Public-Private Data Exchange for Fraud Prevention: Best Practice Recommendations

A P20 Report

October 2023

Foreword

This is the third P20 report on combating fraud and criminal transactions. This time the focus is on data, the lifeblood of this issue. This report asks key questions about critical data sets, who holds them, how they can be shared without breaching current privacy law, how we should use AI, how to improve consumer awareness, and critically, how we can collaborate more effectively?

Criminals are better organized than ever before and realize the value of consumer data to perpetrate fraud. They share data on the dark web for financial gain and are increasingly using AI to drive up their success rates. They are ruthless and operate like a successful business with margins and bottom-line profits that are huge. Most of this criminal activity operates from weak and inadequate legal jurisdictions, sometimes with tacit support from governments. Lastly, these global criminal networks rarely suffer consequences or are held to account for their crimes.

It's becoming more difficult to defeat the criminals, but the industry could do much more, if it was able to marshal all the respective data sets, and agencies were able to collaborate more across borders. Organizations could create pain points for criminals which will slow their activity down and allow organizations to create stronger capabilities against their attacks.

Data is critical in this battle and our report contains best practice actions and recommendations that would help to even up the fight against organized crime. The tensions of sharing personal data versus the benefits of greater fraud prevention and detection are well recognized but will legislators and regulators relax privacy law if it means reducing the incidence of this crime and putting more of the bad actors behind bars?

I want to thank all those who contributed their time and views for this report. They represent leading financial institutions, regulators and a global consulting firm.

I hope you find this report interesting, challenging and useful.

Duncan Sandys
CEO, P20

Recommendations

Key Data

- Agree to a common definition of fraud
- Develop and agree on a protocol and platform for the secure real time exchange of data between FIs, government agencies, law enforcement, tech companies and telcos to help identify suspected fraud
- To help combat fraud, government should issue regulatory guidance on responsible data sharing between entities and on standard data formats
- Industry should have *For Your Eyes Only* access to law enforcement Suspicious Activity Reports (SARs)

Detecting Fraud

- Government should create incentives for industries to expand and deepen AI capabilities
- Government should allow private sector access for the authentication of government data
- Government should create a kitemark for KYC companies who meet specific standards
- Develop a level of risk number that is provided to customers before a transaction occurs

Collaboration

- Create a regulator-led forum to facilitate regular dialogue with the private sector on combating fraud to foster mutual understanding and build trust
- Government should issue public service announcements (risk based interventions not generic warnings) and partner with others outside FIs to change consumer behavior
- Industry and law enforcement should collaborate to prosecute criminals
- Government and industry should work together to develop a fraud prevention protocol setting out circumstances when it is acceptable to override privacy law provisions

Martina King, CEO, Featurespace

"Using privacy enhancing technologies means we can collaborate without using personalized data and achieve comparable results on behalf of the whole payment industry."

Watch Martina's video interview here.

What types of data are critical to identifying fraud and who holds them?

Currently, the way fraud is tackled globally is using data held in multiple locations and data stores and a layered, complex system has evolved, requiring call outs to third parties. At Featurespace, we have been working to establish the least amount of data FIs need for an adaptive machine learning model to achieve optimal fraud protection. And that answer is as simple as it is effective: auth stream data only. The industry has a huge catalog of different data assets and the richest signals sit within the data the banks hold themselves, primarily the auth stream data. Knowing the behavior of existing customers and determining in real time whether a transaction is genuine is recognized as the best way to protect consumers from fraud attack.

When it comes to data sharing, many industries have been working together to compile data assets to create a holistic customer view. Real-time monitoring of both inbound and outbound payments, for instance, is a good example where banks would like to share their data amongst themselves. However, data can't be shared because of privacy laws, as upholding an individual's fundamental right to privacy is as important as protecting assets from financial crime. So, what can the industry do to overcome that problem? We know when working in these collaborative environments that managing the legal issues of data sharing can be hugely time consuming. At Featurespace, we have pushed the boundaries to create a technical solution as an alternative to sharing personally identifiable information. And this is a really exciting thesis: is it possible to teach a machine to provide an answer based on an approximated result that is equal to the answer you would achieve if you had access to personally identifiable data?

What does that mean for the payment industry? Well, it means we can all collaborate effectively while also protecting individual privacy. It means we can put data together and get the best possible outcome on behalf of the whole industry. It's a very exciting advancement that holds the possibility of changing the landscape of the data industry dramatically because if you don't need vast amounts of data and the data doesn't need to contain personally identifiable markers, it is a very transformative moment.

At the second Summit for Democracy, the United States and the United Kingdom announced the winners of prize challenges to drive innovation in privacy-enhancing technologies (PETs) that reinforce democratic values. Announced at the inaugural Summit for Democracy in December 2021, the prize challenges inspired innovators on both sides of the Atlantic to build solutions that enable collaborative development of artificial intelligence (AI) models, while keeping sensitive

information private. The challenges focused on developing PETs solutions for two scenarios: forecasting pandemic infection and detecting financial crime. Featurespace was selected as a winner in the financial crime scenario.

What role can AI play in detecting fraud?

