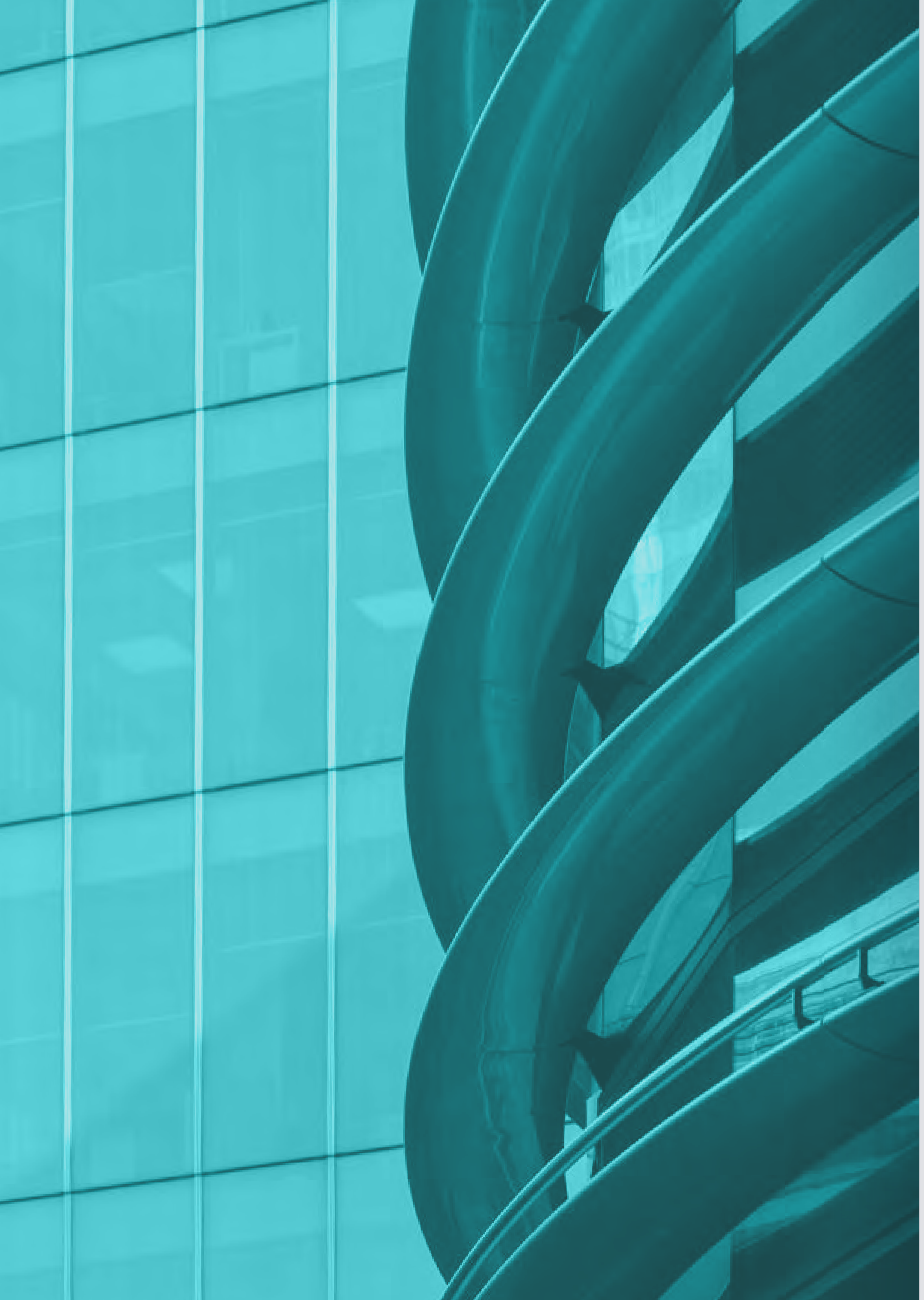
feedzai | FORM3

Combatting APP fraud

How to build a best-in-class fraud prevention solution

Collaborative Whitepaper

June 2024



Executive summary

Managing fraud risk is an ongoing challenge, with fraudsters continually advancing their techniques. Authorised Push Payment (APP) fraud, where victims are deceived into making payments to fraudsters, has emerged as a significant threat. In response, the UK Payment Systems Regulator (PSR) will introduce new rules in October 2024, requiring banks involved in fraudulent transactions to reimburse defrauded customers on a 50:50 basis.

