Focus on Money Mules: A Collaborative Approach to Fighting Financial Crime

A P20 Fraud & Criminal Transactions Working Group Report

September 2022

Foreword

I am delighted to introduce this report on money mules from the P20 Fraud & Criminal Transactions Working Group. I would like to thank the Working Group's Chair, Steve Ledford of The Clearing House, and the other Working Group members listed at the end of this report, for their hard work.

According to the UK's Financial Conduct Authority, every week more than $40 billion is laundered of which only 1% is intercepted and seized. Money mules are a major component in this global criminal web.

This report not only sets out specific best practice recommendations to combat Application Fraud and Payment Fraud but shows the effectiveness of improving anti-money laundering (AML) processes through Machine Learning and better collaboration throughout the whole payment ecosystem.

Reducing financial crime is a pillar of P20 and its members and I hope that you enjoy reading the report and find the insights beneficial.

Duncan Sandys,
CEO, P20

Recommendations

Application Fraud

- Combine data so that nonmonetary and monetary data is looked at in conjunction with applications. Look at common devices, addresses, payers, payees and transaction amounts.
- Complete behavioral profiling to combine session and account behavior to identify commonalities and trends in mule behavior.
- Orchestration of 3rd party data sources (e.g., Fraud consortiums, Credit Bureau data, Device data, Mobile network data) depending on the risk factors, your fraud detection solution should be able to utilize other data sources to enrich fraud profiling decisions.
- Efficient workflows that minimize customer friction for low-risk applicants and allow for medium/high risk applications to have further authentication or manually reviewed if required.

Payment Fraud

- Combine any application data and risk scores with ongoing account monitoring to get a richer view of the customer (e.g. does the type of business or occupation match the amounts deposited or transferred).
- Combine payment risk and mule risk detection where possible to create holistic view.
- Complete behavioral profiling to combine session and account behavior to identify changes that are apparent when a mule is about to receive funds.
- Lifecycle scoring can be used to score mule risk on an account every time customers engage with new products or complete transactions.
- Setup your fraud detection system to intervene in real time when payments are received into accounts so that fraudulent funds can be captured (e.g. offsetting receipts and transfers in close succession are a telltale sign of mule activity).
- Retrospective profiling. Ensure that when mule accounts are identified that they are reviewed to check for links to other existing accounts.
- Dormant account profiling and closure. Identify accounts that are opened and left to then be sold on to criminals.

Introduction

Whether they are committing fraud, dealing illegal drugs, breaching computer systems or trafficking humans, most criminals share two objectives; they want the money produced by their criminal activity, and they don't want to be caught. An entire global industry is helping criminals achieve these objectives. The frontline workers of this vast enterprise are money mules – people who move money to hide its criminal origins. For the payments industry, targeting money mules could be the key in fighting a broad range of financial crimes.

Money laundering is big business. According to the United Nations Office on Drugs and Crime the estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars.

Preventing and prosecuting money laundering is a major policy objective of national governments, and a focus of international collaboration through the Financial Action Task Force (FATF). Money laundering involves moving money, so banks and other providers of payment services are on the front line of anti-money laundering (AML) efforts. AML compliance is one of the most crucial, but also among the more difficult, regulatory requirements faced by banks and payment service providers. In 2020, global banks were hit with $10.4bn in fines for moneylaundering violations, an increase of more than 80% on 2019, according to Fenergo, a compliance-software firm.

The purpose of money laundering is to obfuscate the source, movement and destination of illicit funds produced through criminal activity. This makes the AML prevention and detection efforts inherently difficult.

If the proceeds of illegal activity are cash, money laundering might start with deposits at banks that have gaps in their AML programs or by combining it with the otherwise legitimate deposits of cash-rich business. The proceeds of fraud or embezzlement, on the other hand, are more likely to move directly into bank accounts without the need to deposit cash.

Many money laundering schemes utilize intermediaries, known as money mules, to move illicit fund and make these transactions look legitimate. The methods used are often very sophisticated, involving multiple money mules, complex webs of transactions and other techniques that evolve as industry defenses improve.

As noted earlier, various types of criminals use money laundering to avoid detection. This common reliance on money mules, however, gives banks and other payment service providers a way to identify a variety of financial crimes. Finding the money mules and following the money can help fight fraud, identity theft and cybercrime as well as money laundering. Collaboration between the various departments tasked with cyber defense, anti-fraud and AML efforts can yield results that amplify existing approaches to achieve superior results. The purpose of this report is to provide guidance on how to do so.

