

Market overview

market	Anti-fraud solution	Information sharing service	Addressing service	Hold/freeze instructions	Request for payment	Withdrawal delay	Non-payment messaging
Australia		■	■				
India	■		■				
Japan	■		■				
The Netherlands	■	■					
Nigeria	■	■	■	■			
SEPA	■		■				■
Singapore		■	■				
South Africa	■		■				
South Korea						■	
Sweden			■				
United States	■		■		■		

Legend

■ Live or confirmed ■ Under consideration

Lipis Advisors

Centralized anti-fraud solution

Introduction

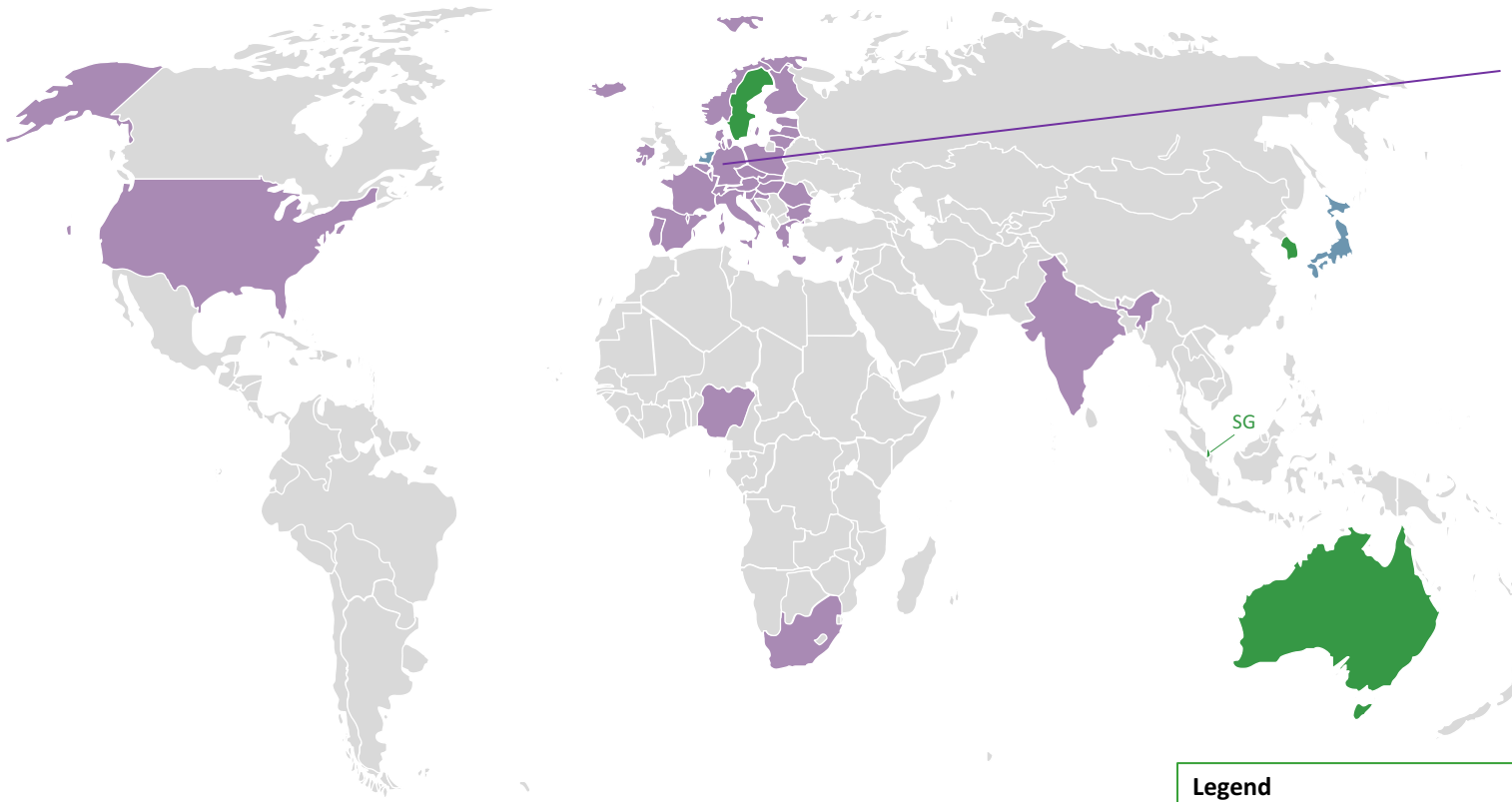
Half of the markets in scope have a centralized anti-fraud solution such as transaction monitoring and scoring, and two others are considering implementing a fraud solution in the near future. Locating the anti-fraud solution at the central infrastructure (CI) level provides several key benefits to the participants. The CI, by its nature of sitting between the counterparties in a transaction, has a broader view of transactions than any one participating party. Therefore, the CI is able to leverage network-wide information to offer anti-fraud services such as transaction monitoring, maintenance of community watch lists, and secure communication channels. Central transaction monitoring services can apply analytics to recognize patterns not only from the sending bank account, but also to the beneficiary account to identify mule accounts and alert the participating PSPs.

