NICE Actimize

eBook

PSR Fraud Liability Shift: Are You Ready?

Updated December 2023 to reflect the PSR’s policy changes

The U.K. Payment Systems Regulator's (PSR) notification of liability changes, on 7 June 2023, impacts all U.K. Financial Institutions (FIs) and Payment Service Providers (PSPs). The notification provided further guidance on the standards and policies on requirements for fraud reimbursement as consumers continue to be victimised by Authorised Push Payment (APP) scams.

In summary, there's a requirement for FIs and PSPs to reimburse 'all in-scope customers' that are victims of APP scams. According to the PSR, sending and receiving FIs and PSPs will share the cost of reimbursement to victims by 50-50. There are also new protections for consumers who may be more vulnerable to APP scams.

The scope of the changes centers on Faster Payments transactions that were adopted in May 2008. Although the foundation of payment rails remains consistent, fraudsters' preference for faster payment mechanisms is in line with an unfortunate reality: payment speed advances both the volume and success of APP scams. In parallel, the PSR expressed that FIs' voluntary efforts to combat APP scams fell short. Consequently, the PSR responded to this growth in APP scams by extending the existing voluntary Contingent Reimbursement Model (CRM) Code that set the stage back in 2019: **The proposed 50-50 shared liability between sending and receiving institutions is now an industry requirement, not voluntary.** These changes reinforce a commitment to see victims of APP scams made whole, but also to encourage FIs to implement more effective safeguards.

Many FIs have adopted Confirmation of Payee (CoP), designed to reduce the risk of payments being sent to the wrong account by verifying that the account name matches the sort code (bank code) and account number provided. This provides another strategy to help consumers avoid becoming victims of APP scams, but it's not a silver bullet solution.

While FIs and PSPs have been processing real-time payments for over 15 years and added compensating risk controls for unauthorised fraud, they must leverage modern multilayered solutions to identify, mitigate, and resolve these new, more complex APP scams.

This replication is a change in mindset (flip of the coin) to solve for APP and scam issues that were once not tackled or addressed with refined fraud strategies modeling.

FIs and PSPs must look at the issue holistically and enhance many internal controls. This will address unanticipated losses from liability shifts, but also help them conform and comply with PSR mandates on APP scams.

Introduction

Important Considerations for PSPs

Data: Banks and PSPs Must Embrace an API-First Data Environment

Fraud Detection and Prediction

Strategy Management: Holistic Approach Using AI/ML Models

Claims & Case Management: An Overhaul and Expansion of Today's Practices

Holistic Approach to Fraud for PSR Compliance

Important Considerations for PSPs – Highlights from the PSR's December 2023 Policy Statement and Final Decision

PSPs and FIs that didn't comply with CRM are expected to **start work now** to implement the reimbursement requirements.

- Banks cannot 'blindly' apply a £100 claims excess against a consumer's claims. Additionally, the excess does not apply to vulnerable consumers whatsoever.
- Victims of APP scams are expected to submit a report to the sending PSP no more than 13 months from the completion date of when their last respective APP scam payment was executed. Consumer education programs need to reference both the 13-month reporting requirement deadline and timely notification of events.
- Time to reimburse: the sending PSP has a limited time for thorough claims review and must arrive at an outcome within 35 business days maximum, including any uses of 'Stop the Clock.'
- Consumers must have regard to tailored, specific warnings raised by their PSP before an authorised push payment is executed.