Types of Mules

Like most types of fraudsters, there's never just one flavor. Money mules are no different. In order to understand how to best stop money mules, it's important to learn about the different types. You can then map the behaviors back to the customer journey and relevant data available for your technology to ingest.

Complicit

The first type of money mules are "complicit" ones. These mules are fully aware of their role as a mule to facilitate criminal activities. They often open more than one account as an opportunity to scale their operation. They may be willing to participate in the cash-out process, something traditionally not taken on by other mules. They may even help recruit additional mules, often through personal connections, job boards and social media sites.

Witting

We then move on to the "witting" mules. These people have a suspicion something is not right, but are drawn in by the prospect of making money and so ignore their instincts. They also may ignore more obvious warnings that are provided. Generally speaking, they act naively and assume this will get them off the hook, should anything be found out.

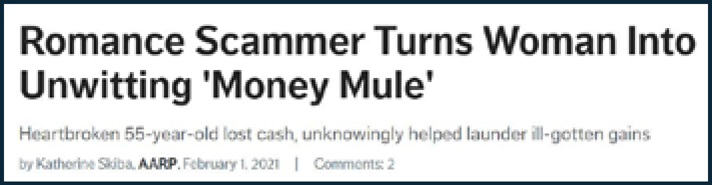
Unwitting

And finally, the most unfortunate type, the "unwitting" money mules. These mules are unaware that they are being used as a mule. It's often part of a scam that manipulates them into thinking the work they are doing is legitimate. It could be disguised as a work-from-home gig or just a simple way to make some extra money.

Recruiting

Fraudsters will often target the most vulnerable in society who are more susceptible to this type of manipulation. For example, students who are new to banking and managing their own finances are recruited to act as mules, or agree to "sell" the accounts they used at university to money launderers. Unemployed individuals might fall for "work from home" solicitations. However, it is important to note, anyone can fall victim to these scams and they are becoming more and more sophisticated.

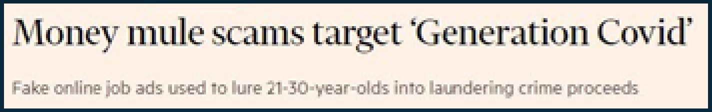
Headlines



Romance Scammer Turns Woman Into Unwitting 'Money Mule'

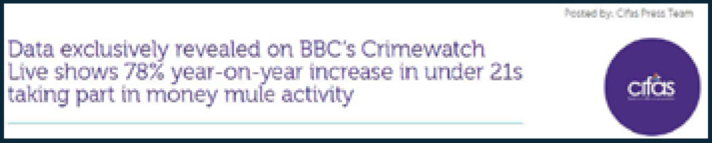
Heartbroken 55-year-old lost cash, unknowingly helped launder ill-gotten gains

by Katherine Skiba, AARP, February 1, 2021 | Comments: 2



Money mule scams target 'Generation Covid'

Fake online job ads used to lure 21-30-year-olds into laundering crime proceeds



Posted by: Cifas Press Team

Data exclusively revealed on BBC's Crimewatch Live shows 78% year-on-year increase in under 21s taking part in money mule activity

https://www.cifas.org.uk/newsroom/mules-six-months-2021

Challenges to managing mule risk

The role of all firms is to ensure their AML compliance in the best way they can.

Money mules can however complicate the process of detecting and remediating financial crime and as such represent a significant AML compliance challenge.

While any routine process may feel like 'box checking', firms need to ensure that those undertaking this work are aware of its importance in preventing crime. This begins at account opening, where robust identity verification needs to be in place.

It may be that the customer identity attributes are false, or that the individual is being groomed to become a money mule.

Automation is increasingly supporting procedural adherence, whether for customer onboarding,

ID verification, or through transaction monitoring to highlight suspicious transaction frequency or volume patterns. Wider industry work, using payment system data, is proving useful to follow funds layering.

Detecting when customers are being used as mules is critical but can only be achieved by implementing sufficient risk-based AML measures. Payment providers may also automate monitoring with a real-time money laundering risk database.

We can expect this challenge to expand further, and it will need careful monitoring by national crime agencies.

