FNA

Building Robust Anti-Fraud & Scam Capabilities at the National Level

Contents

Executive Summary

The introduction of instant payment systems around the world has accelerated in recent years. There are now over 80 instant payment systems globally, with more than 35 being launched in the last five years and 8 currently being built[1]. These systems bring unprecedented speed and efficiency to payments markets, with greater convenience for consumers. However, faster payments also means faster fraud. For example, in Hong Kong, the volume of fraud cases more than doubled in the four years following the introduction of the Faster Payment Service in 2018[2]. Authorized Push Payments (APP) fraud losses - a form of fraud in which victims are manipulated into making instant payments to fraudsters - are expected to climb to $5.25 billion across the US, UK, and India by 2026[3].

Fraudsters use complex and sophisticated transaction schemes that span across banks to conceal the destination of fraudulently acquired funds. This means that no bank has full visibility of this network with their own payments data alone. It also means that standard rules and statistical approaches to fraud detection and prevention based on siloed bank-level data are limited in their effectiveness as they fail to fully capture the network dimension.

We argue that the problem can only be efficiently addressed by capturing the full network, including cross-bank payment flows. This can be done by collating payments data into a central data hub that enables:

- The tracing and tracking of the fund movements in real time, allowing banks to recover funds for victims and identify new mule accounts and schemes faster, as well as reduce the cost of doing so.
- More accurate methods for fraud detection and risk scoring that employ graph features of the data.
- Risk scores and features to be provided to banks in real-time via APIs to improve their own fraud models and enable them to make more accurate and faster decisions on stopping fraudulent payments.

[1] ACI Worldwide (2023)
[2] The Standard Hong Kong (2022)
[3] ACI Worldwide (2022)

01 Background and Challenges

The introduction of instant payment systems around the world has accelerated in recent years. There are now over 80 instant payment systems worldwide, with more than 35 being launched in the last five years and 8 currently being built[4]. The number of instant payments is estimated to surge from 195 billion in 2022 to 511 billion by 2027, representing a compound annual growth rate of 21.3%[5]. But while these advancements create major benefits for economic efficiency and growth, they also increase the risk of individuals and businesses becoming victims of financial crime. Fast payment processing makes it faster for fraudsters to acquire the funds, and more difficult to detect and investigate crimes, such as scams, fraud and resulting money laundering, because fraudsters can quickly move funds within the instant payment system and then withdraw illicit funds from the system. For this reason, instant payment systems are attractive tools for fraudsters.

For example, in Hong Kong, the volume of fraud cases more than doubled in the four years following the introduction of the Faster Payment Service in 2018[6]. Across the US, UK, and India, Authorized Push Payments (APP) fraud losses are on the rise and expected to climb to $5.25 billion by 2026. In the UK alone, over $1.4 billion was stolen by criminals in 2022, equivalent to over $2,750 every minute[7]. The real figures are much larger as a significant majority of fraud incidences are estimated to go unreported.

While the level and types of payment fraud vary across the world, as shown in Annex 3, reducing fraud and scams is quickly becoming a key priority for financial institutions and authorities as well as governments. At the national level, political and societal pressures to reduce consumer losses are driving central banks and consumer protection authorities to look for solutions. This is particularly acute in jurisdictions where the liability for fraud losses sits with consumers. High and growing fraud rates can also lead to the erosion of confidence in digital payments, with damaging consequences for national economic and financial development objectives. In jurisdictions where banks are liable for fraud losses, the industry pays billions every year in reimbursements to consumers, making fraud detection and prevention an increasing priority for banks as well. Annex 2 and 3 provide details on how the United Kingdom, Malaysia, Saudi Arabia, Thailand, Australia, Hong Kong and the European Union are tackling fraud and scams with new national strategies and initiatives.

This paper argues that taking a centralized data approach and deploying technology that takes advantage of this centralized data is critical to robust national anti-fraud capabilities.

[4] ACI Worldwide (2023)
[5] ACI Worldwide (2022)
[6] The Standard Hong Kong (2022)
[7] UK Finance (2023)

02 Data Sharing & Centralization

An increasing number of jurisdictions are turning to data-sharing or centralization arrangements of payments and fraud data (See Annex 3). This is because individual banks lack visibility of the rest of the payment network. Banks typically only have access to the payments their clients are sending or receiving but lack visibility of all other payments made in the economy. This means that banks cannot track funds beyond the confines of their own systems. To efficiently detect and track fraud, a complete dataset needs to capture the full network including cross-bank payment flows. The data fields available centrally need not contain Personally Identifiable Information to be valuable for tracking fraudulent funds across financial institutions.