It's already well proven that AI is now the best tool in our defensive armory against modern cybercriminals. What prevents its wider adoption in combating financial crime and fraud is that it's complex to deploy adaptive models, requires a high level of expertise to manage, and banks don't necessarily have the experts in house or find it daunting to address the layers of fraud protection already in place. And so, fraud losses just increase. So, it's vital as an industry that we make it simpler for companies to purchase and install technology that protects their consumers.

Enterprise AI systems take time to integrate into existing data sets and systems, and we're delighted that we are able to speed up integration so business value is dramatically brought forward. What do I mean by that? Cloud is a big enabler. Our tried and tested enterprise scams product can be shrink wrapped into a very simple, straightforward solution via a templated data schema so that a payment call immediately returns a score without the need for lengthy integration. The result: the industry is protected far faster as many barriers to adopting new technologies are removed.

Should a financial institution be able to refuse to act on the payment instructions of a customer if fraud is suspected?

Yes, they should be able to refuse to enable a payment where fraud has been identified. However, the signals can be challenging to interpret as often the victim is blindsided or manipulated by the criminal, and convinced the transaction they are making is genuine, approving the movement of money – the victim can be an unwitting accomplice. Adaptive machine learning models can cut through the complexity of these behavioral signals to identify the attack while it is taking place, enabling intervention to protect the consumer from the attack by blocking the transaction in real time. Blocking the transaction and forcing a cooling off period significantly reduces losses and the illegal flow of funds.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

Education is hugely valuable despite most people being very suspicious and unwilling to provide their bank details to a stranger. However, the criminals are always identifying new ways of convincing innocent people into being an unwitting participant in their crimes and unfortunately, the losses continue to increase. A client of our merchant monitoring solution recently informed me how our correctly identified alerts have added benefit to their merchants. The alerts stop merchants taking fraudulent orders, an effective added value service. Sending an alert to a consumer with the transaction score, especially where the score identified fraud, could help the issuer, merchant and consumer.

How can the public and private sectors more effectively collaborate on combating fraud?

There's a great deal of work already going on between government agencies, law enforcement and the industry. But the biggest barrier to greater collaboration has been the problem of data sharing. It's so difficult to provide each other with the knowledge the data contains but it is inaccessible. When we can gain access, when we can enable analytics, we will then be able to discover how incredibly valuable data sharing will be. So that again is why Privacy Enhancing Technology, is the key that unlocks access to data and a new era of collaboration in our industry.

Michael Timoney, Vice President, Secure Payments, Federal Reserve Financial Services

"Education is critical to stopping fraud. We need to change consumer behavior as we are often too trusting and act too quickly."

Watch Michael's video interview here.

What types of data are critical to identifying fraud and who holds them?

Historically, transactional data was key to identifying fraud, be it type of payment, amount, date, velocity, etc. And then we looked for trends in the data. While we still need that type of information, today we use non-monetary data elements, such as the device type being used, IP address, user location, what apps they have on their device and even how they use it, including what buttons they press. And so, the behaviors that are exhibited can now be analyzed in conjunction with the transactional data to better identify fraud attempts.

Many different organizations have this type of information. Financial institutions have visibility into their customers, the data within their accounts, how they interact with their accounts, how they make payments, who they pay, etc. But others in the payment system interact with these elements as well. There are payment processors contracted on behalf of financial institutions. Telecom companies know the type of patterns based on using a device. And social networks have information about who we are, how we interact with society etc. So, many different organizations have similar data points but can view it from a different perspective.

What role can AI play in detecting fraud?

AI already plays an important role in fraud prevention and detection as it analyzes large data sets very quickly and effectively. We can then identify anomalies within transactions that may be indicative of fraud in close to real time. AI allows us to create advanced rules and also identify relationships and patterns. So, there's a lot of benefit from using this technology, especially when we start to incorporate some of the behavioral analysis. But AI alone will not solve the fraud issue. Even with AI, we still need processes that focus on fraud and include trained individuals to work the process. Any good fraud solutioning involves a multi-layered approach, viewed holistically across the whole payment life cycle from the beginning and across the relationship.

How can data on known criminal networks be more effectively shared between financial institutions and law enforcement?

We know that criminals are sharing information to commit fraud so it would be no surprise for us to agree that sharing information about the criminals would be beneficial to stopping fraud. The challenge is to do it in a way that protects the data, complies with privacy rules and regulations, and allows the user of that data to be confident it is valid and accurate. Automation would allow

us to share some known data elements on those with confirmed criminal activity. However, these data points and the sharing methodology must be agreed to by all parties. Some countries are already implementing this. Recently, Australia announced a new platform that will give banks the ability to halt a fraudulent transaction, share the intelligence to prevent the loss, and then offer a way to streamline the return of funds. Such collaborative solutions will undoubtedly reduce fraud.

Should a financial institution be able to refuse to act on the payment instructions of a customer if fraud is suspected?

My personal opinion is yes. My rationale is that banks have the prerogative to do business or not, as they carry the risk. However, this also depends on a few factors that the bank needs to take into consideration. One is their risk appetite. They have to look at it from their perspective. The other side of that coin is the customer experience. Banks are in a tough position if they suspect it is fraud. Do they do what the customer wants or do they stop the transaction? So, personally, I do think banks should have the ability to stop a transaction after appropriate evaluation.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

Education is what consumers see today. This must continue so they understand both the threats and the negative impacts of fraud. Fraud doesn't just result in financial loss. It can also have an emotional impact. It can have a behavioral and physical impact, as well. The UK has a successful campaign, Take Five. It encourages people to stop and take five seconds before sending a payment. That's key because education alone will not stop fraud. We need to change consumer behavior as we are often too trusting and act too quickly. There's a fear of missing out on things if there's a limited time to act. We must take time to evaluate every payment decision from a more comfortable and relaxed position and not one of fear or panic.

