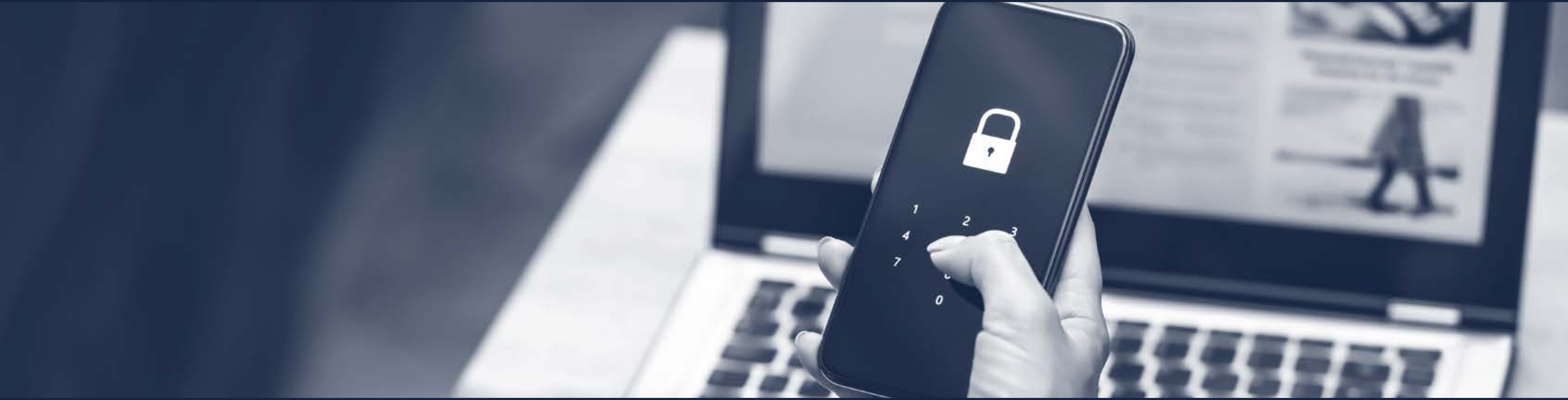
Impact Study

In association with:

Form3

APP Fraud Liability: A Guide for Banks



Finextra | FORM3

Contents

01 | Introduction

The UK Government's 2023 'Fraud Strategy' report highlighted three pillars that would now be prioritised: pursuing fraudsters, blocking fraud, and empowering people. With fraud now accounting for over 40% of crime - but receiving less than 1% of police resources – it is evident that more needs to be done to ensure that the consumer is protected.

This challenged financial institutions to do more, particularly with the announcement that the Financial Conduct Authority (FCA) will assess firms' fraud systems and controls, but also enable payment services providers (PSPs) to adopt a risk-based approach to allow fraudulent payments more time to be investigated.

The report explored how faster payments and real-time payments have led customers and businesses to make payments quickly and efficiently. But fraudsters have also leveraged this to defraud the very same customers and businesses, and in turn, move money rapidly so lost funds can never be successfully repatriated.

While financial institutions and regulators are collaborating to implement new practices – such as Strong Customer Authentication (SCA), Confirmation of Payee (CoP) and The Banking Protocol – to spot suspicious payments, more needs to be done. Currently, the Contingent Reimbursement Model Code (CRM Code) does reimburse customers who are not to blame for the success of a scam. However, there is a stark difference between the reimbursement rate of organisations that are part of the CRM Code, and those that aren't. The Payment Systems Regulator (PSR) revealed that one CRM Code bank fully reimbursed 94% of the APP scam cases reported to it, whereas one bank that is not saw only reimbursed 6% of cases.

To tackle fraud 'upstream', the PSR has called for standardised identification of risky payments, and sharing of this data so that suspicious payments can be recognised in real-time. The PSR have now legislated to ensure APP fraud victims get their money back within five working days. Banks and PSPs will be incentivised to take responsibility, with both sending and receiving firms splitting the costs of this reimbursement 50:50. This type of fraud is prevalent, and increasingly so, as victims are tricked into authorising payments.

As per the Financial Services and Markets Bill, all PSPs will be required to reimburse fraud victims from October 2024.