A complete dataset also requires data on fraud incidents reported by consumers via specialist reporting institutions, financial institutions or law enforcement. This complete dataset enables investigators to train fraud detection models to uncover complex anomalies and behaviors, generate more effective risk scores and improve the accuracy of fraud and mule detection.

The operating models being put in place to operationalize a centralized data approach vary across jurisdictions depending on existing arrangements, responsibilities and liabilities. These arrangements may range from financial institution-led efforts, where data is shared between institutions, to the collection and management of data by the payments system operator, or a combination of both. For example, in countries where much of the liability for fraud losses sits with banks, such as the UK, the industry tends to take a greater lead in tackling fraud. In contrast, where liability is with consumers, such as in Malaysia, the government and central bank often play a greater role. In Hong Kong, law enforcement is leading an effort for bank employees to be co-located in one building to improve the efficiency of fraud-related information exchange between banks.

03 Solutions Enabled by Network Data

The second component is technology that fully takes advantage of the centralized fraud and payments data. This includes new technology for case management, investigation, and fraud detection. The use of centralized datasets and graph features in these tools is critical, as they capture the complex network dimensions of fraudsters' activity.

A centralized data-sharing architecture also enables each of these components to form a shared tenancy system. This means all required stakeholders, which could include the central bank, payment system operators, law enforcement and financial institutions, can have access to intelligence outputs of the same system to support their own objectives.

Case Management

Fraud case management refers to the collective technology and processes for assigning, validating, prioritizing and managing fraud cases. Due to the increasing volume and sophistication of fraudulent payment activity, it is no longer enough to consider fraud cases in silos.

First, many fraud cases reported by individuals are connected by common mules and fraudsters. This is often not taken into account when assigning cases to case officers, leading to longer times for resolving cases and the inability to identify new schemes faster. With full network visibility, connected cases can be assigned to the same case officer, improving the efficiency and effectiveness of case management and investigation. In addition, connected cases can be collected and strategic themes identified, providing further improvements to investigations.

Second, having information on potential connected cases and mule risk scores (see 3.2) and other analytical outputs will also help validate and prioritize cases. A case is likely more valid (and e.g. not related to a dispute instead) if it is connected to known or suspected mules or cases that have already been confirmed as valid. The prioritization of cases can also be based on empirical models on forecasted recoverability of the funds for the victim. Accurate validation also reduces false positive rates, and therefore potential liability associated with blocking or delaying payments.

Case Investigation

Investigators need an automated and real-time ability to track and trace the money trails emanating from fraud events across the financial system. Onward muling of acquired funds can span several

generations of mules in a matter of minutes. The speed of fraudsters' activity in combination with slow manual processes to piece together these money trails, results in low fund recovery rates. With complete and immediate visibility of the money trails, investigators can react fast, requesting the freezing of accounts and blocking any further movement of funds. This improves funds recovery rates as fraudsters don't manage to withdraw the funds from the system.

The ability to track and trace activity from reported fraudsters also helps investigators identify new undetected mule accounts as well as unreported victims. There are several benefits to this. First, it enables investigators to take proactive action instead of having to wait for frauds to be reported. Second, the newly identified mule accounts can be used as evidence in other separate or connected cases. For example, if an individual account that is under investigation is connected to three other newly detected mule accounts it may speed up the investigation outcome. Lastly, the new information feeds into better-labeled datasets and improved modeling (See Fraud Detection section below).

A major problem faced by investigators today is the time delay from the fraud event happening to when it is reported. The longer this timeframe the more difficult it becomes to track and trace the funds. This is because each suspected account in the trail will likely have other inwards and outwards payments activity, obscuring the destination of the funds under investigation. Risk scores can be calculated for payments to describe the probability the payment is associated with the fraud under investigation. This enables investigators to piece together the most likely path through which money is laundered, including the most likely mule actors and their connections to other fraud cases. With this information, investigators are more equipped to deal with fraud cases several days old.