How can the public and private sectors more effectively collaborate on combating fraud?

People should report all actual and attempted fraud so we know the true magnitude of the problem. These data points can prove very valuable. The more data elements we have, the better and more reliable the information is and the better the predictions. Sharing data will enable our models to perform better. We shall see the trends and hopefully we'll then know more about the fraudsters. There's also an opportunity for us to partner on educational campaigns to educate consumers. There are many companies doing things individually but there's an opportunity for us to partner with organizations outside financial institutions such as fintechs, social media platforms and telecom networks. Together, we broaden our reach.

Eddie Cones, Head of Corporate Security & Executive Director, Fraud Fusion, FIS

"AI enables fraud detection to use real time intelligence to keep up with the fraudsters who are working together and pivoting their criminal activity in real time."

Watch Eddie's video interview here.

What types of data are critical to identifying fraud and who holds them?

There are many types of data sets that can be used in both government and the private sector. For instance, we have transactional log-based data, we have demographic details on clients and customers, and government holds that data as well and records of known fraud, disputes and current investigations. There's a huge amount of data and actionable intelligence which can be used to combat fraud.

Does government and its agencies hold data that would help financial institutions in their fight against criminal transactions?

Most definitely government agencies currently retain actionable intelligence, which is crucial for the private sector, such as known fraud records, dispute details, ongoing financial crimes investigations and criminal capabilities on various fraud actors across the entire ecosystem. Their data is critical for the private sector to use when we can have real time access.

What role can AI play in detecting fraud?

AI plays a key role. Its pattern recognition is something that can be deployed at scale so that all activity occurring within an FI is reviewed by a well-trained critical eye. AI gives the capability to do behavioral analysis by ingesting demographic data in real time alongside other records to paint a picture of how an individual, group or entity is spending their money. AI enables fraud detection agencies to use real time intelligence, making it possible to keep up with fraudsters who are working together and pivoting their criminal activity in real time. We need AI to do the same.

It is a critical tool for protecting the ecosystem but AI can be expensive for private sector organizations too. A possible approach is to provide credits or incentives to invest in AI solutions of partners to protect the financial ecosystem. Most institutions today leverage some form of AI as best practice but may not have the resources to stand up such a complex system. So, if there's some type of capability for the government to provide incentives to the private sector to invest in more AI capabilities, the entire ecosystem's payments would be better protected.

How can data on known criminal networks be more effectively shared between financial institutions and law enforcement?

Financial institutions hold much data that can have a major impact. Law enforcement and government agencies have intelligence about organized state sponsored, even low-level criminal activity, that can help financial institutions stop losses in real time. It goes back to intelligence. This includes targeted

accounts, details on criminal capabilities, fraud schemes from inception to cash out.

But the key part is greater trust between the government and the private sector. The private sector needs to know that sharing information on financial crimes will not make them the target of an investigation. Government and their agencies need certainties from the private sector that actual intelligence investigations, live investigations, fraud scenes etc. will only be used to mitigate losses and will not be disclosed publicly. Both sides need to discuss the subpoena process to make intelligence sharing a collaborative process, rather than a time-consuming ineffective exercise which delays the mitigation. These two organizations need to pool their capabilities to accomplish one goal of mitigating fraud and putting bad actors in jail. And the only way we can do that is having both sectors coming together.

What role can government play to verify the authenticity of KYC documents?

KYC is where it all starts. There needs to be a national alignment on this because KYC is about intelligence and knowing a person's true identity. Government authenticated data is critical to confirming an individual's identity but government needs to be willing to share that data. If the government and private sector work together, this would greatly reduce the number of account takeovers, eg. fraudulent accounts that are created to support fraud schemes like unemployment and social security fraud and fraudulent merchants, which impact the entire payment ecosystem. So, KYC plays a major role in fraud mitigation.
Are there any regulator issued liability waivers that would improve collaboration between financial institutions and with regulators and law enforcement?

The answer to this is yes but it ties back to trust. Trust is important to protect information from being leaked. So yes, there should be a regulator issued liability waiver with protections for the private sector to share data in real time.

Should a financial institution be able to refuse to act on the payment instructions of a customer if fraud is suspected?

Yes, because if it's suspected that a customer is trying to engage in or be a victim of fraud, the FI should have the right to refuse the instruction, protect their infrastructure, the entire payment ecosystem and of course their customer.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

The government has real-time intelligence, as does the private sector, so better access to both ends of the intelligence is needed to work out the customer's intentions. For example, consumers should be able to see verification of who owns a targeted account when trying to send a transfer. This happens in the UK and is called Confirmation of Payee. Customers should be better educated on protecting their personal data to include identity as well as financial and have more options to implement multi-factor authentication with their payments. Being able to require a second authentication method on transactions would put a cardholder into a decision-making process and help combat fraud in real time.

Harold Paulson, Senior Vice President & Head of Fraud, Fiserv

"You need to protect your customer without disrupting them from what they're trying to do. That's the yin and the yang of fraud."