To comply, banks must monitor both outbound and inbound payments for fraud risks. This necessitates not merely upgrading existing systems but adopting best-in-class fraud prevention methods, including collaborative intelligence. Such an approach involves analysing behaviour patterns across multiple institutions, rather than within a single bank.

While these regulations pose challenges, they also present an opportunity to enhance the protection of the financial system. By utilising network-level data, embracing collaboration, and implementing real-time risk scoring and machine learning, banks can significantly improve their fraud detection accuracy. This holistic strategy allows banks to identify and prevent fraudulent activities more effectively, ensuring they meet regulatory requirements and better safeguard their customers.

The shift towards collaborative intelligence and advanced technology will enable banks to adapt to evolving threats and reduce financial losses, ultimately leading to a more secure and resilient financial ecosystem.

Evolution of the fraud landscape

Managing fraud risk is an ongoing challenge, with fraudsters continuing to evolve their technology and techniques. In particular, the risk of Authorised Push Payment (APP) fraud – in which victims are tricked into voluntarily making payments to fraudsters – has become increasingly significant in recent years.

Understanding APP fraud

One notable development is the rise of Authorised Push Payment (APP) fraud, whereby victims are tricked into sending money to fraudsters through techniques such as impersonation. In some cases, the account receiving the payment will be the account of a mule who may or may not be aware that they are involved in illegal activity.

According to figures from UK Finance, losses from APP fraud were more than £460 million in 2023, with the most significant types of APP fraud including purchase scams and romance scams:

In a **romance scam**, the victim is tricked into believing they are in a relationship with the fraudster, with subsequent demands for payments – common scenarios include health issues and difficulties in obtaining a visa. Notably, romance scams can lead to significant emotional harm as well as financial loss.

In a **purchase scam**, the victim sends a payment for goods or services that they never receive, such as a holiday rental or car.

While UK Finance data shows that overall losses from APP fraud were lower in 2023 than in the previous year, purchase scams had increased by 34%, while romance scams were up by 17%. Unlike purchase scams, victims of romance scams make an average of 10 payments to the scammer, reflecting the persistent nature of this type of scam.

The PSR's new APP fraud rules

At present, many victims of APP fraud are not reimbursed for their losses: according to UK Finance, the reimbursement rate was 65% for purchase scams, and 63% for romance scams in 2023. As such, efforts are underway to mitigate the risk of APP fraud at the industry level, and to reimburse more victims for their losses.

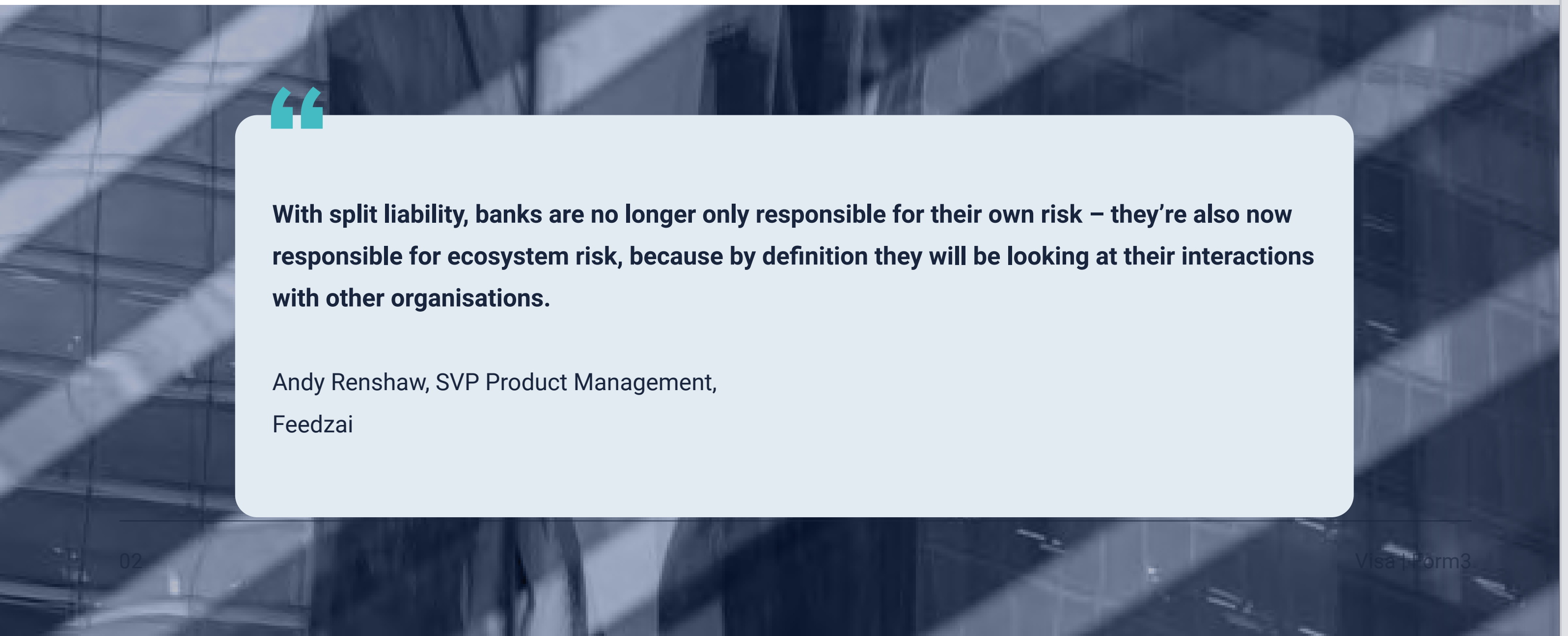
Last year, the UK Payment Systems Regulator (PSR) confirmed that new rules would be introduced in order to prevent APP fraud, and also ensure that more people get their money back if they fall victim to a scam. The final rules are due to be published by 7th June 2024, but key elements include the following:

Most APP fraud victims will need to be reimbursed within five business days, with the maximum level of mandatory reimbursement set at £415,000.

Significantly, sending and receiving firms will both need to shoulder the cost of reimbursing fraud victims, with costs shared on a 50:50 basis.

In order to be eligible, consumers will need to meet the requirements of the consumer standard of caution, which includes reporting scams promptly to their payment service provider and responding to reasonable requests for information. (The consumer standard of caution does not apply to consumers who are identified as vulnerable.)

The new requirements are due to come into force on 7 October 2024, and will apply to any reimbursable scam payments made on or after that date. In order to comply with the new rules, banks will need to take a proactive approach to preventing APP fraud.



With split liability, banks are no longer only responsible for their own risk – they're also now responsible for ecosystem risk, because by definition they will be looking at their interactions with other organisations.

Andy Renshaw, SVP Product Management,
Feedzai

The trouble with current fraud technology stacks

The new rules will drive a greater focus on where banks are sending money, and what their responsibilities are regarding fraud prevention and reimbursement. Banks will therefore need to use the technology available to identify payments that are likely to be fraudulent. And the best way to do this is by looking for patterns of behaviour in accounts and transactions that match previously known criminal behaviour.

However, this can be challenging for a number of reasons:

The need for rapid decisions

With volumes of real-time payments continuing to rise, there is less time for banks to investigate suspicious payments, as criminals can quickly exit fraudulent monies from their accounts. In a real-time world, decisions about fraud also need to be made in real-time.

Information on past behaviour is limited

Another challenge is that banks' existing technology stacks are very much geared to just one leg of the payment. In other words, they only have access to past behaviour in relation to their own accounts and transactions.

A bank sending a payment from a customer's account will have plenty of information about the customer that is making the payment, but little knowledge about the account that the payment is going to. Effectively this is limited to any other payments the bank has previously made to the same account.

False positives lead to customer frustration

Without a clear view of the risk of both sides of a transaction, the ability of banks to identify fraud is limited. There is also a risk that banks will stop a lot of genuine payments, which leads to frustration for customers. If someone wants to send a payment to a friend for a meal they've just shared, they want that payment to be secure – but equally, they want the money to clear instantly, not in three hours' time.

Think of it like a jigsaw. If you only have the pieces for the left side of a jigsaw, you might think you're building a picture of a beach – but actually there could be a great white shark coming in on the right side that you are completely blind to.

Chris Oakley, Head of Fraud
Form3

Harnessing the power of data

These issues can't be addressed simply by enhancing current solutions. A new approach is needed that enables banks to make their investigations as targeted as possible, while supporting customers in the least invasive way they can.