- Vulnerable customers: Money launderers often seek to use elderly and otherwise vulnerable customers as money mules. These customers may attempt to open accounts or engage in transactions with challenger banks that do not match their risk profile.
- Geographic location: Accounts opened by customers located in high-risk jurisdictions present a much higher risk of money laundering. Funds that are received from or sent to high-risk jurisdictions are similarly high risk.

Who owns what between AML & Fraud

The general view appears to be that under the Three Lines of Defense risk model, fraud is first line control and AML second line oversight. AML functions however often appear to span both functions. These two taskes, however, do not always align in terms of goals, methods and outcomes.

Fraud teams need the ability to identify mule accounts if they are to effectively prevent fraud, while AML teams define risk appetite, risk policies and risk management frameworks, as well as oversee an assessment of performance against these.

It remains important in a firm's model that the two functions should work closely together, as without this, the firm will not counter fraud or meet its AML obligations as well as it might do.

Data sharing challenges

Suspicious Activity Reports (SARs) alert law enforcement to potential instances of money laundering or terrorist financing and are made by financial institutions and other professional sectors. They provide information and intelligence from the private sector that would otherwise not be visible to law enforcement. These may be seen as an intrusive additional activity by firms but serve a wider purpose in the collective prevention of financial crime.

It remains important that firms ensure staff are aware of their responsibility not to share any information with a customer which might be seen as 'tipping off' i.e. in any way inferring that they were part of a money laundering investigation or disclosing they are part of a terrorism investigation.

However, data sharing to national crime authorities as a Suspicious Activity Report is encouraged. Any further sharing must have a Defense Against Money Laundering (DAML) in place to ensure protection against the tipping off offence.

Financial institutions have obligations to file SARs in both the UK and the US, however the obligations are slightly different. In the US, under the Bank Secrecy Act (BSA), financial institutions are required to assist U.S. government agencies in detecting and preventing money laundering, which includes reporting suspicious activity that might signal criminal activity (e.g., money laundering and tax evasion). In the UK financial institutions must report their money laundering suspicions by way of SARs to the National Crime Agency (NCA); it is a criminal offence to fail to do so. Where there is a prospect of dealing with proceeds of crime, a defence against money laundering SAR (DAML SAR) must be filed and a defence to a money laundering offence must be received from the NCA before proceeding with a transfer of funds or a transaction. This mechanism for securing a defence in advance is not available in the US. The UK SARs Reform Programme[1] is seeking to address the current regime which may no longer be fit for purpose when set against the scale of the threats faced by the UK.

How crypto has exacerbated the problem

There are many ways in which the money launderer's 'exit strategy' can be pursued, and the three stages of money laundering are focused on achieving this. For the fraudster, the key is to ensure that the funds are within the financial system and able to be transferred without suspicion.

Often this might be achieved by the funds being used to purchase assets such as property or equivalent tangible and saleable assets.

Crypto assets have become easier to purchase through exchanges and with easier trading capability, offer new options for criminals to exploit. Current views are that this may happen particularly through OTC (over the counter) cryptocurrency exchanges, which tend to process higher volume trades and through the introduction of payment cards which allow users to spend crypto assets like fiat currency on an ordinary debit, credit or prepaid card.

The UK's Financial Conduct Authority (FCA) operated a Temporary Registration Regime (TRR) for existing crypto asset businesses from July 2021ending March 2022. FCA found that a significantly high number of businesses were not meeting the required standards under the Money Laundering Regulations. Only firms that were registered with the FCA or on its list of firms with temporary registration were permitted to continue trading. Other firms were required to cease trading from January 2021, with any that did not do so at risk of being subject to the FCA's criminal and civil enforcement powers.

How Challenger Banks Can Comply with AML Regulations

Given the severity of noncompliance penalties, including both financial and reputational consequences, challenger banks must find a way to address their money laundering vulnerabilities without damaging the convenience and commercial potential of the services they offer. FATF guidance recommends that firms take a risk-based approach to AML/Combating the Financing of Terrorism (CFT): accordingly, since they focus on online services and products, challenger banks must build effective risk assessment into their Customer Due Diligence (CDD) and Know Your Customer (KYC) measures to cope with the recent influx of customers. In practice this means implementing the following AML controls:

- Identity verification: CDD relies on being able to accurately establish and verify the identities of customers, including the beneficial ownership of customer-entities. Enhanced due diligence measures should be available for higher risk customers.
- Transaction monitoring: A foundation of KYC, transaction monitoring allows firms to understand their customers' behavior and the risk they present. During the pandemic, the transactional behavior of their new customers may be unfamiliar and challenger banks must focus on adapting their monitoring tools to accommodate changes in risk.
- Screening: Building on accurate CDD, firms must be able to screen their customers for relevant AML/CFT risk factors. These include running checks against international sanctions and watch lists, screening for politically

Strategic mule measures and recommendations

Application Fraud

Application fraud is a crime on the increase. Organizations face the challenge of remaining competitive and being able to have seamless customer experiences. Approaches such as instant application approval allow less time to assess customers and detect fraud. The most effective

[1] https://www.gov.uk/government/publications/home-office-major-projects-appointment-lettersfor-senior-responsible-owners/suspicious-activity-reports-sars-reform-programme-sroappointment-letter-accessible-version

strategy is to prevent fraud and decline potential mules at the point of application. This requires the detection of potential mules before their applications are accepted and without adversely affecting your speed of decisioning and customer experience.

Organizations will need to check application data for anomalies within the current application, anomalies against previous applications and matches against previous known and suspected fraudulent applications. These anomalies and matches can lead to applications being quickly and efficiently declined.

Here are some best practice measures you can implement as part of your Application Fraud strategy:

- Combine data so that nonmonetary and monetary data is looked at in conjunction with applications. Look at common devices, addresses, payers, payees and transaction amounts.
- Complete behavioral profiling to combine session and account behavior to identify commonalities and trends in mule behavior.
- Orchestration of 3rd party data sources (e.g., Fraud consortiums, Credit Bureau data, Device data, Mobile network data) depending on the risk factors, your fraud detection solution should be able to utilize other data sources to enrich fraud profiling decisions.
- Efficient workflows that minimize customer friction for low-risk applicants and allow for medium/high risk applications to have further authentication or manually reviewed if required.

Payment Fraud

Money mules can be very difficult to detect through the onboarding process, especially if the applicant is an individual with no previous fraud offences. Organizations need to ensure that as well as profiling new applications, they should monitor open accounts and use multiple data sources, including payment data to spot potential mule accounts after account opening. Understanding and being able to profile how a mule herder and mule use account facilities will help you create a strategy to identify them at the earliest opportunity. Understanding both genuine customer activity and comparing that against known mule behavior will also help you define a better performing mule prevention strategy.

Here are some best practice measures you can implement as part of your Mule Detection strategy:

- Combine any application data and risk scores with ongoing account monitoring to get a richer view of the customer (e.g. does the type of business or occupation match the amounts deposited or transferred).
- Combine payment risk and mule risk detection where possible to create holistic view.
- Complete behavioral profiling to combine session and account behavior to identify changes that are apparent when a mule is about to receive funds.
- Lifecycle scoring can be used to score mule risk on an account every time customers engage with new products or complete transactions.
- Setup your fraud detection system to intervene in real time when payments are received into accounts so that fraudulent funds can be captured (e.g. offsetting receipts and transfers in close succession are a telltale sign of mule activity).
- Retrospective profiling. Ensure that when mule accounts are identified that they are reviewed to check for links to other existing accounts.
- Dormant account profiling and closure. Identify accounts that are opened and left to then be sold on to criminals.

Applying machine learning to AML

Application of machine learning to anti-money laundering is a relatively new approach - most AML products on the market are built on a combination of rulesets and list-based screening. So, while more advanced techniques have been applied widely to combatting fraud, AML is still in the early stages of utilization machine learning to improve prevention and detection efforts.

With the advent of network-based machine learning, the adoption of consortia-level analytics, and the ability of Financial Institutions to integrate with low-latency managed services, this adoption of machine learning in AML has increased. Organizations are now in a position to apply contemporary data science - including machine learning - to the support AML efforts, generating a new class of products in the process.

While this is an exciting breakthrough in the fight against financial crime, the fact that this is a new type of service means that it takes some explaining, as the community who will benefit from this tool don’t have equivalent legacy services to compare them to. Hence, it’s important to be able to explain the most complex components of these AML services - the machine learning at the heart of AML algorithms.