Watch Harold's video interview here.

What types of data are critical to identifying fraud and who holds them?

The successful identification of fraud is reliant on access to a large volume of relevant data that has enough depth and breadth to provide dimensionality, which can be obtained and analyzed in a timely manner. The type of data needed can vary by use case. For example, identifying transaction fraud or credit card fraud might be dependent on customer history, card information, and data from the merchant, whereas identifying account fraud may require personal information or bureau data. That said, the real key to using data to combat fraud is to leverage as much data as possible in decision making. Organizations such as financial institutions, merchants, processors, card brands and even government entities have access to large data sets that are relevant in thwarting financial fraud. These organizations are also able to share data responsibly, strengthening decision making by working collaboratively in a collective effort to minimize fraud across the ecosystem.

Does government and its agencies hold data that would help financial institutions in their fight against criminal transactions?

Yes – government agencies have access to data that they can and do share with financial institutions to prevent financial crimes. For example, in 2022, the Social Security Administration (SSA) created the fee-based eCBSV (electronic Consent Based Social Security Number Verification) Service that allows entities to match a social security number against a name. Banks and credit unions are using this because it provides needed certainty around validation of information. This is a good example of a government entity enabling other institutions to leverage data in a positive manner.

What role can AI play in detecting fraud?

Preventing and detecting fraud is about having a multi-layered approach. It's about using multiple capabilities in combination with each other, based upon the risk you are trying to manage. To that end, AI by itself isn't a silver bullet. It's helpful in fraud scoring, it's predictive and it adds more granularity to decisions – but AI needs to be used in concert with other capabilities, which also underscores the fact that AI will only be as good as the data fed into it.

AI can be adaptive, and it allows entities that may not have a high degree of sophistication to use a very powerful tool in an efficient manner. These entities can detect anomalies faster, understand them better, and identify patterns of good and bad in a more seamless way.

How can data on known criminal networks be more effectively shared between financial institutions and law enforcement?

This is a tremendous opportunity if we can be better aligned as an industry, and if we aren't aligned, we are a step behind how our adversaries are working. Think about this: criminals collaborate and share data all the time, they collaborate on the dark web discussing how to defraud companies, they have exchanges where data is bought and sold.

Now when you think about our industry, how we share information is very different. Across the US, UK and EU, you've got a lot of different entities that are trying to fight fraud, many of them by themselves. Yet one way to really win in the fight against fraud is to unlock the understanding we have individually and share it with others – using data for good, potentially through a fraud consortium. At Fiserv, we are developing a fraud risk exchange that will enable participants to share information, to share trends, and then enrich others who participate so they can make better decisions. To be able to use that data in a collaborative way is how we will stay one step ahead of criminals.

How can the public and private sectors more effectively collaborate on combating fraud?

Every time we get people together in our industry and start talking about what's happening, you find a lot of synergy. So, part of this is that we need to spend more time communicating and collaborating. We need to spend more time talking across lines of business and across business groups. We need to spend more time talking across different corporations and different types of entities that play in different markets.

We know government entities see a lot of things that our industry may not. Law enforcement agencies, for example, see trends from Suspicious Activity Reports (SARs) which gives them a distinct viewpoint. Getting public and private sectors in the room discussing current trends, the evolution of fraud as it is happening, and then determining how we work together is something we must do more of. We owe this to our customers. We cannot think we're going to win if we continue to fight this by ourselves. We need to collaborate, we need teamwork and to partner, and then we need to figure out how to share information so we can all make better decisions. You need to protect your customer but at the same time, you need to figure out how not to disrupt them from what they're trying to do. That's the yin and the yang of fraud.

Ryan Schmiedl, Global Head of Payments Trust and Safety, J.P. Morgan

"One of the best deterrents to prevent criminals making fraud attempts is to hold them accountable in a court of law."

Watch Ryan's video interview here.

What types of data are critical to identifying fraud and who holds them?

There are various types of data that are critical to detecting and preventing fraudulent events. At a broad level, let me review some examples. One, transactional data. Information about what took place might include parties, dates, amounts, locations. Two, is customer information. What we know about the customer that might help us determine whether that particular transaction is abnormal, whether it's purchase history, profiles, preferences, that type of information.

Another element is device and network information specifically for online transactions. Things such as device ID, which is your phone, computer, IP addresses, geolocations, network logs, things that can help determine whether or not that is actually the consumer or the right consumer making the purchase. Fourth, external sources. These could be public records; it could be third party enrichments that help take some of the data you've captured and provide more context. An example can be taking an IP address and retrieving the geolocation of that IP address where that device made that purchase. Last and not least is historical information. Data about the patterns of transactions either that the consumer, merchant or product that have taken place.

The importance of each of these pieces of data is relative to the use case. Things that are online events tend to lend most to digital information. In my experience, things like IP device location tend to be top performing features in detecting fraud, whereas with non-digital type transactions, like an ACH transaction, you might index more on the consumer, the originator or the beneficiary information to determine whether this is suitable.

When it comes to data, it's not just getting that data, it's also the ability to transform that data and interpret what the patterns mean. So, for example, how many transactions have occurred within the last 60 seconds to detect things like a bust out or card testing type scenario. So those combinations of features and the ability to aggregate, massage, calculate and engineer, those features really are important in order to detect various types of fraud. As it relates to who owns it, it depends on the context. Financial organizations, credit card companies and merchants are typically the top collectors. But vendors and network providers can provide things like device and network information as well as third party enrichments.