To do this, banks need to unlock insights that they are not currently able to access. Arguably, the last big change in banks' infrastructures was driven by the arrival of real-time payments and digital banking in the mid-2000s. The focus at the time was not on data sharing, but on maximising the insights that could be gleaned from on-premises local data.

Over time, banks have realised that operating only within their own estates doesn't necessarily maximise value. But when it comes to sharing data, banks need to balance two competing factors: certainty and timeliness.

Any situation in which data can only be shared if instances of fraud have already been labelled typically requires a high burden of proof. And by the time that burden of proof has been met, and the institution is willing to share the data with other organisations, it's likely that the fraudsters will be long gone. There is also a risk that if transactions are mislabelled as fraud, individuals or businesses could ultimately end up being debanked by multiple institutions.

How, then, can banks tap into the wealth of information held within the financial system in order to assess the risk of fraud more accurately, in a way that is not materially damaging to the customer or organisation?

> **Think of it like a jigsaw. If you only have the pieces for the left side of a jigsaw, you might think you're building a picture of a beach – but actually there could be a great white shark coming in on the right side that you are completely blind to.**
>
> Chris Oakley, Head of Fraud
> Form3

The new approach to fraud prevention

In order to identify instances of fraud more accurately, banks need to increase the accuracy of alerts without requiring additional resources or increasing friction for customers. This means adopting a new approach to fraud prevention that leverages network-level collaborative payment data. Crucially, this needs to be done in a way that does not adversely affect consumers and businesses.

feedzai | FORM3

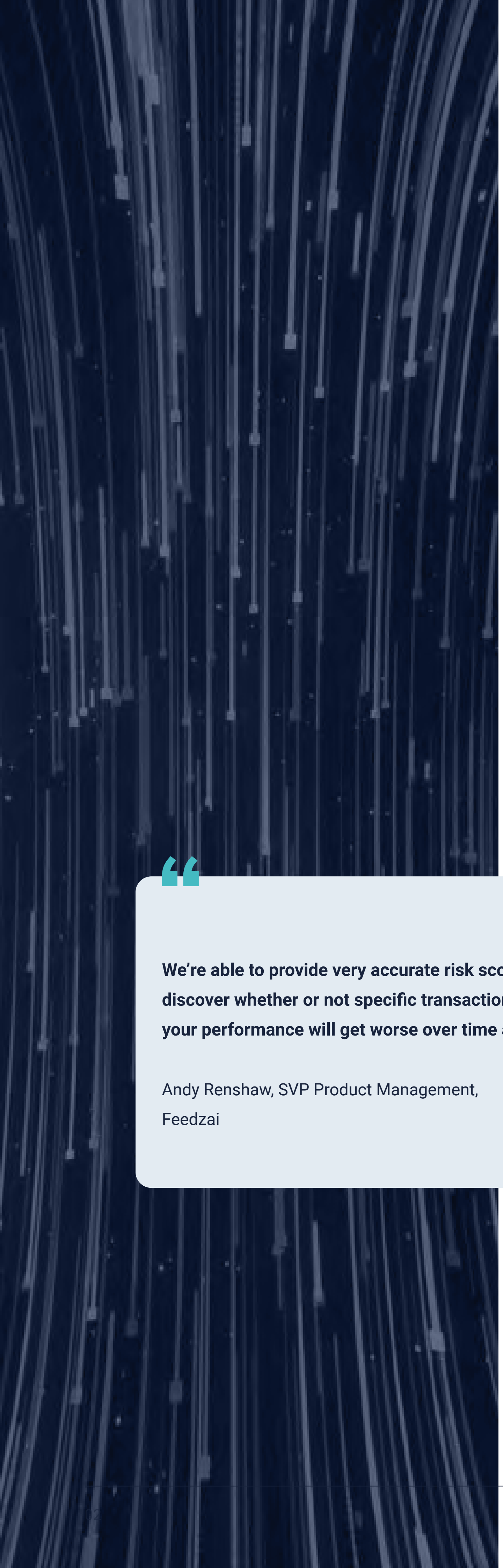
Why collaborative intelligence?

To achieve the step change that is required, the industry needs to tap into what we call collaborative data – in other words, intelligence that is sourced from a network, rather than from a single institution. Using a wider pool of data, banks can spot developing trends and risk actors that are operating across multiple institutions.