Introduction

Important Considerations for PSPs

■ ■ ■

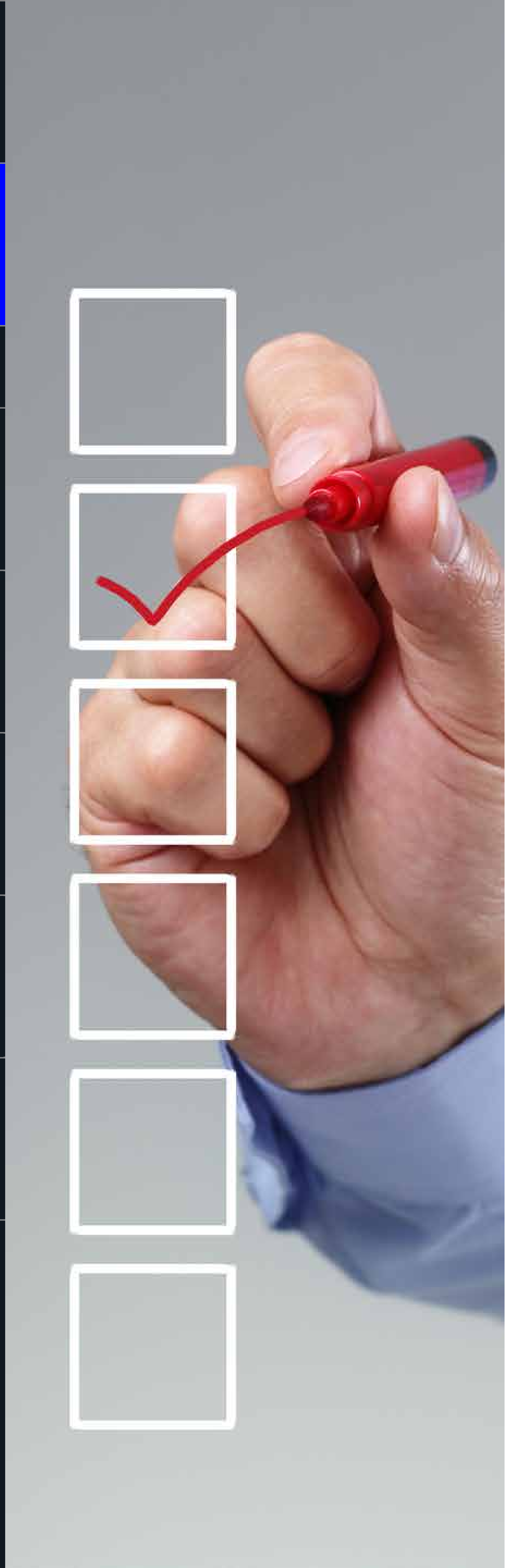
Data: Banks and PSPs Must Embrace an API-First Data Environment

Fraud Detection and Prediction

Strategy Management: Holistic Approach Using AI/ML Models

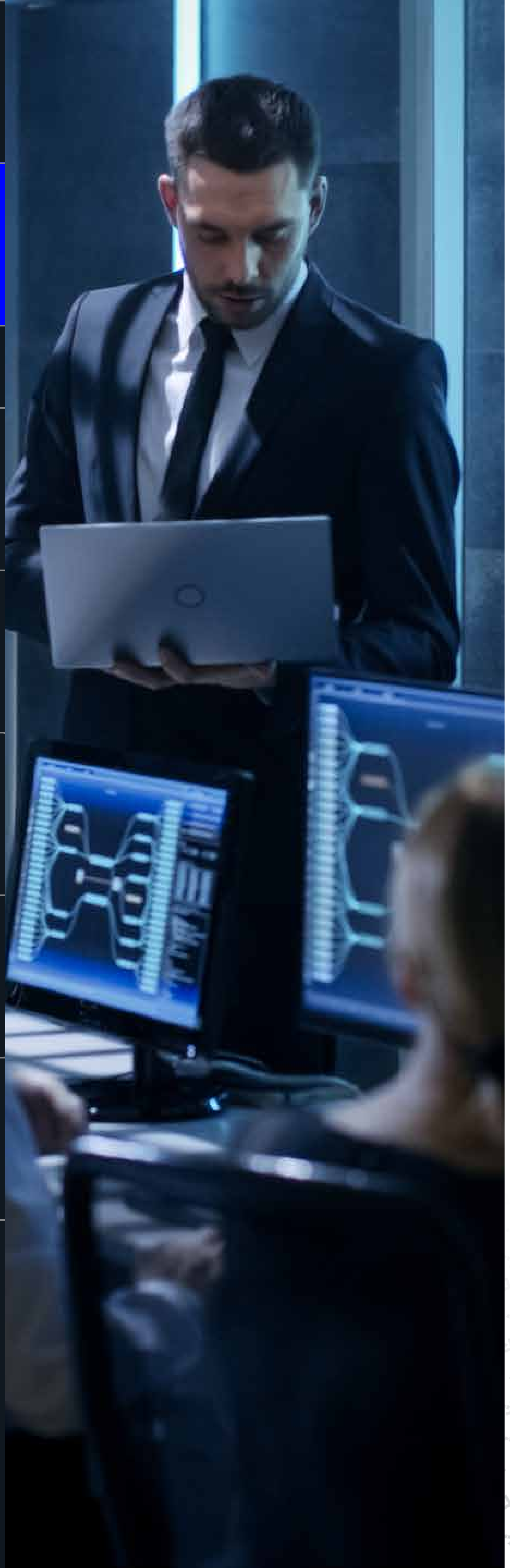
Claims & Case Management: An Overhaul and Expansion of Today's Practices