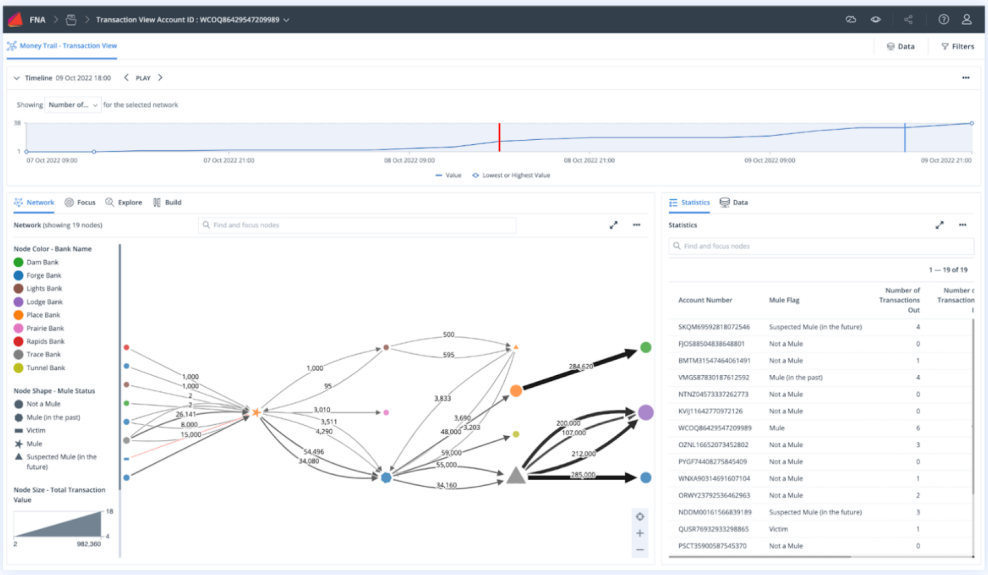

Figure 1: Screenshot of Automated Money Trails

Beyond individual case investigations, track and trace capabilities also help investigators uncover wider criminal schemes and identify the ‘big fish’ individuals in these schemes. Better visibility on the

scale of the schemes helps all stakeholders to move quickly and prevent new victims through education and law enforcement activity.

The money trails need to display a variety of data and analytical information to be of greatest use. This information helps the case officers to more quickly understand the complex set of data and make decisions. They also need the ability to filter information based on the role of the user, for example, masking personally identifiable information where it's not needed or only sharing details of customers with the customer's bank.

Fraud Detection

In addition to the ability to efficiently manage and investigate cases reported by consumers, countries can also take a proactive stance to detect unreported frauds and previously uncovered mule accounts. It is estimated that the majority of fraud instances go unreported and mule accounts unidentified, limiting the value of even the best national fraud registers - where they exist.

This can be done with machine learning algorithms that are run periodically to identify anomalies. Unlike models run at the bank level, network-level payments data allows the use of network or graph features of the data as inputs to the models. Research conducted by the Bank for International Settlements finds that current siloed data arrangements and rule-based approaches are hindering fraud detection capabilities[8]. In another paper by IBM Thomas J. Watson Research Center and ABN AMRO Bank the researchers find that taking into account "graph features" that summarize the position of the sender and receiver in the payment network, improves the accuracy of models by 30%.

Improvements in the accuracy of models have several advantages. Fewer false positives mean lower investigation costs and a lower number of legitimate payments that get blocked. More accurate models also mean faster identification of mules so that fraud losses can be reduced, as well as better information to validate and investigate cases, leading to faster case resolution times. On a national level, these benefits accumulate quickly.

Moreover, as investigation capabilities are improved, benefits also accrue. With better-labeled data (ie, data about known mules) used to train fraud detection models, we can improve the accuracy of the models over time. This virtuous cycle continues as the models become better and better at detecting fraudulent activity. This is particularly advantageous to more static, rule-based approaches to fraud detention, where fraudsters learn to adapt their behaviour to avoid being detected. With a machine learning approach, the models are also continuously adapting to fraudster behaviour, limiting criminal actors' ability to avoid detection through changing behaviours.

Compared to siloed data and standard statistical modeling approaches, a graph-based approach also reduces the ability of any one fraudster to avoid detection. This is because fraudsters are only able to change their own behavior to obscure their activity, but not those of the accounts they are interacting

[8] BIS (2023)

with, such as the victims'. Graph features capture these neighbouring behaviours and interactions within the risk scoring, thus improving detection rates.