In practice, identifying criminal behaviours tends to be hardest for tier three banks which have the smallest amount of transaction data available to build pattern behaviour. Smaller banks also tend to have some of the highest thresholds for risk as they are more focused on growing their customer base. However, a collaborative approach that harnesses network level data can make the whole system safer and benefit all parties, including those that operate with a higher risk threshold.

As Nick Fleetwood, Head of Data Services at Form3, explains, "If one bank is looking at the risk associated with sending a payment, and the bank that receives the payment is looking at the risk of receiving it, it's possible that neither threshold may be high enough to warrant intervention. But if the account that received the inbound payment instantly sets up an outbound payment for the same amount, that could be a red flag."

> **If you could put together all the operations teams that are working in every financial institution, you could then harness the output of those combined workforces and all the transactions they're interacting with. That's a really powerful proposition.**
>
> Nick Fleetwood, Head of Product - Data
> Form3



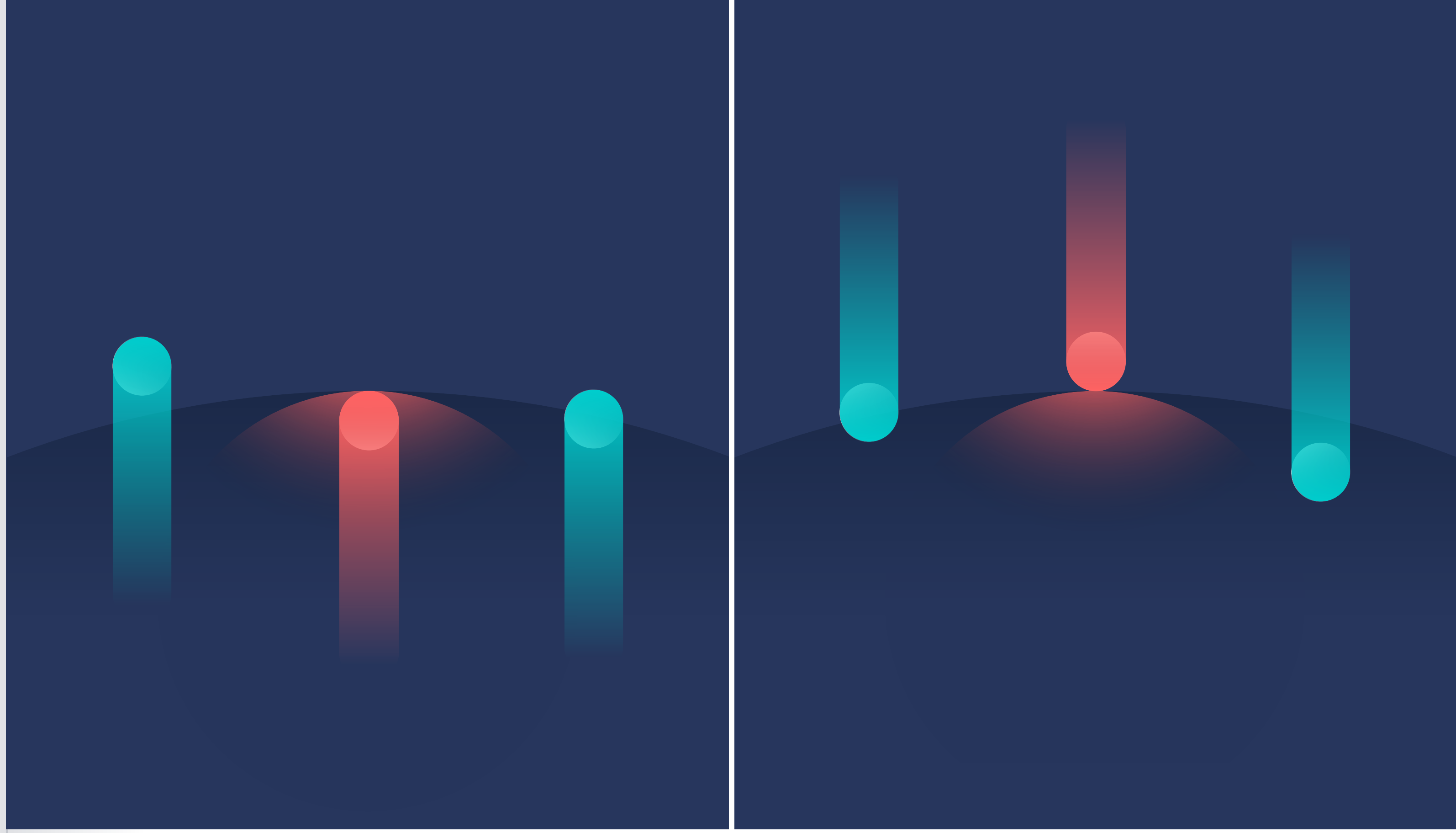
Risk scoring and machine learning

Banks can use collaborative intelligence to apply a risk score to individual payments. With a clearer view of the risk associated with a specific payment, banks can then decide whether or not to intervene.