Holistic Approach to Fraud for PSR Compliance



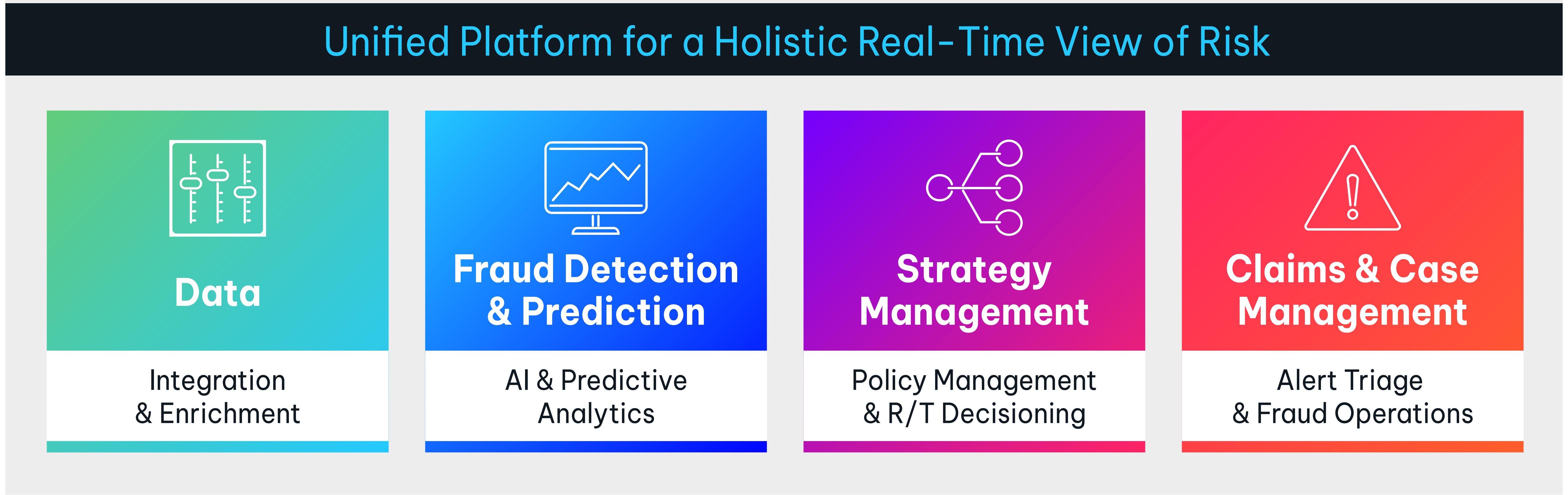
The new reimbursement requirements are underpinned by **9 key principles**, designed as a balanced package to set out the framework of the policy:

1	**Reimbursement requirement for APP fraud is only applicable to Faster Payments** (Inclusion of CHAPS is planned on behalf of the Bank of England)
2	**Receiving PSPs will be responsible for 50%** of the cost of a claim to the sending PSP, 50% of any later retrieved or recovered funds must be returned to the sending PSP by the receiving PSP
3	**Exceptions for APP fraud claims cases where the customer has acted:** • Fraudulently (first-party fraud) • With gross negligence (referring to the customer standard of caution)
4	**Time limit to reimburse**—PSPs must reimburse customers within 35 business days. For specific actions, the PSP can 'stop the clock,' but not past 35 business days
5	**Claim excess**—Sending PSPs have the option to apply a claim excess of £100
6	**Customer Standard of Caution Exception**—PSPs' means to deny false and fraudulent claims is limited
7	**A maximum per case reimbursement** of £415,000
8	**Time limit to claim**—Sending PSPs can deny claims submitted more than 13 months after the final payment to the fraudster
9	**Customer treatment**—The customer standard of caution and claim excess shouldn't be applied to individuals defined as "vulnerable customers" according to the policy



End-to-End APP Fraud Coverage

In order to effectively manage APP Fraud and forthcoming changes, FIs and PSPs must take action in four key areas:



Unified Platform for a Holistic Real-Time View of Risk

Data

Integration & Enrichment

Fraud Detection & Prediction

AI & Predictive Analytics

Strategy Management

Policy Management & R/T Decisioning

Claims & Case Management

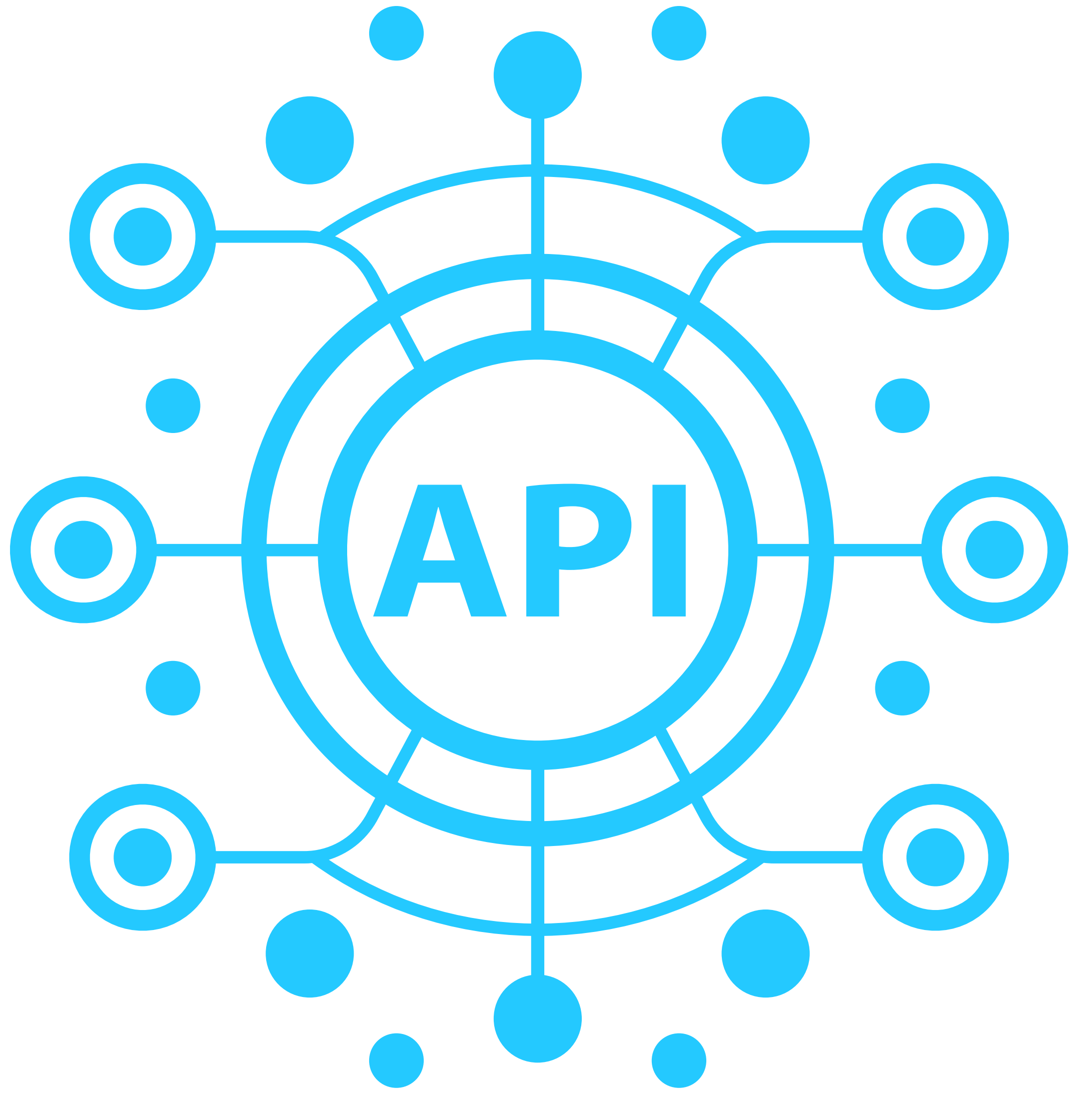
Alert Triage & Fraud Operations

Data: Banks and PSPs Must Embrace an API-First Data Environment

Numerous data-related requirements will be mandatory to ensure vital customer, transaction, and claim details are seamlessly transmitted securely through APIs when possible.

Third-party data, such as behavioural biometrics and other risk signals, are useful to detect certain types of scams or data sources that include compromised accounts and payors, providing early visibility into money mule accounts.

Information sharing between FIs and PSPs is critical, so using APIs can bring quick resolution to the significant volume of APP claims.