What is the challenge?

How banks can effectively manage the liability associated with APP fraud, and manage being 100% responsible for refunding victims. With this coming into effect in 2024, banks must implement new methodologies to be able to investigate effectively.

How can banks avoid this operational nightmare?

By increasing access to the right levels of intelligence. This is easier said than done, but the liability shift provides banks with a key date to act. Banks, under the new requirements, must reimburse the customer. However, the key question in the industry is: to what extent will banks need to prevent reimbursements having to be provided and at what cost?

This dichotomy of priorities will require:

1. Payments to be risk scored;
2. The false positive rate to be considered;
3. The right intelligence to be implemented;
4. The intelligence to be embedded into the strategy;
5. Explainability to be ensured; and
6. Improved customer experience.

02 | Risk score payments

Why risk score payments?

APP fraud, when an individual is tricked into sending money to a fraudster posing as a genuine payee, can be devasting for people. APP scams can involve either a 'malicious payee', for example, duping someone into purchasing goods that don't exist or are never received, or 'malicious redirection', when a fraudster impersonates bank staff to get someone to transfer funds out of their bank account and into that of a fraudster.

UK Finance figures show that a staggering £239.3 million was lost to APP fraud in the first half of 2023. What is also evident with this statistic is that potential financial losses are colossal. With banks on the precipice of being liable for refunding fraud victims, financial institutions must establish a robust strategy to protect themselves from financial losses and reputational damage – whether that be as a victim of fraud or as a bank now responsible for remedying the impact.

After the UK Treasury's legislation to allow the PSR to require victim reimbursement for APP scams came into effect with the Financial Services and Markets Bill receiving Royal Assent in June 2023, it was revealed to the industry how this mandatory reimbursement would work in practice, with the publishing of the legal instruments by the PSR in December 2023. This includes:

- new Faster Payments rules, the system in which the vast majority of APP fraud currently takes place;
- all payment firms incentivised to take action, with both sending and receiving firms splitting the reimbursement costs 50:50;

- customers more protected under consistent minimum standards, with most APP fraud victims being reimbursed within five business days and additional protections given to vulnerable customers; and
- clearer guidance and the ability to apply a claim excess and maximum level of reimbursement.

The PSR stated that these requirements will be implemented as quickly as possible, but advised banks to continue to develop their fraud detection and prevention strategies and ensure they are able to respond to ongoing risk of fraud. Alongside this, the widespread rollout of Confirmation of Payee (CoP) – where the sending bank checks the beneficiary account name against the account number.