As outlined previously, fraud labels can have an adverse effect on customers if they are used or interpreted inaccurately. A more effective approach is to design a system which uses labelling and risk-based scores in a balanced way alongside other risk indicators, rather than regarding it as a definitive way to make a decision.

In today's market, fraudulent behaviour can change quickly as fraudsters adapt and as consumer habits evolve. Banks, likewise, need to have the agility to update their processes quickly, which is where machine learning comes in. A system that uses machine learning to adapt as more information becomes available will be better placed to improve its performance over time.

> **We're able to provide very accurate risk scores – and we're able to adapt and learn as we discover whether or not specific transactions really were fraudulent. If you don't keep moving, your performance will get worse over time as fraudsters adapt to existing processes.**
>
> Andy Renshaw, SVP Product Management,
> Feedzai



Inbound and outbound monitoring

A best-in-class fraud prevention solution also needs to harness both inbound and outbound monitoring. Under the new rules, a payment that receives funds from an APP fraud will be liable to reimburse 50% of the payment to the customer – which means that banks need to start thinking about monitoring their inbound payments in a more intelligent way.

Historically, banks' fraud prevention efforts have focused almost entirely on outbound monitoring. There are good reasons for this: prior to the rise of APP fraud, the main threat was account takeover, which has been mitigated over time by measures to ensure that the person making a payment really is the person who owns the account in question.

APP fraud is different, because the person sending the payment is not the criminal, but the victim of the scam. Inbound monitoring can identify suspicious payments by looking at the account receiving the payment and identifying transactions which might differ from payments usually received by that account. The bank receiving funds will therefore be better placed to stop transactions before money is received in the account.

Even more powerful is the ability to monitor both inbound and outbound payments at the same time. By combining both types of monitoring, banks will be better placed to identify suspicious activity, highlight discrepancies between inbound and outbound flows, and mitigate losses. And crucially, banks will be able to achieve more operationally without increasing the number of people working on alerts.

Holistic view of fraud

“What banks have to think about is how they merge their inbound and outbound strategies together,” comments Chris Oakley, Head of Fraud at Form3. “What you can then do is understand the risk of an inbound payment, but mitigate it on the subsequent outbound payment, because you only crystallise a liability position when those funds leave your organisation.”

For example, if A sends a payment to B as the result of an APP scam, B’s bank can prevent cash from leaving B’s account, meaning that A’s money is protected and neither bank has to shoulder the cost of reimbursement. This can be applied regardless of whether the fraudster plans to move the cash using an account-to-account payment or a physical card.

“You have to start bringing all that together into a holistic solution,” says Oakley. “If you’ve got a card payment going out, you ought to be checking whether a high-risk inbound payment has come in within a certain period of time. What you then have is a transaction-centric solution, rather than a solution that is focusing on a specific channel.”

He adds that real-time risk scoring is a crucial part of this because of the speed at which fraudsters move money. The reality is that when a fraudster receives a payment from a victim, they immediately drain the account. But banks don’t want to slow down payments – so to protect their customers, they need to be able to prevent fraud in real-time. And that requires real-time decisions.

Our APP Fraud Solution

By using technology like Form3’s APP Fraud Solution powered by Feedzai, banks can effectively monitor the developing picture of fraud risk.

Built using fully supervised machine learning, the solution combines Form3’s account-to-account payment processing with Feedzai’s fraud and financial crime analytics. The product uses collaborative intelligence to understand the behaviour of both the person sending the money and the person receiving it. This is used to determine the risk of the payment being made in real-time.

The solution is able to identify over 97% of all fraudulent activity when both institutions are within the consortium developed by Form3, and provide accurate labels. At the same time, the solution can reduce false positives by over 25%, reducing friction on non-fraudulent payments.

As a result, banks can operationally improve the effort needed to identify fraudulent payments, and spend more time working with genuine victims to help them understand that they are the victim of a scam, and prevent the fraudulent payment from taking place.