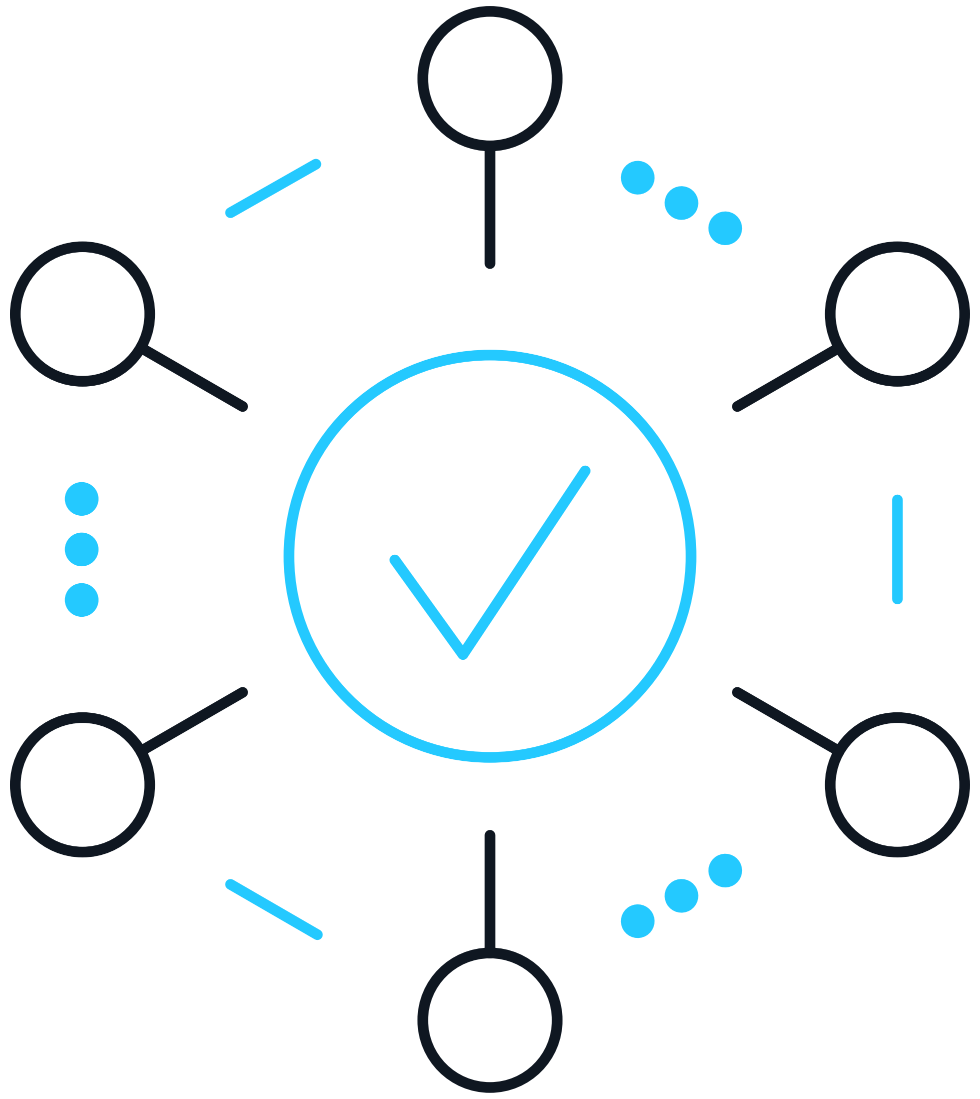


Fraud Detection and Prediction

Early detection and identification are key components to a successful fraud prevention strategy.

Prevention: Employ advanced real-time prevention strategies to swiftly identify instances of first-party fraud and mule activity within newly established accounts. Early account monitoring needs to include analyzing incoming and outgoing transactions in conjunction with comparative behavioural patterns exhibited by peer profiles. This accelerated detection capability significantly curtails potential risk by facilitating expedited intervention procedures. By using a range of tailored fraud indicators optimised to spot anomalous behaviour, FIs can intervene much sooner, mitigating risk.

Real Time: The accepted idea that Faster Payments equal faster fraud highlights a critical challenge demanding immediate attention. To effectively counter this expected uptick in fraud, FIs and PSPs must implement real-time monitoring. It's only through managing payments in real time that they can proactively detect and respond to fraudulent activities in the dynamic instant payments landscape.



Intelligence: Under PSR's Final Policy, December 2023 (Chapter 7, para. 20 and Chapter 8), FIs must use intelligence that standardizes how customer data will be sent, ingested and used in transaction risk assessments. NICE Actimize Collective Intelligence Models leverage feedback data to continuously tune models for enhanced detection.

Enrichment: A comprehensive risk assessment approach will integrate third-party data sources for enrichment. Combining insights from online and mobile risk factors is the way to effectively identify scams and mule activities. When merged with transaction-level data, these risk insights form a coherent strategy that enhances fraud detection while also minimising false positives.