What role can AI play in detecting fraud?

There is no single mechanism that can be used to detect fraud. And in my experience, you need a multitude of different mechanisms layered on in order to help you prevent, detect and remediate

fraudulent attacks. Artificial intelligence and machine learning play a strong role in helping financial institutions identify anomalous or suspicious behavior and there are a handful of different techniques that are leveraged widely across the financial sector.

One is called a supervised technique. In essence, it is taking the known fraudulent attempts that have happened in the past and using it to train a model that can help you detect future attempts that are similar to that behavior. The second technique is unsupervised techniques or unsupervised models. You can think of this as ways that you can determine anomalous behavior. You're not sure whether that behavior is known to be fraud or not. You can tell it doesn't behave like its peers or it's not normal for that type of activity. And that is good for identifying fraudulent attempts that you might not have seen in the past. And the third thing is networks which have been evolving over the course of the last two decades and are important to find relationships and data, find non-obvious things like identifying a particular device making transactions on a multitude of customers. And so those are three of the main things that are used to detect and prevent fraud.

How can the public and private sectors more effectively collaborate on combating fraud?

There are multiple ways for collaboration between public and private sectors. Top of mind is data sharing. We are starting to make progress in this area but I think more can be done to share data about bad actors, whether that is confirmed fraudulent attempts within financial institutions or merchants or cyber attacks. Data is critical and the understanding of strictly labeled data. And what I mean by that is having a consistent bar that describes what is fraud and what we are attaching that data to. So, for example, what I have seen over the course of time is that one actor or one institution might claim something as fraud that is abuse or buyer's remorse versus something that truly is a bad actor compromising accounts to grab funds. So, one is sharing, two is working together to kitemark a common definition. The other area that can play a better role is collaborating on prosecuting known bad actors. One of the best deterrents is not just preventing it but holding ramifications for those that try to defraud others and holding them accountable in a court of law. We have seen that productively used and it's one of the strongest mechanisms to prevent criminals if there are consequences associated with making fraud attempts.

Lindsay Anan, Former Associate Partner, McKinsey & Co.

"Collaboration between public and private sectors is critical to fight fraud but it also requires mutual trust and accountability between partners."

Watch Lindsay's video interview here.

Does government and its agencies hold data that would help financial institutions in their fight against criminal transactions?

The public sector holds a significant amount of data, which could be a resource to help prevent fraud, and much of this data sharing occurs already today. Public records could be used to verify customer identities and identify any red flags while government agencies maintain watch lists that can help financial institutions screen customers and transactions.

Governments track cross border travel and analysis of patterns can help identify instances of money laundering. Tax and income data from filings from individuals and businesses can reveal anomalies. Government also monitors cyber threats and receives reports of crime from public and private victims while also sharing data on criminal activities. All of this can help strengthen cyber defenses of financial institutions. But a key point in sharing data between entities is compliance with applicable laws, regulations and care must be taken to protect the privacy and security of the data being shared.

What role can AI play in detecting fraud?

AI does but will play an increasing role in fraud detection. Machine learning, network analysis and behavioral analytics detect complex patterns of fraud that humans or rules-based systems might miss. AI can also help spot anomalies, connecting the dots across large sets of data to uncover sophisticated fraud rings. Generative AI also detects red flags and text, fraudulent sentiment analysis or entity analysis, and look at fraudulent pattern recognition, across text, voice, emails etc. And AI continuously learns and adapts from the new data to improve detection capabilities. While AI can be a powerful tool in detecting fraud, it's not a one size fits all solution. The use of AI should be carefully evaluated and implemented, making sure that there's enough governance, compliance and consideration.

How can data on known criminal networks be more effectively shared between financial institutions and law enforcement?

Data sharing consortiums like the Financial Services Information Sharing and Analysis Center (FSISAC) facilitate data sharing between entities to prevent and mitigate cyber threats to financial institutions.

Multi-party data analysis platforms are another option. This is where contributors can access and analyze shared data in a controlled environment, and participants can work collaboratively on common data sets. Today, some health insurance consortiums use all payer claim databases which pool claims across multiple providers, aggregates and identifies trends, fraud, waste and abuse. The raw data is restricted with only the aggregate

insights and analysis being distributed to members.

Government could consider potential frameworks on responsible data sharing between entities, where fraud is suspected, stating the types of permissible data exchanges, mandatory controls around privacy and use, or standard clauses for data sharing agreements, and regulatory oversight of data sharing partnerships. Law enforcement often receives data from financial institutions for investigations but it could also provide more intelligence on things like typologies and criminal networks without compromising an ongoing investigation. Providing guidelines on standard data formats and protocols to allow for better integration and analysis across different systems and organizations would allow for standardized exchange of data which could lead to secure data sharing platforms that facilitate the secure exchange of data.

Should a financial institution be able to refuse to act on the payment instructions of a customer if fraud is suspected?