Countries are adopting these capabilities in both batch and real-time capacities. Batch mode is suitable for sharing account-specific information, such as mule scoring, and has the advantage of not requiring real-time data integration. Real-time scoring, on the other hand, provides a more comprehensive set of risk scores but requires processing time (which is typically sub-second). The process of scoring can also be decoupled from payment release, meaning that a financial institution can carry out detection as soon as they receive the trade, and then choose whether to act on risk scores at their discretion before eventually releasing the payment.

Centralized Fraud API

In more advanced systems, financial institutions can query information about the recipient account and decide then (at their discretion) if they want to process the payment. This information can include both traditional and graph features of centralized datasets, as well as mule scores calculated by a real-time version of the service discussed in section 3.2.

The main objective of this is to support banks making independent decisions based on their own models on whether to stop a payment. In practice, some smaller banks with less advanced internal models use the risk score directly, while larger or more advanced banks use their own data and other features provided by the centralized fraud API service to enhance their own models. This all works in isolation from the payment system, to reduce any disruption to payment processing. How the query and feedback are integrated into bank systems and decision-making is the responsibility of the bank.

This approach relies on access to payments and case data from the whole system. To avoid data protection issues, the visibility of granular data elements can be defined for each stakeholder so that Personally Identifiable Information is only visible to the consumer's bank. Moreover, the value-added services for each stakeholder (payment system operators, banks, law enforcement, and the financial intelligence unit) can also be customized. See Figure 2 for a summary operational framework for this centralized fraud API.

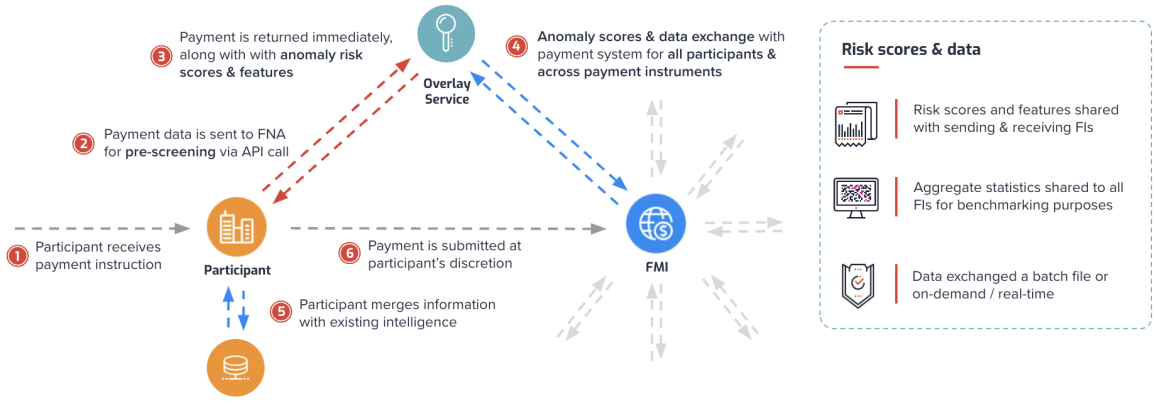

Figure 2: Proposed operational framework for this centralized fraud API

01 Annex 1: Data Requirements

This section delineates the essential data prerequisites needed to enable an effective centralized fraud case management and investigation system, along with its integration with fraud detection models. This section is strictly limited to data elements and excludes system architecture considerations.

It is important to note that solutions discussed in Section 3 determine a fraud risk score based on the main features of the transaction as part of the network of transactions. As these solutions neither require personal data nor use blacklists nor whitelists, they guarantee the privacy of the agents participating in the payment system.

Core Payment Data

The payment data processed by the instant payment system required by the centralized fraud case management tool should encompass all transaction types, including both on-us and off-us transactions. Each record should minimally include:

- Sender account identifier
- Receiver account identifier
- Payment amount
- Date and time of the transaction
- Transaction ID (if required to match transactions with fraud data)

Additional Data Elements

While not mandatory, incorporating additional data elements can enhance both the investigation process and the fraud detection accuracy. Supplementary fields may include:

- Transactional context (location, device used, ...)
- Security flags or alerts raised during the transaction process

Fraudulent Activity Labels

To enable the training of robust fraud detection models, transactions must be tagged with labels indicating whether they are associated with fraudulent activity. This labeled dataset is a needed requirement for fraud detection. The reported frauds must be explicitly linked to the payment data.