Orchestration: Efficient data wrangling and adept handling of data flows will play a pivotal role in the detection process and the management of alerts within operational groups. NICE Actimize's typology-centric detection approach, coupled with purpose-built operational reviews, is designed to tackle the intricate and specialised aspects involved in scrutinising both outbound scam and inbound mule transactional activities.

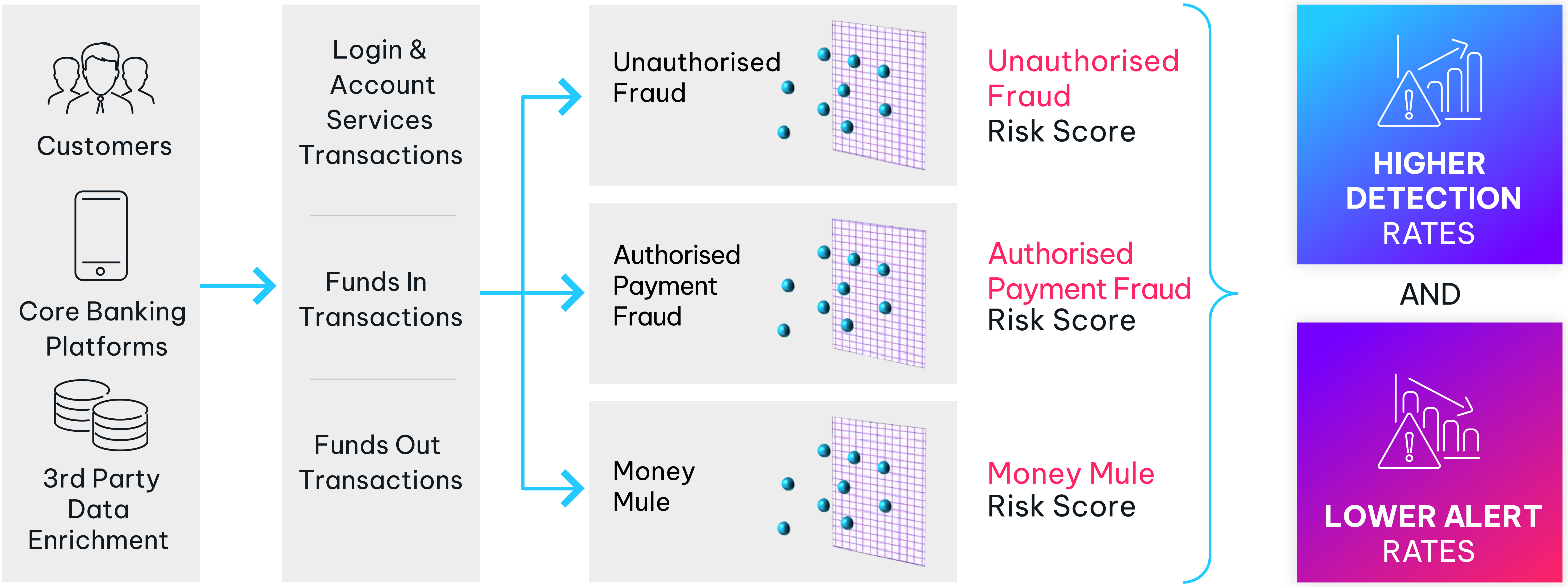
Strategy Management: Holistic Approach Using AI/ML Models

FIs have made significant strides in mitigating third-party fraud losses in recent years. Their success at mitigating third-party risk can be replicated to combat APP and money mule threats. Fraudsters exploit consumers through deception tactics, manipulating them into becoming operatives in their schemes. Analysing monetary and non-monetary events generates a holistic risk assessment.

It's now essential to consider third-party involvement, APP scams, and money mule activities in the overall strategy management. FIs can speed up scam detection and identify mule activity by updating data analysis approaches to incorporate third-party enrichment, pooled collective intelligence, and historical profiling consumer activity. This enables FIs to construct a comprehensive risk assessment framework.

FIs can address these challenges head-on with NICE Actimize's Multi-Model Execution (MME) methodology, adept at navigating diverse risk scenarios to decode evolving attack methods. MME machine learning models generate a three-part score encompassing unauthorised, authorised, and mule fraud scenarios. Organisations are empowered to pinpoint victims and culprits with heightened detection precision while minimising any adverse impact on genuine clients.