Financial institutions should have clear and robust policies and procedures to assess fraud, risk escalation, verification, decision making and ensuring that staff are sufficiently trained if an institution detects potential fraud and ultimately refuses payment.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

Public awareness campaigns and consumer fraud alerts could help highlight emerging threats and educate consumers on the risks of phishing, identity theft, online fraud, phone scams as well as ways to mitigate those risks. Fraud monitoring services track consumer accounts, credit reports, transaction identity to detect fraud as early as possible with timely alerts for consumers to take action. Some of this is already offered by financial institutions or credit bureaus and tech companies.

How can the public and private sectors more effectively collaborate on combating fraud?

Controlled data sharing between the public and private sectors could detect sophisticated fraud that any one organization can't see alone. Timely sharing of tactical strategic intelligence on fraud and cyber crime can improve risk awareness and alert companies to imminent attacks. Pilots have the added benefit of building trust and understanding. Regular dialogue between the public and private sector could help foster a mutual understanding and alignment in combating fraud. Collaboration between public and private sectors is key to help fight fraud but it also requires strong communication, mutual trust, shared goals, coordinated efforts, and a strong commitment to information security, privacy and accountability between partners.

Claire Simpson, Senior Manager, Payment Systems Regulator

"We at the PSR work very closely with the other UK authorities – all are focused on pursuing and blocking fraudsters and empowering the public."

Watch Claire's video interview here.

What types of data are critical to identifying fraud and who holds them?

The Payment Systems Regulator (PSR) is the UK's operational regulator of payment systems. We regulate all payment systems and mechanisms, including cash and cheques. We know that data is critical to identifying all types of fraud risk in payments. More data needs to be identified and shared effectively, particularly at the point a fraud is occurring. For example, sending firms hold all the KYC information provided by customers as well as transaction details. Do the two match up, eg. for students recruited as money mules, does the turnover on the account reflect student status? The work we – and others – are doing is understanding how critical that data is and how it can be shared more widely.

The first basic step is to ensure sending firms are sharing that reported fraud data with receiving firms to enable greater scrutiny of the receiving account which potentially is being used for criminal purposes – and report them to law enforcement. As you may have seen from the British media, banks are telling us that a significant proportion of fraud also comes from a small number of tech platforms so also sharing fraud data with those firms could help to address fraud at source. To better incentivize this, we are now requiring firms to collect data on both sending and receiving levels of fraud and where that fraud originates and plan to publish it so all firms across the ecosystem are held to account.

It is also important to look at the systems to enable better data exchange as part of a payment journey. In the UK, we were responsible for introducing Confirmation of Payee which name checks a new payee to your account and that is communicated between the sending and the receiving firm to verify the identity of that account. This has been really successful and over 92% of payments across the UK's Faster Payment System are now identified in this way. This has unlocked a capability within the system that could generate more important data points about the transaction and create a potential 'risk indicator' associated with a payment, even before a fraud has occurred.

Should a financial institution be able to refuse to act on the payment instructions of a customer if fraud is suspected?

This particular type of authorized push payment (APP) fraud is a significant issue for the UK's Faster Payment System. Whilst there are huge benefits in this system as it provides the ability to move money instantaneously, people are exposed to increased risk as the funds are often difficult to recover once a victim realizes they have been defrauded.

But to the question, absolutely yes. FIs should not make a payment where they have a reasonable

belief that a crime is being committed or a fraud is being undertaken. It may very well be the case that FIs are better informed about the risks of a transaction than the customer who is being socially engineered by a sophisticated scammer. In the UK, the banking protocol allows firms to stop payments in very specific circumstances, including suspected fraud and in 2022, this protocol was used 11,643 times on transactions worth £55m in total.

In addition to this, the UK Government is also working towards a risk-based approach to delaying payments on the sending side as well as delaying crediting the account on the receiving side so that such suspected fraudulent payments can be properly investigated. We recognize that both stopping and delaying has the potential to cause frustration for customers making legitimate payments, so we want to see risk assessments be transaction and account specific to minimize inconvenience and allow legitimate transactions to flow.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

This is a real challenge in relation to APP fraud because the characteristics of different people groups are targeted through multiple methods and channels. Whilst we see different scam types emerging, eg. impersonation of your FI, customer understanding of APP fraud is not great. In customer research, we see that customers believe it is low level opportunistic criminals, not highly sophisticated multi-network criminal activity and often customers are reluctant to see themselves as genuinely at risk.

Our tools are becoming more effective: confirmation of payee, and also AI will undoubtedly play a role and of course better education programs by the banks. Again, data will help unlock issues so that more targeted and specific engagement with consumers can occur such as effective warnings.
We work very closely with the UK authorities, other regulators and government; all are focused on pursuing and blocking fraudsters and empowering the public, as set out in the recently published UK Home Office strategy. Consequently, there will be a greater coordinated approach to engagement with consumers across the fraud ecosystem.

How can the public and private sectors more effectively collaborate on combating fraud?

We work closely with the UK government, the police, the Financial Conduct Authority (FCA) and Ofcom, the UK's communications regulator. Together we are working to put in place effective measures to address APP fraud.

Firstly, it is vital to understand the true size of the APP fraud issue in the UK, so for the first time, banks and payment service providers will collect data on their APP performance fraud rates, how much they reimburse and critically, we will publish this data. Those that have the highest levels of fraud will be identified. This will give us a better understanding of the size and dimension of the problem. We are also collecting data on the source of fraud and where these frauds originate. As above, the big tech platforms and telecoms have a role to play, so should be also held to account across the network.