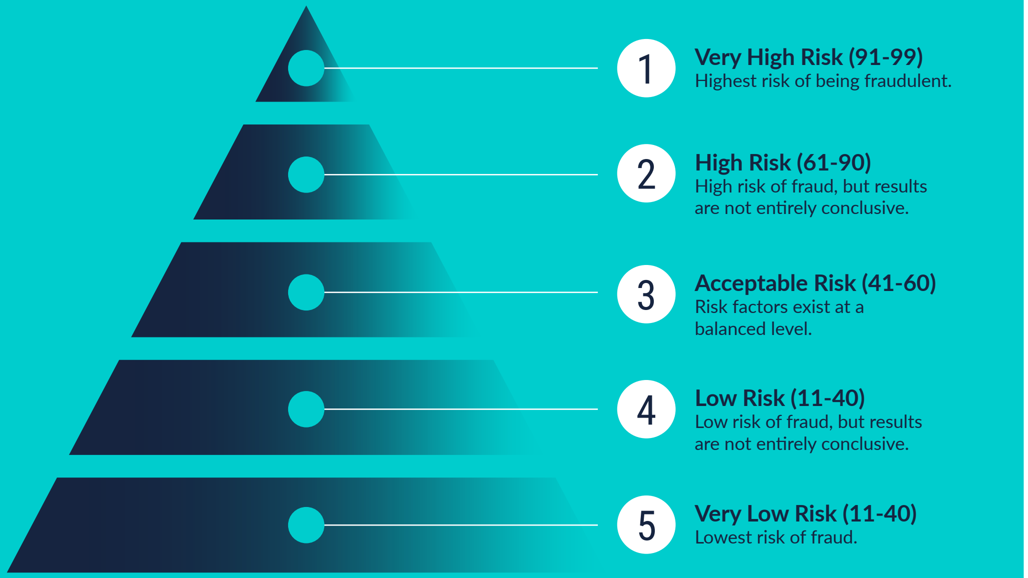
How to risk score payments effectively

Risk scoring assesses the level of risk associated with a particular transaction or user. A scoring model assigns values to different elements of a transaction. Points are added or subtracted according to predetermined features, such as if the payee is new or it is a larger amount for a single transaction in comparison to the payer's normal transactions. When a final score is calculated, it helps to quantify the risk that a transaction presents.

Fraud scoring is helpful for cases that are not clearly fraudulent, and not clearly legitimate, and the score will be weighed against other indicators. By looking at a transaction holistically, a bank can determine whether the payment is genuine or not. However, fraud scoring deciphers the transaction more closely and can generate a score that is based on factors that are not obvious, exposing fraud that may have not been otherwise noticed.

Typical Fraud Scoring Model

Transactions are assigned a score based on a calculation of risk factors.



1 **Very High Risk (91-99)**
Highest risk of being fraudulent.

2 **High Risk (61-90)**
High risk of fraud, but results are not entirely conclusive.

3 **Acceptable Risk (41-60)**
Risk factors exist at a balanced level.

4 **Low Risk (11-40)**
Low risk of fraud, but results are not entirely conclusive.

5 **Very Low Risk (11-40)**
Lowest risk of fraud.

Historically, risk scoring has been reliant on manual rule-based systems, but with advancements across artificial intelligence (AI), organisations are starting to leverage this technology and utilise fraud detection APIs to automate and streamline the process.

Fraud detection APIs use algorithms and data analysis to assign a fraud score to each transaction, indicating the likelihood of fraudulent activity. When integrating with systems such as payment gateways, these APIs can process transaction data in real-time and provide risk scores instantaneously.

Banks can then use these insights to make informed decisions about approving, declining, or reviewing transactions, while at the same time, protecting customer information and decreasing the risk of financial losses. Risk scoring APIs take this a step further and can analyse a wide range of data points, including user behaviour, device information, as well as transaction history.

Integrating APIs into existing systems automates fraud detection, which in turn, improves efficiency and allows businesses to handle larger volumes of transactions without compromising on security. Risk scoring also allows banks the flexibility to dictate their own thresholds for fraud, making sure that their systems align with the risk tolerance of the business.

However, challenges persist. As with any new protocol, banks require the technical expertise needed to coordinate the new with the old systems and keep up with continuous monitoring and updates. Fraudsters continuously adapt their tactics; therefore, banks must also regularly update and monitor their fraud detection systems. After all, no technology is foolproof and false positives are still possible.

03 | Consider false positive rate

Why consider false positive rate?

APP fraud continues to be a challenge to mitigate. Banks have upgraded systems so that they prevent and detect criminal activity such as account takeover that is associated with transactions leaving bank accounts. Know-your-customer (KYC) and digital biometrics do prevent anyone who wasn't the account holder from accessing accounts, but there has been a lack of focus on the bank account receiving the payment.

This is the key to preventing APP fraud. By considering the bank account receiving the payment, rather than the one sending the money, a bank can then differentiate between the true account holder and the criminal – the latter being the receiver, rather than the sender. With the UK losing £2,300 per minute to fraud, according to UK Finance, banks are forced to decide whether they must investigate a case – at a significant expense, or consider it a false positive, and on top of that, now be forced to remunerate the victims.

Further, in a policy update from the PSR in 2022, the regulator announced that the "industry needs to do more to prevent APP scams. This includes identifying potentially fraudulent payments before they are sent and preventing fraudsters receiving payments in UK bank accounts. We think that the Faster Payments ecosystem as a whole – Pay.UK and PSPs – needs to work together to prevent harm to consumers who use the payment system."