Multi-Model Execution



Customers

Core Banking Platforms

3rd Party Data Enrichment

Login & Account Services Transactions

Funds In Transactions

Funds Out Transactions

Unauthorised Fraud

Authorised Payment Fraud

Money Mule

Unauthorised Fraud Risk Score

Authorised Payment Fraud Risk Score

Money Mule Risk Score

HIGHER DETECTION RATES

AND

LOWER ALERT RATES

Introduction

Important Considerations for PSPs

Data: Banks and PSPs Must Embrace an API-First Data Environment

Fraud Detection and Prediction

Strategy Management: Holistic Approach Using AI/ML Models

Claims & Case Management: An Overhaul and Expansion of Today's Practices

Holistic Approach to Fraud for PSR Compliance

Claims & Case Management: An Overhaul and Expansion of Today's Practices

The forthcoming PSR mandates will have global, significant impact on the mandatory reimbursement process, as it encompasses all FIs and PSPs operating within the U.K. market. The introduction of a 50-50 reimbursement split between the sending and receiving institutions adds a layer of complexity to the existing operational procedures. In preparation, organisations must initiate comprehensive evaluations across critical stages, such as:

- Claim Intake and Capture
- Triage and Investigation
- Consumer Reimbursement
- Financial Recovery
- Claim Finalisation, Tagging, and Reporting

The scale of this undertaking becomes especially apparent when considering the £485 million in reported U.K. APP Fraud Losses in 2022.[1] It will put key operational KPIs in managing full consumer reporting under the new 2024 PSR requirements to the test.

[1] UK Finance: What did the 2023 UK Finance fraud report tell us?

Introduction

Important Considerations for PSPs

Data: Banks and PSPs Must Embrace an API-First Data Environment

Fraud Detection and Prediction

Strategy Management: Holistic Approach Using AI/ML Models

Claims & Case Management: An Overhaul and Expansion of Today's Practices

Holistic Approach to Fraud for PSR Compliance

Within the framework of the PSR's Final Policy, organisations will need to conduct comprehensive reviews across several crucial areas right now, including:

- **Intake & Attestation of Events:** Evaluate processes for capturing and verifying incoming claims or incidents, ensuring the customer-provided information is accurate and complete as a fundamental step in addressing fraud-related matters

  - **PSR Final Policy, December 2023 (Chapter 6, para. 23 and Chapter 8):** Intake analysts will need to assess whether the FCA's definition of vulnerability has been met in order to apply different claim handling standards and to record this within records of the system.

- **Triage:** The triage process is where claims or incidents are categorised and prioritised based on their severity and potential impact. Developing an efficient, well-defined triage mechanism is essential for streamlining subsequent actions
- **Investigation:** Delving into the investigation phase, organisations need to ensure procedures are crafted to scrutinise claims or incidents. This includes analysing evidence, verifying authenticity, and determining the legitimacy of the reported events from the customer. Under the PSR guidelines, investigators will need to leverage newly formed communication channels to ensure there is no customer collusion or claim abuse in play

  - **PSR Final Policy, December 2023 (Chapter 5):** Investigation and determination of Consumer standard of caution exception requirements (gross negligence). One of these exemption requirements is Police reporting, which is intended to deter first-party fraud.

- **Consumer Financial Resolution & Reimbursement:** The procedures for handling consumer reimbursements and financial resolutions must be assessed. This involves not only the actual reimbursement process but also the communication and support mechanisms for affected consumers. Additionally, should there be successful recoveries received during the investigation/post-investigation process, then claim financials are adjusted

  - **PSR Final Policy, December 2023 (Chapter 1, para. 46):** Fraud systems will need to track the recovery of funds in all cases. They will be able to apply user-defined parameters determining fund allocation in individual cases. This will enable the correct allocation of funds to cases that have previously been reimbursed.

- **Finalisation—Send and Receive Bank Traceability:** As part of the reimbursement process mandated by the PSR, the traceability of funds from all banks is necessary to maintain regulatory compliance. This is accomplished by prioritising transparency and accuracy in the finalisation stage.
- **Dashboard Visualisation:** To effectively manage the intricate landscape of fraud-related activities, organisations need to develop clear and insightful dashboard visualisations. These visual aids offer a consolidated overview of the entire process, aiding decision-making and key metrics monitoring. Managerial reporting for claim pipeline, loss exposures, and adherence to regulatory timelines is key in the day-to-day management of fraud claims

  - **PSR Final Policy, December 2023 (Chapter 3, para. 18 and Chapter 4, para. 34):** Fraud systems will need to retain records of when claims were made by customers and track the timeframe to complete them. It will support the production of management information on time required to investigate claims. The solution will produce exception reporting of cases nearing user-defined SLAs (e.g., five days) and allow individual cases to be paused ("stop the clock") whilst additional information is gathered. Fraud systems will need to support exception reporting of cases in this state.