Here are some of the benefits:

- Best-in-class detection rates through enriched intelligence
- Single API for connectivity
- Significant reduction in fraud losses
- Ease of adoption using existing FPS Payment Message and Fraud labels
- Improved customer experience with less friction on non-fraud payments

Learn more →

Reaping the rewards of a best-in-class approach

To understand the benefits of this approach to fraud detection, banks need to consider three different levers and how they interact, namely financial loss, customer experience, and operational capacity.

When banks aim to catch more instances of fraud, they will also need to get in the way of more non-fraudulent activity. To reduce financial loss, for example, a bank might aim to increase the number of alerts it receives. This, in turn, will mean that more people need to work on those alerts. It will also lead to an increase in the bank's false positive rate, meaning that more customers are negatively affected by fraud investigations.

What banks really need is to achieve better intelligence about their payments, while becoming more efficient with their operational resources and reducing the friction customers experience as a result of false positives. If banks can be smarter about which alerts people need to work on, they can drive improvements across all three of these areas.

This is only made possible by harnessing collaborative intelligence to gain a clearer understanding of customer behaviour in real-time and assess the risk of individual payments more effectively. By adopting this approach, institutions will be better placed to increase the amount of fraud detected, reduce false positives and improve their customer experience.

Deprogramming victims of fraud

It takes time to deprogram the victim of an APP scam from the programming they've gone through to make a payment to a criminal. In the case of a romance scam, the victim believes they have built a relationship with the person they're sending money to. And in a purchase scam, the victim is motivated to buy a particular item at what they believe is a favourable price.

Banks need to spend time working with victims in order to help them recognise that they are the victim of a scam, and to prevent the fraud from taking place – a process which also includes an element of victim support. It's therefore crucial to create time for operational teams to be able to work those alerts, confident that they've correctly identified an instance of fraud.

How banks can be ready for the new regulations

The new regulations will come into effect in October 2024. While the regulation makes it clear how banks will need to reimburse their customers, it doesn't stipulate which steps banks will need to take to protect themselves. But that doesn't mean that doing nothing is a viable option. Indeed, it's likely that regulators will closely monitor the approach banks take to managing fraud risk and driving a culture of continual improvement.

> “
>
> **If you haven't started engaging with your C-suite and board approvals, you need to change how you're doing things. In my opinion, the status quo is not going to be an acceptable position for the regulator in light of the new regulations.**
>
> Chris Oakley, Head of Fraud
> Form3

As such, banks will need to focus on technical enhancements to their existing fraud strategies so that they can identify new intelligence points that they aren't currently accessing.

To achieve this, banks should:

01

Use collaborative intelligence solutions as part of the intelligence they use to identify risk.

02

Ensure their operational teams understand the nature of the risk score and how it can help them manage their customer interactions.

03

Develop inbound screening and introduce a volume of alerts that is focused on inbound screening.

Achieving this may be challenging with legacy systems which are not equipped to screen and alert for inbound payments. As such, banks will need to look at how they achieve this architecturally. They will also need to consider how different scenarios will be managed, and how institutions will take decisions in line with their responsibilities.