Minimal Data Volume for Model Validation

To assess the performance of the fraud detection model, a minimum data history of 4 months is recommended during a model configuration phase, including core payment data and fraudulent activity labels. This volume should be sufficient to capture transactional cyclicity and seasonality, which are important for the model in order to understand normal versus fraudulent patterns.

Anonymity and Data Privacy

The system does not require any personally identifiable information (PII) or demographic data related to account holders. Measures should be in place to ensure the anonymity of individuals to maintain privacy and comply with data protection regulations.

02 Annex 2: Fraud Payment Rates and Type by Country as of 2022

Country	Instant Payment Systems	Volume of Transactions	Payments Fraud Rate[9]	Top 3 Payment Fraud Types
Brazil	PIX, SITRAF	29.2B	22.6%	Confidence trick, Card details stolen in person, Card details stolen online
Canada	Interac e-Transfer	1.1B	24.6%	Confidence trick, Card details stolen in person, Card details stolen online
France	SCT Inst	202M	15%	Confidence trick, Card details stolen in person, Bank account hacked
Germany	SCT Inst	1.1B	14.8%	Confidence trick, Card details stolen in person, Card details stolen online
India	IMPS, UPI	89B	44.6%	Confidence trick, Identity theft, Card details stolen in person
Nigeria	NIP	5.1B	40.4%	Confidence trick, Card details stolen in person, Card lost or stolen
Saudi Arabia	Sarie	352M	33.2%	Confidence trick, Digital wallet account hacked, Card lost or stolen
Singapore	FAST, PayNow	283M	25.3%	Confidence trick, Card details stolen in person, Identity theft
United Kingdom	Faster Payments	4B	16%	Confidence trick, Card details stolen in person, Card details stolen online
United States	RTP, Zelle	2.8B	30.7%	Confidence trick, Card details stolen in person, Identity theft

[9]Payments Fraud Rate is the percentage of population who reported being a victim of fraud in the last four years.

03 Annex 3: Selected National Initiatives to Combat Consumer Fraud and Scams

There are several examples of the initiatives a number of countries globally (Malaysia, Thailand, Hong Kong, Australia, United Kingdom, Euro Area, and Saudi Arabia) have taken to protect consumers from fraud and financial crime losses. While the initiatives vary across jurisdictions, we see that central banks in each jurisdiction play an active role in either promoting, starting a pilot, or implementing a technology to investigate fraud and scams.

Malaysia

Malaysia formed a national payments network and shared central infrastructure for Malaysia's financial markets called Payments Network Malaysia Sdn Bhd (PayNet) in 2017.[10] In early 2018, it launched the Real-time Retail Payments Platform (RPP), which enables Malaysian consumers, businesses and government agencies to make real-time, data-rich payments between accounts at participating financial institutions.

The number of fraud cases in Malaysia increases each year. For example, 19,165 cases of online banking fraud involving RM94.6 million were reported by customers of financial institutions in the second half of 2022, up from the 9,735 cases totalling RM39.9 million reported in the first half of the year.[11]

Since 2022, BNM has taken a number of initiatives and coordinated with other stakeholders to combat financial fraud and scam in Malaysia. For example, BNM has been collaborating with Polis Diraja Malaysia (PDRM), Malaysian Communications and Multimedia Commission (MCMC) and the financial industry to create greater public awareness on new fraud tactics.[12] Since September 2022, BNM has also required all banks in Malaysia to adopt several countermeasures to strengthen safeguards against financial scams, such as a requirement for banks to migrate from SMS One-Time Passwords (OTP) to more secure authentication methods and tightening banks' fraud detection rules and triggers to detect and block suspicious transactions.[13]

In October 2022, the Malaysia government established the National Scam Response Centre (NSRC), in which BNM Is one of its important stakeholders. NSRC is a command center to coordinate rapid

[10] PayNet Corporate Profile. PayNet was created through a merger between the Malaysian Electronic Payment System and Malaysian Electronic Clearing Corporation Sdn Bhd
[11] BNM (2022). Financial Stability Review.
[12] BNM (2022). BNM steps up collaboration with banks and law enforcement agencies to combat new modus operandi by financial fraudsters.
[13] BNM (2022). Governor's Speech at the Launching of Financial Crime Exhibition.

response for online financial scams, to deal with a growing number of cyber fraud cases in the country. It also serves as a dedicated scam hotline for victims to contact the banks to report scam incidents promptly. Since the beginning of its launch, NSRC has handled 15,723 cases with total losses valued at RM141.47 million from October 2022 until June 2023.