A centralized solution is complementary and supplementary to the banks own fraud prevention systems, thereby augmenting and extending the participants' capabilities. Of the markets that have a solution, about half have been mandated by the regulator. The other half has been implemented voluntarily or for commercial reasons. In short, centralized anti-fraud services provide a floor, or minimum level of security, while extending the banks' bilateral view of transactions to take advantage of a network-wide view.

Lipis Advisors

Centralized anti-fraud solution

Market overview



SEPA PSO/CI stakeholders in scope of this study that offer a centralized anti-fraud solution include:

- EquensWorldline
- STET

Legend

- Market without centralized solution
- Market planning/considering centralized solution
- Market with centralized solution

Lipis Advisors

Centralized anti-fraud solution

Functionality overview

Market	PSO / Service	Transaction monitoring	Transaction scoring
India	NPCI	Mandatory	Mandatory
Nigeria	NIBSS	Mandatory	Mandatory
SEPA	STET	Voluntary / VAS	Voluntary / VAS
SEPA	EquensWorldline	Voluntary / VAS	Voluntary / VAS
South Africa	BankservAfrica	Mandatory	
United States	TCH RTP	Voluntary / VAS	Voluntary / VAS

Legend

Voluntary / VAS

Mandatory

Lipis Advisors

Centralized anti-fraud solutions

Case studies

Nigeria

The NIBSS anti-fraud solution monitors interbank transactions in real-time, 24/7, reporting on fraud as it occurs, and logging the associated Bank Verification Number (BVN), thus mitigating future instances of fraud. In a circular issued in 2015, the CBN mandated that all interbank transactions must pass through the central anti-fraud solution at NIBSS.

The same CBN circular empowers NIBSS to issue transaction "hold" instructions and advise the participating bank to freeze accounts identified in fraudulent transactions. CBN has also mandated banks to implement across all electronic channels an enterprise fraud monitoring system, for behavioral monitoring, patterns, and hold/block controls on transactions suspected to be fraudulent. Banks are permitted to build this solution themselves, or outsource this function. NIBSS offers an enterprise anti-fraud solution for this purpose.

South Africa

BankservAfrica has developed a central transactional fraud monitoring solution, which is scheduled to launch in 2017. As the processor of interbank payments, BankservAfrica are able to see both the initiating and beneficiary side of transactions. The solution will deploy interbank fraud detection on Electronic Funds Transfer (EFT) credit payments (ACH payments) and Real Time Clearing (RTC) payments. This holistic view of payment transactions will be leveraged in order to augment banks' own fraud systems.

The system creates profiles by combining data from various South African payment streams, including RTC payments, EFT payments, and debit orders. It uses a rule-based mechanism to detect potentially fraudulent transactions, which then alerts both the paying and the beneficiary bank, allowing the parties to investigate further.

Centralized anti-fraud solutions

Case studies

India

The National Payment Corporation of India (NPCI) has designed and implemented a Real-Time Fraud Risk Monitoring and Management solution (FRM), a rule-based real-time transaction monitoring tool for fraud detection and prevention.

The solution is offered as a value-added service, free of charge, to NPCI's member banks. It monitors payments that flow through any NPCI channel, including – among others – the real-time payment system, IMPS, and the Unified Payments Interface (UPI), a mobile payments platform built on top of the IMPS infrastructure. System participants monitor alerts through web-based access provided by NPCI.

United States

TCH are building a component that will identify potentially fraudulent transactions as well as mule accounts on the receiving side by leveraging the aggregate view of transactions flowing through their system. It will detect patterns in network-level activity that could indicate fraud or money mule activity. Once the system detects transactions that look like other fraudulent transactions in the system, it will notify affected system participants.