What this means is that banks will need to invest in solutions that better identify APP fraud and address that liability has shifted from the customer and onto them. Fraudulent transactions that are of small value add another layer of complexity to a bank's decision of whether to intervene with every instance of theft. Despite the obstacles that operational cost may present, the cost of customer experience must also be considered, which can be jeopardised by failed payments and false positives.

How to consider false positive rate effectively

False positives are when legitimate transactions are alerted by fraud prevention systems, due to having similar characteristics to fraudulent ones - for example high value, new payee, or increased frequency of payments. False positive rates are very specific to a sector, type of product, or even to a particular bank, because every bank will have a unique or different level of risk appetite and profile of customer. False positives also result in a poor customer experience, adding friction and payment verification to a legitimate payment.

Rule-based decision systems can help banks detect and prevent fraud, identify anomalies, and group risk factors, but are not the best at reducing false positives because of the nuances involved. If rules are oversimplified or incorrect, far too many alerts would be raised and in turn, investigation teams would become overwhelmed.

Instead, banks need automated systems that run on machine learning (ML) models to reduce overall costs and improve false positive rates. ML models leverage data to allow more non-fraudulent transactions through without friction while stopping more fraudulent transactions. Data accuracy and adequate analysis is also of paramount importance when deploying a solution to reduce false positives – an aspect of fraud prevention that banks often overlook.

While data matching can help reduce false positives, a lack of data validation in existing systems severely restricts what can be achieved. The flow of data must be considered, particularly as financial institutions often have legacy or third-party systems performing checks and already identified, problematic applications are fed back into fraud systems. This can create unnecessary false positives that impact the transaction approval and customer experience.

On the other hand, considering the flow of data and how data matching or rule-based decision systems fit within a bank's processes can often yield a reduction in false positives, cutting investigation cost and time down significantly. Sharing information about known risks and accessing intelligence databases that are populated by trusted industry partners can also refine investigative processes and score the level of risk a transaction poses much more accurately.

A bank being part of a consortium dataset also allows customers to trust in that the institution is doing all it can to protect itself from fraud. Predictive analytics techniques such as data modelling systems are the next step, but the cost of deployment into a real-world business environment is high because of the speed of change required within the organisation. Although, as the cost of migrating applications to cloud has reduced, the opportunity for evolving software, recalibrating data models and deploying change is vast.

04 | Implement the right intelligence

Why implement the right intelligence?

To prepare for the PSR's incoming rules, banks must consider several different eventualities. They must think about the type of partner they want to collaborate with and the solution they will need to meet the demand of screening inbound payments. Another hurdle to address is how to operationally process all fraud alerts that are generated. Leveraging data is also emerging as a key step in effectively tackling APP fraud as well as enabling the creation of intelligent models that enhance the accuracy of fraud detection. With the new regulation being implemented in October 2024, swift action will be the catalyst to mitigate risk, customer experience issues, and rising costs. By embracing these changes, banks can proactively adapt to evolving threats, reinforce customer trust, and navigate the changing regulatory landscape into the future. To facilitate this evolution, banks are turning to ML.

A subset of AI, ML can mobilise large datasets and advanced algorithms, identify patterns and anomalies that indicate fraudulent behaviour, and make it possible for businesses to detect and prevent fraud in real time. There are three main types of ML:

1. **Supervised learning:** where the computer algorithm is given a dataset with both the input data (problems) and the correct output (answers). The algorithm studies this dataset and learns the relationship between the input and output. Eventually, the algorithm can make predictions or decisions for new data that it has not seen before.
2. **Unsupervised learning:** where the computer algorithm is given a dataset with only input data, without any corresponding correct outputs (answers). The algorithm's job is to analyse this data and discover underlying patterns.

3. **Reinforcement learning:** where the computer algorithm, often called an agent, explores an environment and makes decisions. For each decision, it receives feedback as either a reward or a penalty. The algorithm aims to learn the best strategy to make decisions that maximise its cumulative rewards over time. It does this through trial and error, improving its strategy based on feedback.