The second area is putting in place financial incentives. In June 2023, we announced that we will require reimbursement to customers of APP fraud. This obviously provides a better consumer outcome as those genuine victims of fraud will get their money back but it also puts the incentives on the right parties to act and put effective controls in place. We shall therefore split liability 50/50 between the sending and receiving firms. This puts a significant set of responsibilities on the receiving side which don't currently exist. But we also want to help consumers to act responsibly and carefully when making online payments, therefore we will

levy an excess on reimbursement to incentivize caution.

We recognize that this is a significant shift and we are making sure that payment firms have the tools to manage fraud effectively and we really want to engage with industry on this. We touched earlier on the ability to share risk indicators and also the ability to delay payments.

Thirdly, is informing and empowering customers, moving beyond the kind of generic warnings to genuine risk-based interventions in that payment journey.

The final area is effective law enforcement, and we think the banking industry has a really important role to play here. Victims of fraud are more likely to report it to their bank than they are to law enforcement. So, we'd like to ensure that there is sufficient intelligence sharing between them, to assist law enforcement in being able to effectively target the criminals behind these frauds.

Kate Frankish, Chief Business Development Officer, Pay.UK

"Education is key because fraudsters move so quickly that by the time you release a new tool, the fraudsters have diversified."

Watch Kate's video interview here.

What types of data are critical to identifying fraud and who holds them?

There's no real silver bullet for fraud but there are lots of different sources. As the UK's retail payment systems operator, in 2022 we processed 10 billion transactions and we see transactional data as key. There's also things like customer profiling, biometrics and black and red lists of good and bad actors that the market holds. Additional data from telcos and social media companies is becoming really important for fraud tracking because in the UK, nearly 80% of APP fraud starts on social media platforms with another 18% starting from telcos. We're starting to track that data and combined with transactional and customer data, we start to have rich data that shows patterns that can be used to help our banks track and stop as much fraud as possible.

Does government and its agencies hold data that would help financial institutions in their fight against criminal transactions?

In the UK, there are a number of different government agencies who hold key data. For example, the Passport Office holds significant amounts of detail on passport numbers that have been flagged as criminal based. But the challenge is sharing that data or getting access to it. The difficulty is permissions and people feel uncomfortable with sharing data. When you take a step back and look at it, fraud is not a competitive market. Maybe it is for the fraudsters but for the people who are trying to stop it, we should be collaborating much more. But until we have a government body covering everything and pulling all parts of the industry together to look at a consolidated view, we're going to struggle to get real traction.

What role can AI play in detecting fraud?

AI is beneficial if used properly and that's probably the most important part of the discussion. Because what consumers and businesses want are frictionless payments and they want them to be secure. And what we've done in the UK, with things like Confirmation of Payee, is put friction into the journey. It asks the payer to put in a name of the individual and their bank details and it sends back a yes, a no or maybe to give the payer confidence that they are paying the right person or business. This service has been significantly successful and is now seen as a hygiene factor by payers. So, some friction is good, but too much friction may put people off actually making payments. What AI can do in the background is send a risk flag to the bank. Each bank has different risk appetites so it's up to them to decide how they use AI and it's only one of the elements of making a decision to let a payment go or to push it into a fraud queue to look at it more carefully. So AI does definitely have a place because it doesn't add friction but it's one of a number of different elements that a financial

services company would need to take into account when looking at fraud.

What role can government play to verify the authenticity of KYC documents?

There are hundreds of technical companies globally who offer KYC services for banks and PSPs. What the government could do to make things easier would be to recommend a number of those companies. It's a bit like a construction project: you want to use a recommended builder with a good reputation. And so, some form of stamp or kitemark from the government would be really helpful for the industry.

Are there any regulator issued liability waivers that would improve collaboration between financial institutions and with regulators and law enforcement?

There's nothing specific that I know of today, and this is where we always get stuck because with laws like GDPR, which are there for the right reasons to protect consumer data, it puts barriers in place for organizations to be able to share data because a data breach has a consequence and the consequence is normally financial and quite significant. That's the really big sticking point. You want something that's well controlled but for certain circumstances such as the prevention of financial crime and fraud, there should be some way that data can be shared in a protected way.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

It comes down to education every time. But even saying that, some of the APP scams that we've seen recently are so realistic that even somebody who's incredibly savvy can be tripped up. But if people are educated over and over again, then it helps people stop, think, don't do things in a rush when you're being pressured into it, certainly don't make a payment or give out your bank details in that kind of circumstance. Education is key because fraudsters move so quickly that by the time you release a new tool, the fraudsters have diversified. So, continued education and something coming from government to the whole population would have a better cut through than the great work that individual banks are trying to do with their customer bases.

Rodney Abele, Director of Regulatory and Legislative Affairs, The Clearing House

"The private sector can assist government in the effort to fight financial crimes but detection and reporting without prosecution simply allows criminals to repeatedly attempt their crimes."

Watch Rodney's's video interview here.

What types of data are critical to identifying fraud and who holds them?