There are many mechanisms to help explain machine learning based models, typically relying on highlighting which features are the most important to alerts and scores, or which example events had the most effect on the training of the model. A third, more recent approach is to focus on counterfactuals: answering "what-if" style questions about what would have to be true for a particular example to receive a high score.

To translate these ideas to the world of mules could explain:

- What aspects of a bank account are most important to look at when deciding whether or not they're a mule (feature importance)
- What kind of transactions are most likely to indicate money laundering (example importance)
- How a bank account would have to look different before it was identified as a mule (counterfactual)

In practice, the first of these three tends to be most useful, often in terms of reason codes which are often higher-level concepts derived from the important features. While these mechanisms are useful to explain individual decisions a model makes, they often fall short of explaining how the service as a whole works - how the model acts in the context of the product. For that we look to the world of visualization.

Internal collaboration

Financial crime pathways are blurring traditional distinctions between cybercrime, fraud and AML. Money mules offer a good opportunity to study these cross-functional use cases that are increasingly becoming the norm rather than an exception. Thus the 'mule'-disguised transfer of funds acquired illegally (e.g., through fraud, scams, human and drug trafficking) comes in combination with insider fraud (e.g., bank employee's credentials stolen with the help of insiders), cyber breaches (e.g., malware installed on the bank's computers to prevent discovery of transactions or route the funds to 'mule accounts') and engagement of sanctioned individuals or entities.

Untangling these increasingly complex criminal cases requires significantly more effective collaboration across functions within the bank. Operationally, AML, fraud, and cybercrime present significant synergies across process, controls, data and tools.

First, there is an opportunity to risk-score customers using common or similar customer data (e.g., financials, digital footprint, non-digital records). Customer risk rating and due diligence in AML, digital forensics in fraud and credentials management in cyber contribute to a much more comprehensive view of the parties involved.

Second, there are synergies in risk scoring of transactions using similar analytics and common use casing based on timing, destination/source, value and frequency, device/geolocation intelligence. The data to support this risk scoring of transactions can be sourced from transaction monitoring and name screening in AML and fraud, device and voice analytics in fraud, and Security Operations Centre (SOC) and Network Operations Centre (NOC) enabled monitoring in Cyber.

Finally, establishment of a common feedback loop across functions allows the bank to develop a holistic view on modus operandi (MOs) and drive top-down use case development. Moreover, this creates an opportunity to pool resources and capabilities to accelerate the bank's response to a threat.

Leading institutions are actively pursuing these synergies and trying to move away from siloed organizational teams with separated frameworks and taxonomies, infrequent information sharing (e.g., ad-hoc and only for most emblematic cases) and team capabilities that are developed separately and considering only departmental needs. Instead, they are embracing various degrees of integration across functions.

The less integrated models focus on fostering close collaboration with good practice joint committees, and interaction on an operational level. The functions maintain independent reporting, roles and responsibilities and frameworks built by each unit.

The more advanced model allows for each financial crime unit to maintain its independence, but ensures a consistent framework/taxonomy, roles & responsibilities, and shared systems or orchestration layer (e.g., across systems and data sources). Moreover, the three functions often join effort on prevention or high-risk forensic investigation.

The most advanced and integrated model contemplates a consolidated unit at least for part of the value chain (e.g., investigations). Operations follow a single framework, use common assets and systems to manage risks (e.g., single view of the customer, shared analytics) and include a mix of generalists and experts, acting upstream and downstream respectively.

Collaboration across AML, fraud and cyber promises significant benefits. With an effective exchange of data and analytical insights, Fraud is more likely to leverage intelligence from AML and cyber that are also relevant for a fraud incident (e.g., fraud proceeds being passed on through false accounts). It also allows for the leveraging of common technology platforms, with different modules and user interfaces. Last but not the least it addresses the often lagging communications for incidents that affect fraud, AML crime and cyber, besides leveraging diversity of knowledge and skills across functions.

External Collaboration

A complete approach for detecting monkey laundering would follow payments and transactions at a network level and across payment systems.. Ready access to data at a network level would also be extremely valuable to law enforcement, particularly when targeting organized criminality, and would be far less time consuming and costly than the current approach of liaising with each financial institution separately. Maximum network coverage can only be achieved by financial institutions working together. There are significant technical challenges to achieving this, particularly in terms of system integration and aggregation of data sources. Even within the same firm, systems often don't talk to each other. Powerful tools are expensive - although when the costs are measured against the annual cost of financial crime, it's likely to look like money well spent.