Recently, as part of the important initiative to address the payment fraud problem, BNM has been working closely with PayNet to develop an industry fraud portal, where banks report all the accounts or transactions that they suspect as fraudulent. The main objectives are automating and increasing the ability to trace the fund and enhancing the portal with more comprehensive data to identify the money mules.[14]

Thailand

PromptPay, the real-time payment system in Thailand, was launched in 2016. It allows users to transfer money using their citizen ID, mobile phone number (or recipient's other identification number) and bank account number via digital channels.[15] It has 48 million average daily payment numbers, THB 128 billion average daily payment value, 30 banks and 121 million account numbers.

In 2021, the Office of the National Economic and Social Development Council (NESDC) conducted a study that uncovered nearly half of the people in Thailand had been scammed "through the Internet and modern communication" within one year, with an average damage value of about THB2,400 per person.[16] Data from the Ministry of Digital Economy and Society (DES) shows that more than 1,500 people were arrested in Thailand for online fraud and gambling in 2022, and that 58,463 bank accounts were opened illegally for cybercrime purposes.[17]

To counter fraud, cybercrime and scams in the country, the Thailand Government has enacted new legislation. The Royal Decree on Measures for Protection and Suppression of Technology Crimes was published and took effect in Q1 2023. The Royal Decree would empower the data sharing on suspicious transactions between financial institutions and related authorities, also, the immediate block of any suspicious transactions by financial institutions and the imposing apparent penalty against those involving mule accounts, as well as strengthening collaboration of related organizations for more concrete.

In March 2023, Bank of Thailand (BOT), the Thai Bankers' Association (TBA), and the Government Financial Institutions Association (GFA) jointly announced to step up in combating financial fraudulent activities. Bank of Thailand issues additional measures to combat financial fraudulent activities. For the preventive measures, banks mutually agree to stop sending SMS with links to their customers and constantly improve the fraud surveillance systems. For the detective measures, BOT is set to launch the Central Fraud Registry. Central Fraud Registry is an automated solution to fight scams and

[14] www.businesstoday.com (2023). BNM, Banks, Govt Agencies Unite To Battle Rising Online Financial Fraud.
[15] Bank of Thailand (2023). PromptPay.
[16] ComplyAdvantage (2023). Central Fraud Registry.
[17] Bangkok Post (2022). 1500 Arrested for Online Fraud Gambling.

address illegal payments, fraud and mule accounts. For the responsive measure, banks are required to set up a hotline call center, available twenty-four hours, seven days a week for financial fraud victims to directly contact.[18]

Hong Kong

Hong Kong launched its fast payment system (FPS) in 2018. FPS is operated by Hong Kong Interbank Clearing Limited (HKICL). As of August 2022, the number of FPS users (both consumers and merchants) was 10.9 million with more than 900,000 average daily payment numbers.[19]

Fraud continues to pose a high threat to the banking sector in Hong Kong. In 2022 alone, it led to approximately HKD 4.8 billion monetary losses.[20] Given the concerning threat that fraud brings to the banking sector, fraud prevention and detection is a priority for HKMA. Recently, Chief Executive of HKMA, Mr. Eddie Yue, expressed the importance of the use of data and technology as well as joint-collaboration among various stakeholders to address the fraud problem in Hong Kong: "Working collaboratively, we will scale up the use of data and technology in the fight against abuse of the financial system by fraudsters and criminals, with a view to maintaining safety and efficiency of our banking system".[21]

In May 2023, HKMA and Deloitte co-published a report entitled "AML Regtech: Network Analytics".[22] The report describes an initiative led by HKMA to protect consumers from fraud and financial crime losses. As part of its collaboration with industry (e.g., banks) and law enforcement (e..g, Hong Kong Police Force), HKMA has started a pilot using network analytics to detect mule account networks and help disrupt movements of fraud proceeds. This report highlights the potential of combining intelligence-led analytical tools with rules-based monitoring systems, which will help banks to enhance anti-deception efforts in the prevention, detection and disruption of financial crime.