How to implement the right intelligence effectively

ML can be used by banks for fraud detection and prevention due to its ability to analyse large amounts of data, identify patterns and adapt to new information – it is the right form of artificial intelligence to use. In addition to risk scoring, as previously discussed, ML can be used in the following ways to mitigate fraud risk:

- **Anomaly detection** – identify unusual patterns or deviations from normal behaviour in transactional data.
- **Network analysis** – techniques like graph analysis, can help analyse relationships between users, accounts, or devices and identify unusual connections or clusters.
- **Text analysis** – analyse unstructured text data, such as emails, social media posts or customer reviews, to identify patterns that may indicate fraud.
- **Identity verification** – verify user-provided information, such as images of identification documents or facial recognition data, to ensure that an individual is who they claim to be.
- **Adaptive learning** – retrain on new data, allowing models to stay better equipped to detect emerging fraud patterns.

Banks have already started expanding and evolving to include diverse data to understand trends, emerging technologies to manage market disruption, but now financial institutions are liable for reimbursing fraud victims, not having a robust fraud strategy is no longer tenable.

05 | Embed intelligence into the strategy

Why embed intelligence into the strategy?

Now that the PSR has legislated that APP fraud victims must get their money back within five working days, a strategic intelligence management strategy is essential for fostering innovation within a bank. Banks and PSPs will be incentivised to take responsibility, with both sending and receiving firms splitting the costs of this reimbursement, but as discussed, more will need to be done to prevent fraud in the first instance. Potential reimbursements, false positives and a growing number of sophisticated fraud attempts must be factored into a bank's overall objectives and innovation goals.

How to embed intelligence into the strategy

Because fraudsters are increasingly becoming sophisticated and leveraging different forms of AI to formulate attack strategies, banks must also use AI to establish a real-time automated information flow to continuously gather insights and develop innovative ideas. Through automation, AI can update innovators with new ideas instantaneously, which can be used to build business cases.

5 steps to develop an effective innovation ecosystem:

1. Align strategic intelligence management strategy with your bank's overall innovation goals.

2. Integrate strategic intelligence management into your existing innovation management system.

3. Implement strategic intelligence tools to support innovation activities and initiatives.

4. Evaluate the benefits and challenges of integrating AI into strategic intelligence management efforts.

5. Continuously monitor, assess and adapt your strategic intelligence management strategy to ensure its ongoing effectiveness.

06 | Ensure explainability

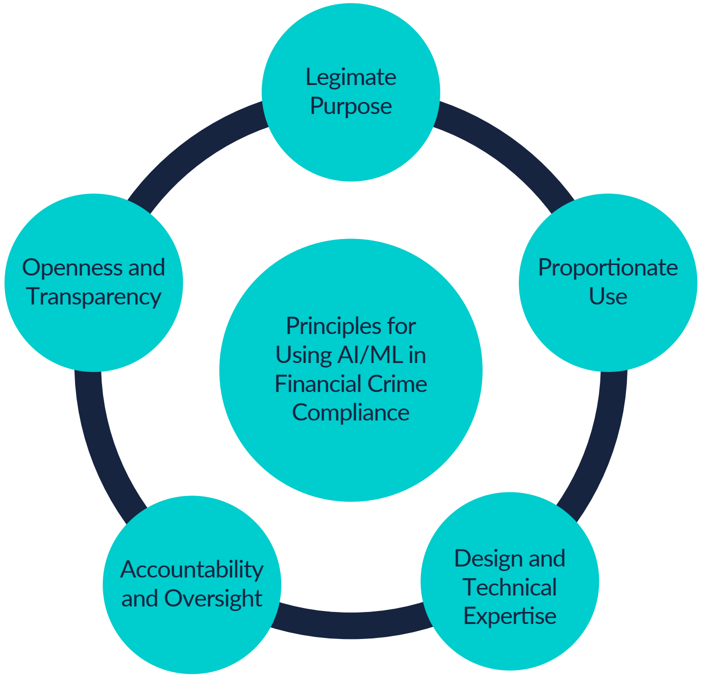
Why ensure explainability?

It is evident that AI and ML can support bank fraud teams maximise their efficiency in a cost-effective manner and respond to criminal threats with automated speed and accuracy, all the while communicating with their customers. Banks are currently using AI to set fraud transaction monitoring thresholds based on an analysis of risk data. This means that when a customer breaches said threshold, ML may be able to decide whether to trigger a fraud alert based on what is known about the customer's profile or financial situation.