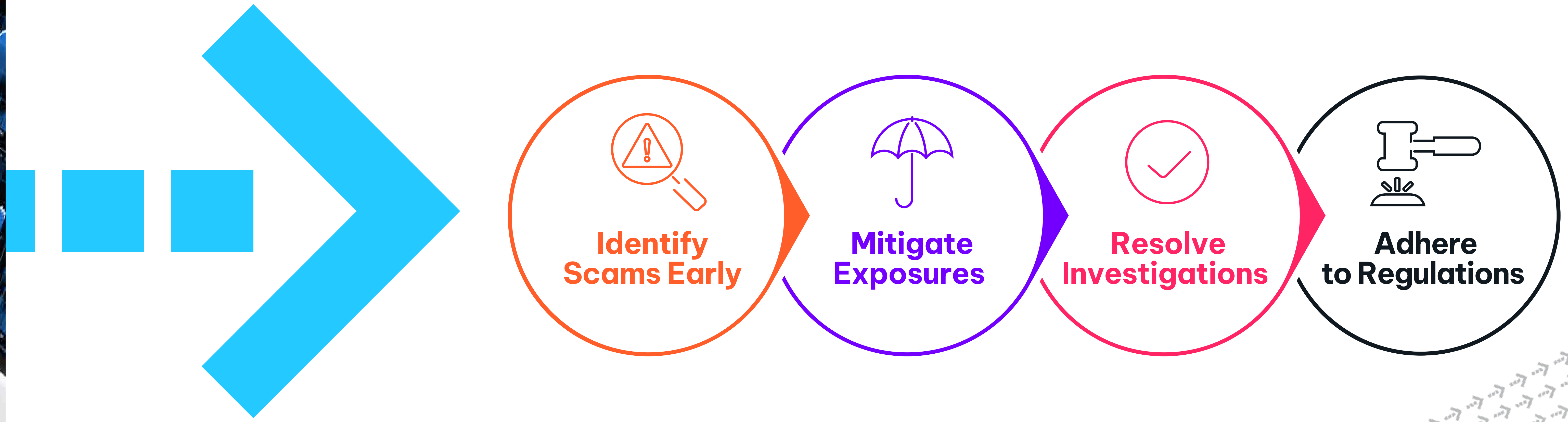
- **Communication Channels and Interoperability Between Investigating Organisations:** Effective communication channels and seamless interoperability between investigating organisations are necessary to streamline collaboration. Assessing these aspects ensures that information flows efficiently, promoting better coordination in addressing fraud-related concerns

- **PSR Final Policy, December 2023 (Chapter 8, para. 19, Table 7):** Organisations and systems will need to have the flexibility to align with Pay.UK EFD (Enhanced Fraud Data) through which standardised customer data will be sent, ingested, and used in transaction risk assessments and fraud investigations.
- **PSR Final Policy, December 2023 (Chapter 3, para. 21, Point 2):** Sending PSPs must notify a receiving PSP of an APP scam case within a to-be-determined timeframe set by Pay.UK. Considering well-known scam claims and recovery difficulties in industry, PSPs will need fraud systems that allow for real-time notifications to other PSPs via case management platforms, so as to notify the receiving PSP as quickly as possible of an APP fraud claim. Fraud systems will also need to be capable of receiving a real-time notification of a receiving account from another PSP. The solution will facilitate the sharing of case information between the two firms.
- **PSR Final Policy, December 2023 (Chapter 5, para. 32):** PSPs can encourage victims to contact the police and request a crime reference number. There may be cases where this is not possible, like if a customer has vulnerabilities that would make this difficult. In these cases, the sending PSP should support the customer in notifying the police. Failure to notify the police cannot be considered a reason to deny a reimbursement claim.
  - Fraud systems should have the capability to interact with police reporting systems including batch reporting of claims made by customers (real-time notification not required.)

Holistic Approach to Fraud for PSR Compliance

Going forward, FIs and PSPs that take a holistic approach and enhance internal controls can shield themselves from liability-shift losses, but also comply with new PSR mandates on APP scams. Though new reimbursement requirements won't be in effect until 7 October 2024, now is the time to update processes and technology. Implementing new controls now can mitigate risk while protecting customers from fraudsters who seek to circumvent an FI's internal controls by using money mules and executing APP frauds.

Act now to:



Identify Scams Early

Mitigate Exposures

Resolve Investigations

Adhere to Regulations

Explore NICE Actimize fraud prevention solutions.

NICE Actimize

Learn more

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com