Apart from the technical challenges, data privacy issues present another hurdle. In the US, section 314(b) of the USA Patriot Act provides financial institutions with the ability to share information (that may involve money laundering) with each other under a safe harbor if certain criteria are met. In fact, FinCEN strongly encourages financial institutions to do so.

A key strategic priority within the UK Government's current Economic Crime Plan is pursuing better sharing and usage of information to combat economic crime, within and between the public and private sectors. Unfortunately, the much trumpeted information sharing gateways added in recent years to the Proceeds of Crime Act 2002, are generally considered to be a bit unwieldy and labour intensive and appear to be little used for that reason.

In terms of public-private partnerships, there are good examples in the money laundering space. When the Joint Money Laundering Intelligence Taskforce (JMLIT) was established in the UK in 2015 it was a highly innovative partnership between law enforcement and a small group of retail banks. Since then, this type of partnership has become more mainstream and JMLIT equivalents are now present in numerous jurisdictions. However, they remain relatively small scale, participation is generally voluntary and there tends to be limited resources devoted from the public side. It's noteworthy that the international standard setting organization for anti-money laundering, the Financial Action Task Force, does not prescribe Government support for, or mandate, public private partnerships in the fight against money laundering. Another example of partnership working is CIFAS, which facilitates the sharing of fraud data, based on the principle of reciprocity.

If data sharing partnerships are to be scaled up to tackle economic crime as a whole, we will certainly need better legislative gateways and greater funds made available by government. It will also be important for regulators to lend their support in navigating roadblocks. After that, the challenge will be integrating collaboration into operations and, given the cost and effort, how firms can be incentivized to get on board.

Geographical Approaches

How financial institutions combat money mules can vary by geography. All, however, agree more proactive measures need to be implemented. Aite did an interesting study, interviewing fraud executives from 22 of the top 40 U.S. banks and four large U.K. banks. More than 80% of fraud executives interviewed believe that more can and should be done to mitigate the risk of mule activities in the industry.[2]

In the U.S., in particular, mule detection tends to be more reactive. This is primarily because money mules are viewed narrowly as a money laundering concern, which restricts mitigation to what is required by regulations and reporting on suspicious activity. This results in a less compelling business case for banks to proactively manage mules. The other challenge is that financial institutions often don't know how much mule activity is running through their network. The same Aite report explains that "FIs in general, but banks in the U.S. market in particular, suffer from a lack of consistency in how they track and measure mule activity."[2] The inability to track and quantify the problem leads to challenges in solving it or at least drumming up a business case to solve it.

The U.K., in comparison, has more formal reporting standards and this has contributed to a more coordinated approach to combating money mules. This may be due to the Contingent Reimbursement Model that has been adopted by many banks in the UK and outlines that firms must take reasonable steps to detect accounts which may be, or are being, used to receive Authorized Push Payment (APP) scam funds. This means that if banks don't combat mules then they may end up being liable for the fraud loss rather than the sending bank.

The Aite report goes on to say "all of the fraud executives interviewed for this report from U.K. Financial Institutions (FIs) are able to provide much more detailed descriptions of mule detection capabilities that are more mature and more

[2] Aite, Mule Activity: Find the Mules and Stop the Fraud

sophisticated than those of all but two of the programs reported by the 22 FIs interviewed from the U.S. market". [2] That said, there are still improvements that can be made on the U.K. side of the pond.

Conclusion

Historically, the tools developed to address financial crime have been deployed in silos, limiting the ability to harness the full potential of the enterprise, the industry and public/private partnership. A focused, collaborative approach to money mules could not only address this crucial link in crime networks but could serve as a model for broader cross-discipline collaboration to fight financial crime. The payments industry has an historic opportunity to make a difference with an intelligent attack on money mule activity.

Report Contributors

Working Group Chair: Steve Ledford, The Clearing House

Jane Barber, NatWest

Liam Cooney, Mastercard

Nicole Tuckwell, Mastercard

Lee Kyriacou, The Clearing House

Claire Lipworth, Hogan Lovells

Kate Robu, McKinsey & Co

PJ Rohall, Featurespace

Mark Taylor, Featurespace

About P20

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

P20 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.

P20

payments20.com

P20 - Payments 20