The report also highlights two other important initiatives that HKMA has started and engaged with the banking industry, business community and relevant stakeholders. First, starting in November 2021, HKMA has conducted three AML Regtech Lab (AMLab) sessions to promote the use of network analytics and low-barrier technologies for banks. To date, 14 banks in Hong Kong have engaged in the initiative. Second, in May 2017, HKMA launched the Fraud and Money Laundering Intelligence Taskforce (FMLIT), which comprises representatives from the law enforcement, the regulator and the banking industry. To date, about 60% of FMLIT bank members are deploying network analytics technology. As a result, HKMA has observed a positive increase (2022 versus 2021) in the number of

[18] Bank of Thailand (2023). The Bank of Thailand (BOT), the Thai Bankers' Association (TBA), and the Government Financial Institutions Association (GFA) jointly announced to step up in combating financial fraudulent activities.

[19] HKMA (2022). The Fourth Anniversary of the FPS - from person-to-person to merchant and cross-border payments.

[20] RTHK (2023). Crime jumps 8.7 percent in HK after rise in scams.

[21] RTHK (2023). Crime jumps 8.7 percent in HK after rise in scams.

[22] HKMA & Deloitte (2023). AML Regtech: Network Analytics.

new suspicious accounts/entities identified (62%) as well as a positive increase in the amount of criminal proceeds restrained / confiscated (113%).

In addition to the ongoing pilot discussed above, Ms. Carmen Chu, Executive Director (Enforcement and AML) at HKMA, also discussed in the report that HKMA also promotes innovative approaches, including proactive, real-time monitoring and interception of fraud-related payments.

Australia

launched its New Payments Platform (NPP), an open access infrastructure for fast payments, in February 2018. The NPP came about as a result of Reserve Bank of Australia (RBA)'s Strategic Review of Innovation in the Australia Payment System. The NPP was developed via industry collaboration to enable households, businesses and government agencies to make simply addressed payments, with near real-time funds availability to the recipient, on a 24/7 basis.[23]

Fraud and scams pose a serious and growing threat in Australie. The Australian Competition and Consumer Commision reported a record $3.1 billion lost to scams in 2022, 80% higher than the financial losses in 2021. Investment scams were the highest loss category ($1.5 billion), followed by remote access scams ($229 million) and payment redirection scams ($224 million). Australia's Scamwatch received 239,237 scam reports last year, a 16.5 per cent drop on the number of reports received in 2021. However, financial losses reported to Scamwatch in 2022 totalled more than $569 million, a 76% increase compared to losses reported in the previous year.[24]

In 2023, Australia launched the National Anti-Scam Centre to coordinate government, law enforcement and the private sector to combat scams. It builds on the work of the Australian Competition and Consumer Commission (ACCC)'s Scamwatch service.[25] In 2023, Australian banks have also launched a new digital platform, Fraud Reporting Exchange (FRX), that will facilitate the quick reporting of fraudulent payments en route or transferred to another bank.[26] This will help disrupt fraudsters and scammers by allowing the reporting of scam payments in close to real time, boosting the likelihood that funds can be frozen and returned to customers. The FRX is owned and operated by the AFCX.

United Kingdom

The UK's Faster Payment System (FPS) has been created since 2008, enabling individuals, businesses and government agencies to make real-time payments. It is operated by Pay.UK, regulated by the Bank of England, Financial Markets Infrastructure Directorate (BoE-FMID) and the

[23] Reserve Bank of Australia (2023). The New Payments Platform.
[24] Australian Competition and Consumer Commission (2023). ACCC calls for united front as scammers steal over $3bn from Australians.
[25] Australian Competition and Consumer Commission (2023). National Anti Scam Centre.
[26] Australian Banking Association (2023). Australian banks join new Fraud Reporting Exchange digital platform to help halt payments to scammers

Payment Systems Regulator (PSR). In 2021, FPS processed 3.4 billion transactions with a value of £2.6 trillion. This represented a year-on-year volume increase of 568 million payments, or 20%, and a 24% jump in values (up from £2.1 trillion in 2020).[27]

``Fraud is the most commonly experienced crime in the UK, with online fraud estimated to account for 80% of all fraud.[28] According to the Office of National Statistics, there were 3.7 million incidents of fraud in England and Wales in the year ending December 2022. 86% of fraud instances are estimated to go underreported.[29]

Victims of fraud range across vulnerable individuals, major corporations, smaller businesses, as well as the public sector. £2.46 billion lost by businesses and individuals alone to fraud in the financial year 2021/22. This is a 17% increase on the year 2020/21.[30]