TCH will be using a third party system to rate payments and play back to the sending and receiving banks when it thinks a payment looks suspicious. However, it is up to the sending and recipient bank to analyze the payment and decide whether to continue to credit it to the recipient or not. Repeated fraudulent payments will be flagged and the associated accounts frozen preventing further damage to customers.

All financial transactions and Request for Payment (RfP) messages will be scored. This will help augment the banks' decision engines with aggregate level scoring, making the banks' systems more intelligent.

Centralized anti-fraud solutions

Case studies

STET (SEPA)

STET offers fraud scoring as a value-added service for SEPA Credit Transfers (SCTs), and SEPA Direct Debits (SDDs), and card payments. It uses the IRIS Analytics solution, which uses statistical models and predefined expert rules, to score transaction fraud risk in real time. The relevance of the score is optimally generated through supervised self-learning algorithms based on large volumes of eligible transactions. STET will also implement a real-time payments fraud scoring service based on its current fraud scoring system, which, according to its website, has delivered cost saving to PSPs of more than EUR 50 million per year through fraud detection.

EquensWorldline (SEPA)

EquensWorldline has long-standing expertise in card processing, and have been detecting card fraud for more than a decade. It intends to leverage its card fraud detection expertise to offer a solution for non-card payments. The solution, which is envisioned to screen both SEPA Credit Transfer (SCT) and SEPA Instant Credit Transfer (SCT Inst) payments, is still under development and is scheduled to go live at the end of 2017. It plans to deliver it to their clients as a BPO service. Our contact explicitly said that EquensWorldline could not reveal more information this close to launching the solution.

Addressing services

Introduction

Central addressing services provide access to a directory where FIs can centrally register beneficiary information. Services can then be made available to FIs and end-users. For example, FIs can offer their account holders additional information to ensure that they can make an informed decision before initiating a transaction. It is important to note that, while not explicitly created to combat fraud, addressing services can offer powerful tools for combating APP fraud. The result is that most addressing services are not mandatory, and are instead being offered as value-added services.

Given the nature of APP fraud, security measures to prevent unauthorized access are insufficient to protect victims. Instead, security can focus on ensuring that the account holder has the necessary information to make an informed decision. One common APP scam involves falsifying beneficiary information, for example, claiming to be in an official capacity (such as the police) to trick the victim into making a payment. Addressing services, such as beneficiary verification, can alert the sender if the beneficiary information differs from the account holder, thus reducing fraud by increasing the difficultly for fraudsters to deceive potential fraud victims.

National and standardized account IDs can help to underpin a transparent and efficient verification system. National bank IDs can be used to associate accounts across multiple institutions. This is especially helpful in building a database of information on accounts associated with fraud. Such services can help FIs to effectively assess risk, and to reduce future cases of APP fraud as well as prevent criminals from repeat offences.

Addressing services

market	National/ standardized ID	Account masking/proxy	Beneficiary lookup	Verification of beneficiary
Australia		Voluntary / VAS		Voluntary / VAS
India	Mandatory	Voluntary / VAS		Voluntary / VAS
Japan				Voluntary / VAS
Nigeria	Mandatory	Voluntary / VAS		Voluntary / VAS
SEPA		Voluntary / VAS		Voluntary / VAS
Singapore		Voluntary / VAS		
South Africa			Voluntary / VAS	Voluntary / VAS
Sweden		Voluntary / VAS		
United States			Voluntary / VAS	Voluntary / VAS

Legend

Voluntary / VAS

Mandatory

Lipis Advisors

Addressing services

Case studies

National ID (Nigeria)

The Bank Verification Number (BVN) is a unique ID number that links a customer's account(s) at any Nigerian bank(s) using biometric details, which gives the customers a unique identifier that can be verified across the Nigerian banking industry. The goal of the BVN is to increase security and reduce the risk of fraud for financial transactions. Customers are now required to enroll for a BVN at the bank where the person has an account or intends to open an account. Once the BVN has been generated, it can be linked to accounts at multiple banks. A BVN remains with a person for life.

Proxy database (Singapore)

The Central Addressing Scheme (CAS) is an account mapping system for the FAST payment system. In the case of the customer, the account number will be linked to a mobile number, and assigned a Unique Entity Number (UEN). In the case of businesses, they register a UEN with the Accounting and Corporate Regulatory Authority (ACRS). The CAS is primarily aimed at improving the user experience, but it is also expected to reduce fraud by increasing the difficultly for fraudsters to deceive potential fraud victims.