Alongside this, ML can help banks detect groups of customers that may be at a higher risk of being the victims or perpetrators of fraud, as well as reveal fraud in adverse media searches using natural language processing (NLP). With alert prioritisation, higher-risk alerts can also rise to the top of the review backlog, reducing time wasted on false positives.

Once the ML models have completed their tasks, it is then the responsibility of human analysts to perform deeper investigations and decide whether to act. In 2022, the Wolfsberg Group shared best practices to ensure AI and ML are used responsibly in managing financial crime risk.

Each system relying on AI should demonstrate:


Legimate Purpose
Proportionate Use
Design and Technical Expertise
Accountability and Oversight
Openness and Transparency
Principles for Using AI/ML in Financial Crime Compliance

How to ensure explainability

To meet the five Wolfsberg Group best practices, banks must ensure explainability is a part of their chosen AI risk management solution. This helps avoid using an AI system's decisions without understanding why it made them. Explainability is essential for enabling trust and ensuring responsible use of technologies, and as per the FATF's definition, explainability can be defined as solutions or systems that are "capable of being explained, understood, and accounted for."

Beyond the expectations and requirements of regulators, ensuring explainability can also ensure that a bank's processes are continually assessed, effectiveness and fairness are improved, and unforeseen problems like algorithmic bias are mitigated. One way in which to ensure AI decision explainability is to use an 'ensemble method' – which is essentially combining multiple models to improve the desired results.

According to the Corporate Finance Institute, "ensemble methods are techniques that aim at improving the accuracy of results in models by combining multiple models instead of using a single model. The combined models increase the accuracy of the results significantly. This has boosted the popularity of ensemble methods in machine learning." By implementing ensemble methods, predictability in models can be improved as several models are combined to make one very reliable model. These methods are ideal for regression and classification, where bias is reduced, and variance is boosted to improve the accuracy of the models.

Ensemble models can bolster the explainability of an AI or ML-based fraud prevention solution, but this must be used as a tool to supplement human expertise. With banks being liable for reimbursing fraud victims, a human's responsibilities have only increased; humans can still be held legally responsible for AI-informed decisions and should correct errors that conflict with human rights.

When choosing a fraud prevention solution, banks must weigh up the benefits of building in-house or outsourcing to a technology vendor. However, with the rise in AI and ML sophistication, banks may want to consider solutions that help automate their fraud compliance processes. For banks that have established in-house systems but need to upgrade with minimal upheaval ahead of the PSR's liability standards coming into force, hybrid systems can also be an effective solution.

In this case, purpose-built AI solutions can overlay an existing system, enhancing it without requiring a total overhaul. Since PBAI uses an ensemble model, it is explainable and can thus be a cost and a risk-effective way for firms to upgrade legacy systems.

07 | Conclusion

Customer experience is at the heart of putting an APP fraud liability strategy in place within a bank. While managing the experience of those suspected of being victims of fraud, a bank must also introduce a minimal amount of friction to prevent fraudulent transactions from taking place.

It isn't just about how a bank communicates with their customers, it's about potentially looking at different strategies that can sit alongside explainability that can help optimise customer experience in a way that is reflective of the challenges they are currently facing.

Customer intervention leads to customer noise, and unfortunately, customer attrition. That is the risk involved in managing the payments journey, rather than facilitating the flow of funds. For banks, the time to act is now.

About

Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to www.finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers.

The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:

Visit **www.finextra.com** and become a member,
follow **@finextra** or reach us via **contact@finextra.com**.

Form3

Revolutionising financial crime detection.

Our APP Fraud Prevention solution enables real-time inbound and outbound intelligence (score and explainability) to drive both enhanced fraud detection and lower customer interventions for genuine transactions. This is crucial as with APP fraud it is not about who sends the payment, but who receives it.

Elevate your fraud prevention technology with the use of 'consortium intelligence' to identify and prevent financial crime and take back control from the fraudsters.

Find out more: **www.form3.tech/additional-services/fraud**

For more information

Finextra Research
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Follow
@finextra

Web
www.finextra.com