The most important data elements that FIs hold are the identities of the sender and the recipient, as well as the patterns of their past behavior. In contrast, network-level monitoring is typically used to protect the health and functioning of the network and wouldn't identify possible instances of consumer fraud on a per transaction basis. Also, it would add operational complexity and slow down the efficiency and speed of payments. However, network-level tools may be useful to the sending financial institution if they help validate the legitimacy of an intended recipient before a payment is initiated. And so in some cases, network-level tools may be helpful in reducing fraud across the system. While it is still early in its implementation, this appears to be working well in the UK with their Confirmation of Payee scheme.

Does government and its agencies hold data that would help financial institutions in their fight against criminal transactions?

Regulated financial institutions always welcome opportunities for increased partnership with government and look for ways to improve information sharing, particularly from government and law enforcement. The FBI, in particular, already has access to a significant repository of data and, if it was shared more easily with banks, might allow FIs to prevent bad actors opening multiple accounts and perpetuating their fraud across the system.

What role can AI play in detecting fraud?

Artificial intelligence and machine learning technologies have made impressive strides lately. You can't ignore the headlines that they've captured. And many FIs already use sanction screening programs using this technology but it is a long way away from being mature enough to be mandated across FIs. Currently, the technologies are not without certain weaknesses and their success depends on how these tools are used within each bank's particular compliance program. Banks would be well served if both AI vendors and regulators worked together to help banks by testing and validating tools prior to their deployment. As always, regulators must maintain technology neutral and remain focused on the outcomes that screening programs produce. Mandating the use of any particular technology though should be carefully weighed against the risks of its future obsolescence.

How can data on known criminal networks be more effectively shared between financial institutions and law enforcement?

The private sector can assist government in the effort to fight financial crimes through detection and reporting of malicious behavior. Reciprocal data sharing by government agencies to the private sector is also critical to ensure payment systems are not used for financial crimes. In cyber security, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Systemic Analysis and Resilience Center (FSARC) have proven to be very successful models for the government to keep the private sector informed of new and ongoing cyber threats.

I believe industry would welcome more information from government to identify and limit the spread of payment scams, perhaps building on the successful models for cyber security. But detection and reporting without prosecution simply allows criminals to repeatedly attempt their crimes using another bank. Financial crimes like account takeover, business email compromise and P2P scams are not victimless crimes. Only law enforcement has the power to prosecute criminals and prevent them from repeatedly attempting these frauds on additional victims.

Are there any regulator issued liability waivers that would improve collaboration between financial institutions and with regulators and law enforcement?

We want to improve constructive data sharing to prevent fraud but doing so should not impose additional risks of liability or burden. We have an example of this kind of reduced liability in the context of information sharing between FIs under Section 314(b) of the Patriot Act in the case of activities that may involve money laundering or terrorist activity. But it can be difficult for banks to determine when instances of fraud might be money laundering. And so, this highlights the limitations of attempting to use Section 314(b) to address payments fraud more broadly. But it's worth exploring whether a similar statutory authority should be passed to permit data sharing specifically to prevent and remediate instances of financial fraud.

What tools could industry and government provide to consumers to assist them in avoiding being defrauded?

Even with perfect consumer education and real-time fraud monitoring alerts, consumers will sometimes insist on proceeding with a payment transaction. We recognize that industry and government will never rid fraud from all payment networks. However, I want to distinguish between purchase fraud and payments fraud.

In purchase fraud, the fraud revolves around the "what" that the sender thinks they're buying. They think they're buying a car; it ends up being a toy car. In payments fraud, the fraud revolves around the "who" the sender thinks that they're sending money to. This kind of fraud relies on concealing the true identity of the recipient account holder. This is true in business email compromise scams where the intended recipient is legitimate but the receiving routing and account numbers have been changed. In many P2P texting scams, recipients impersonate reputable businesses or utilities and cajole victims into sending them payments, sometimes through fake threats of account closures.

One key to reducing electronic payment fraud would be to give better information to senders on the true identity of the receiving account holder. If senders could verify a routing and account number of their intended payee, it would reduce the incidents of deceptive payment inducements.

How can the public and private sectors more effectively collaborate on combating fraud?

To better combat electronic payments fraud, industry and government should collaborate on ways to better digitally authenticate KYC during account opening and verify to payment senders that a recipient account holder is the sender's intended payee, preferably with identification that is more reliable than a social security number. However, these solutions will take significant time to come to market.

In the near term, government and industry should tackle the misuse of text message and SMS fraud as it's one of the most common vectors for initiating payments fraud. Many text message scams rely on the fraudster spoofing the identity of a known sender like telcos, streaming services or package delivery companies. Increased prevention of caller ID spoofing is low hanging fruit and would reduce the number of victims of payment scams. In the US, telcos and the FCC should address this in the near term.

About P20

P20 is a UK/US-led forum where the best informed and most influential people in payments convene to discuss issues of importance and to influence the thinking around policy development.

P20 convenes industry, government, regulators and law enforcement to accelerate progress on our 4 Pillars: Combating Fraud & Criminal Transactions, Cyber Security, Financial Inclusion and Environmental, Social & Governance (ESG).

It is a collaborative space for thought leadership, best practice and ideas for harmonizing global standards on these key non-competitive issues. P20 hosts forums for these conversations to flourish and regularly publishes thought leadership and best practice reports.

Our vision is to create a more accessible, secure and inclusive payments ecosystem in which commercial competition can thrive in a safer environment for the benefit of all.

payments20.com
P20 - Payments 20