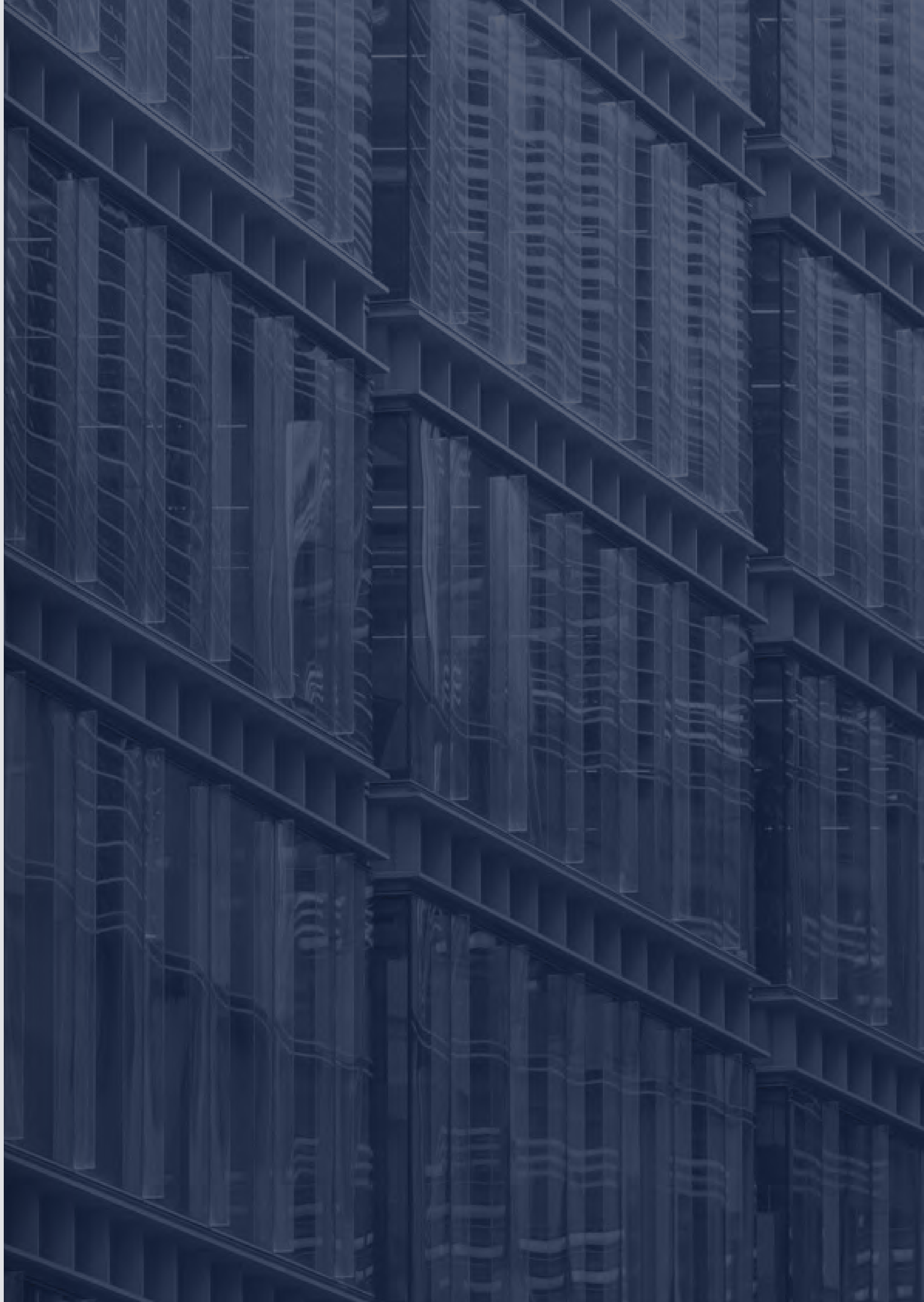
Embracing the underlying intent

Last but not least, banks should also be looking at the new regulation as a positive change, rather than yet more red tape. While effort will be needed to comply with the rules, this is an opportunity for banks to create better outcomes for their customers and for their staff.

The key to success lies not just in adhering to the regulations, but also in embracing the underlying intent. Cooperation between institutions is a major focus for the new rules: the 50:50 liability split for customer refunds means that both the sending and receiving banks are equally responsible for preventing fraud from taking place. As well as protecting their customers, banks will also need to focus on identifying bad actors and preventing them from operating within the financial system.

To achieve this, banks need to take a proactive approach, seek out innovative solutions and collaborate across the sector. By participating in network solutions, sharing the intelligence that has been generated by labels and being more open in terms of helping to complete investigations, banks can help to build a system in which everyone is protected.

> **I firmly believe that by adapting to these new regulations and taking a more collaborative approach, the UK can become the first market that truly takes a massive step forward in preventing fraud within its borders.**
>
> Nick Fleetwood, Head of Product - Data
> Form3



Conclusion

There's no doubt that the PSR's new APP fraud rules represent a significant shift for financial institutions.

Adapting to the new requirements will be a challenge, but by taking advantage of network-level data provided by consortium learning models, banks can access significantly more data to assess transactions for fraud risk. The use of inbound and outbound monitoring will enable banks to increase the accuracy of their fraud detection and improve their operational efficiency – all while reducing the friction experienced by customers.

Contact us →

This paper has been written by Form3 in collaboration with Feedzai

Andy Renshaw
SVP Product Management
Feedzai

Chris Oakley
Head of Fraud,
Form3

Nick Fleetwood
Head of Product – Data,
Form3