To address the fraud and scams problems in the country, the UK launched Action Fraud in 2009. Action Fraud is a national reporting center for fraud and cybercrime. It is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB), who are responsible for the assessment of the reports and ensuring fraud freeport information is shared. In the year ending March 2021, Action Fraud received victim reports totalling a loss of £2.35 billion.[31]

Then, in 2018, Pay.UK's Faster Payments team rolled out new technology that enables banks to track and pinpoint fraudulent payments transactions across multiple, connected mule' accounts. The technology alerts financial institutions to suspect money laundering accounts within their own four walls, so they can act to avoid potential losses, fines and reputational risk. It also enables institutions to work together at industry level to shut down mule networks, disrupting fraud and money laundering, which amounts to millions of pounds annually. Financial institutions receive dispersion tree visualizations, and both individual FI and industry money mule network reports.

In 2019, the UK Government published a Fraud Strategy policy, aimed to reduce fraud by 10% by December 2024. Some of the initiatives include establishing a national fraud squad with over 400 new specialist investigators, replacing Action Fraud with a state-of-the-art reporting system, revolutionizing tech company action to block fraud at an industrial scale, and helping banks slow down suspicious payments. The government will disrupt crucial money laundering techniques and protect the public by delivering a coordinated response from government, regulators, law enforcement, industry and organizations working with young people. This will bring together campaigns and education to raise public awareness of the risks of getting involved, innovation by the financial sector to identify mule networks and freeze funds, law enforcement work to target the mule recruiters and controllers, and action by social media companies to close down recruitment routes, balancing deterrents and safeguarding for identified money mules.[32]

[27] Pay.UK (2023). Faster Payment System.
[28] National Crime Agency (2023). National Economic Crime Centre.
[29] Office for National Statistics (2022). Crime in England and Wales.
[30] National Crime Agency (2023). Fraud and economic crime.
[31] UK Government (2023). Fraud Strategy.
[32] UK Government (2023). Fraud Strategy.

Euro Area

The European Commission has unveiled a legal framework that paves the way for the introduction of an electronic currency across the 20 member states that use the euro, called Digital Euro. Digital Euro would be an electronic system of payments and transactions, by the European Central Bank (ECB). It would give consumers the option to use central bank money in a digital format, complementing banknotes and coins. A digital euro would provide a digital means of payment universally accepted throughout the euro area, for payments in shops, online or from person to person.[33]

As part of the Digital Euro Project, ECB has published a document that presents an initial investigation on the fraud prevention and detection for the Digital Euro.[34] The document describes the vision to build a central utility fraud model called Central Support Service (CSS). The CSS would provide controls such as fraud monitoring and risk scoring, maintaining gray and blacklists, and information sharing between intermediaries. On top of fraud prevention and detection at intermediaries, there are three optional degrees of support that ECB is considered for the CSS:

- CSS is involved directly in pre- and post-fraud analysis, also in real-time
- CSS is involved directly in post-fraud analysis, not in real-time
- CSS is involved indirectly only

Saudi Arabia

The Saudi Central Bank (SAMA) launched an Instant Payment System in 2021, called Sarie. It is operated by Saudi Payments, a wholly-owned subsidiary of SAMA.[35]

In 2022, Saudi Central Bank Governor Dr. Fahd bin Abdullah Al-Mubarak inaugurated the Joint Operations Center for Saudi Banks, tasked with following up and monitoring cases of financial fraud that bank customers may be exposed to. The center brings together all Saudi banks under one roof to improve the customer experience and tackle confirmed cases of financial fraud. The formation of a joint center is one of the quick and effective procedures, which reflects the cooperation and integration required between all Saudi banks to limit the development of fraud cases, in addition to the previously issued instructions and regulatory requirements related to combating financial fraud.

The Joint Operations Center to combat financial fraud cases, which the Saudi Bank “Albilad” took the initiative to host, operates 24/7, under the direct supervision of the Saudi Central Bank, and is located on a total area of 1,300 square meters, and includes 162 workstations.[36]

[33] European Central Bank (2023). FAQ on a digital euro.
[34] European Central Bank (2023). Fraud prevention and detection.
[35] Sarie (2023). About Sarie.
[36] Saudi Press Agency (2022). SAMA Governor Inaugurates Saudi Banks’ Joint Operations Center to Combat Financial Fraud.