Beneficiary verification (South Africa)

The Account Verification Service (AVS) enables banks' customers to verify account information across participating banks before making payments. The AVS verifies – among others - the bank account number, account holder's name, and company registration number, ensuring that the funds reach the payer's intended beneficiary. This reduces the risk of fraud and rejected transactions due to misleading or incorrect bank account information. AVS is delivered by BankservAfrica as a valued-added service to both banks and merchants.

Beneficiary verification (Japan)

The infrastructure provider NTT Data offers banks the functionality to verify the provided account information, including the bank account number or bank identification number. Senders are able to confirm if the payment is properly addressed. For example, it is common for online banking systems to verify the beneficiary account information at the time of payment initiation by referring to the database maintained at ZENGIN. The system then notifies the user if the account number or the bank identification number exists or not.

Lipis Advisors

Addressing services

Case studies

Proxy service (SEPA / Europe)

STET plans to implement a proxy database that allows PSPs to consult the database to ascertain the BIC and IBAN of the beneficiary from a given mobile number or email address. This service will allow participating PSPs to offer a verification of beneficiary service to their customers, reducing misdirected payments and fraud.

As a side note, the European Payments Council (EPC) is in the process of creating the framework for a Pan-European proxy service called the Standardised Proxy Lookup (SPL) service, which will use mobile numbers as proxy for IBAN.

Beneficiary lookup (USA)

TCH''s Real Time Payments (RTP) system will use names as well as routing and account number details to avoid fraudulently misdirected payments. TCH is working with alternative directory suppliers to get the database of account routing and numbers and names in order to supply this functionality. TCH has noted that they have not had the same data protection issues that other jurisdictions may faces; so that customers will be opted in to this service automatically.

Proxy service (Australia)

PayID, also known as the Addressing Service, is a feature of the NPP that allows customers of financial institutions connected to the NPP to link their financial account information to simpler aliases, such as email addresses and phone numbers. Consumers are not required to have a PayID - it is rather a service that consumers can choose in order to simplify sending and receiving payments. Before a payment is made, the PayID Name will be visible to the payer, giving the payer the opportunity to validate that the payment is going to the correct beneficiary before final initiation.

Beneficiary verification (USA)

Before a payment can be initiated, the payer receives a confirmation message from the directory that states the beneficiary's information for verification. If the registered beneficiary name does not match the intended beneficiary, the payer is alerted to a potentially misdirected or fraudulent payment.

Lipis Advisors

Information sharing services

Introduction

Services that enable stakeholders to share fraud data underpins a systematic fraud prevention policy. A database of fraudulent activity, such as accounts and persons associated with fraudulent activity and methods of fraud, allows a community to identify and stop fraudsters more quickly than any stakeholder acting alone. The result can be that financial institutions have a broad view of fraud across an ecosystem, not only fraud involving their own accounts. Fraudsters that are black-listed at one bank can not move to target new victims at another.

Fraud prevention is underpinned by data, and the more this data is shared the more robust the fraud solution. Account blacklists, whitelists, data on known mule accounts, data on offenders and how frauds are being committed, and data on what constitutes an individuals normal and abnormal payment behavior provide the foundational data needed to deliver fraud solutions. Fraud information services aim to collect and disseminate fraud data across a community. Other services process data and layer value-added services for participants on top. Finally, these solutions need to balance consumer protection with maintaining a good user experience. While these services are not focused specifically on APP fraud, they help to reduce all cases of fraud. The following examples illustrate fraud information services in select markets.

Information sharing services

Data collection and sharing essential to fraud prevention

Industry Fraud Desk & Portal (Nigeria)

All PSPs are required to maintain a dedicated Fraud Desk in their respective organizations. NIBSS (PSO & CI) maintains a centralized fraud desk staffed 24/7 to exchange information and coordinate the industry response to fraud attempts/incidents. The Anti-Fraud Portal is a shared platform for banks where electronic payment frauds can be reported, monitored and tracked to avoid reoccurrence within the sector. Banks submit details of fraudulent activities, known fraudsters and their methods, to the portal where they are stored and can benefit the entire community.

Australian Financial Crimes Exchange

The Australian Financial Crimes Exchange (AFCX) was established in 2015 with the remit to be the primary channel for the exchange of fraud data for the purposes of managing and preventing financial and cyber crime. Participation in AFCX is open to all entities, both private and public sector, affected by fraud or cybercrime and will provide a direct link to law enforcement. Banks will directly feed fraud data into the AFCX system. In addition to active monitoring, AFCX will have analytical capabilities, leveraging the broader data set, to share insights with the financial and banking community.

BVN Watch-list (Nigeria)

The BVN Watch-list is a database of bank customers identified by their Bank Verification Number (BVNs) who have been involved in confirmed fraudulent activities. The database is hosted by NIBSS (PSO & CI), who is responsible for updating the database using watch-list reports submitted by banks. NIBSS is also responsible for providing banks with a portal for the verification of watch-list individuals, and an API for banks to integrate their systems to the watch-list database for online verification of watch-list individuals at the time of transaction.

National KYC Utility (Singapore)

MAS (Singapore central bank and regulator) is piloting a national KYC utility for financial services in partnership with the Ministry of Finance and GovTech, the lead agency for digital and data strategy in Singapore. The utility is expected to become the sole source for customer identification. The scheme aims to strengthen identity authentication for financial service providers on various occasions and it makes it difficult for fraudsters to use their account in criminal activities.

Lipis Advisors

Other functionality and services

Fraud and related services

Hold/freeze instructions (Nigeria)

NIBSS (PSO & CI) is empowered to issue transaction "hold" instructions on behalf of any participating bank and to advise FIs to freeze accounts identified in fraudulent transactions.

Request for Payment (USA)

TCH (PSO) offers a Request for Payment (RfP) service to request a payment directly through the central infrastructure. System rules prevent someone from sending a RfP unless money is owed or the receiver has agreed to receive such request. Prior to initiating a RfP, system rules require banks to conduct KYC measures and establish that there is a legitimate reason for using the RfP message. The receipt of a RfP message allows the payer to initiate a push payment to the beneficiary without having to enter the account details.

Withdrawal delay (South Korea)

In order to protect consumers from voice phishing fraud, the FSS (financial regulator) mandated all financial institutions that handle transactional accounts to implement a so-called 'withdrawal delay system'. The FSS found that 84% of transfers made to voice phishing fraudsters were three million won (£2050) or more. The new measure prevents cash withdrawals of transferred funds exceeding thee million won until at least 30 minutes after the transfer. According to the FSS, this gives financial authorities a window to detect suspicious activity and to suspend accounts used in voice phishing scams before withdrawals are made.

Recall request (SEPA CSMs)

Both the SEPA Credit Transfer (SCT) scheme and the upcoming SEPA Instant Credit Transfer (SCT Inst) scheme allows for Recall processing using non-payment messaging. The Recall procedure can be initiated only by the Originator Bank, which may do it on behalf of its customer. A bank may initiate a Recall procedure for the following reasons only: (1) Duplicate sending, (2) Technical problems resulting in erroneous credit transfer(s), or (3) Fraudulent originated Credit Transfer. However, to our knowledge, the function does not apply to APP fraud.

Acknowledgements

This research would not have been possible without the assistance of the local market experts who generously gave their time and expertise. We are especially thankful to the following organizations who contributed:

Organization	Country
Australian Financial Crimes Exchange (AFCX)	Australia
Bankgirot	Sweden
BankservAfrica	South Africa
Dutch Payment Association	The Netherlands
EquensWorldline	SEPA
European Payments Council (EPC)	SEPA
The Federal Reserve	USA
Financial Supervisory Service (FSS)	South Korea
Finans Danmark	Denmark
Japanese Bankers Association (JBA)	Japan
Monetary Authority Singapore (MAS)	Singapore
NACHA	USA
National Payments Corporation of India (NCPI)	India
New Payments Platform (NPP)	Australia
Nigeria Inter-Bank Settlement System (NIBSS)	Nigeria
Riksbank / RIX	Sweden
STET	SEPA
The Clearing House (TCH)	US
Zengin	Japan

About Lipis Advisors

Advising payments industry stakeholders is our core business

Company overview

Lipis Advisors is an international consultancy focused exclusively on the payments industry. We provide consulting services to clients around the world, including banks, PSPs, FinTechs, payment processors and system operators, technology vendors, industry associations, and governments.

Qualifications

- Broad global experience, deep local expertise
- Detailed knowledge of payment systems and infrastructures
- Experienced leadership, interdisciplinary team
- Highly respected & qualified subject matter experts
- Proven frameworks for delivering client value
- Extensive insights into payment systems

Contact

Nat Scheer, Director

nscheer@lipisadvisors.com

+49-30-8892-2049

Knesebeckstrasse 61a

10719 Berlin, Germany

www.lipisadvisors.com

Lipis Advisors