



Best Practice Approaches For Combating Payee Scams



Foreword

I am delighted to introduce this timely report on payee scams 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.

"Payee scams" – authorized payments made in response to some form of fraudulent inducement by the payee – were a growing problem before the advent of COVID-19 but the pandemic has seen incidents rise at an alarming rate. As the world moved overnight to operate remotely and digitally, so did the fraudsters.

Governments, regulators and the industry approach this issue differently and although there are some common elements, there is little harmonization. For instance, the U.K. has been collecting and publishing data since 2017 and so is able to release very detailed statistics on the pandemic's effect on various payee scams.

This report puts forward specific Best Practice Recommendations for governments, regulators and industry to improve upon current practices, and to develop a more harmonized approach. Central to the recommendations is customer education and awareness, along with developing better fraud data, detection systems and prevention techniques.

I hope that you enjoy reading this report and that you find its insights and recommendations beneficial.

Duncan Sandys
CEO, P20

Best Practice Recommendations

For Governments & Regulators

- Create standard definitions to enable measurement of the problem
- Understand, define and publicize the problem
- Create and launch a consumer education campaign
- Encourage continuing education on these issues for banking and finance professionals
- Create a framework that encourages collaboration, data sharing and transparency

For Industry

- Continue to use and expand the use of technology for risk analysis and fraud prevention
- Develop a holistic approach to analyzing transactions that combines behavioral analytics and financial analysis of both the remitter and the beneficiary
- Create an effective process for post-payment analysis and data sharing
- Customize the approach, content and use of warning messages to consumers
- Integrate these issues within continuing education programs

Executive Summary

This paper aims to clarify market developments around “payee scams” (where a payment was properly authorized by the payer, but the payee fraudulently induced that payment) and evaluate options that might help protect customers and banks and reduce the ability of fraudsters to benefit from generic weaknesses in the ‘push payment’ market. Concerns over payee scams have increased with the wider adoption of ‘instant’ payment services, but apply where any payment is deemed irrevocable e.g., wires and most real-time credit-push payment systems (the paper does not address issues around the usage of cash). The different ways in which a payee can defraud a payer fall into two categories:

- where the payee misrepresents who they are; and
- where the payee misrepresents what they will do.

Current methods designed to deter fraudsters from initiating payee scams or to mitigate the impact of payee scams include:

- payer education;
- bank notification of payment irrevocability prior to payment completion;
- mechanisms that help to confirm payee identity; and
- fraud screening solutions that can identify suspect payees.

Of these, customer education is still considered to be the first line of defense.

Payee Scams vs. Unauthorized Payments

Fraud involving a payment is generally classified into two main types: customer “unauthorized” or customer “authorized” –payments. For the purposes of this paper the challenges of consumer protection for payments which have not been authorized by the payer (“unauthorized” payments) are not taken into consideration.

Fraud involving an authorized payment relates to the circumstance where the payer through some scam or misrepresentation of services offered or possibly because the beneficiary is induced to make the payment to a designated beneficiary.

Even though fraud is an integral part of these “scams,” the payment itself is not fraudulent.

In the U.K. these scams are referred to as “authorized push payment fraud,” while in the U.S. they are referred to more generically as fraud involving an authorized payment. In this paper, we use the term “payee scams” as a generic term to cover authorized payments involving misrepresentations by the payee.

Types Of Payee Scams

This graphic lists and describes the more common scams where a payer makes an authorized payment to a fraudster:

These payee scams involving an authorized payment can be classified into two categories, based on whether defrauding payee misrepresents:

- (1) **Who they are**, e.g., claiming to be a company CEO or a charity; and/or
- (2) **What they will do**, i.e., what goods, services or personal commitments they are to provide in return.

This distinction between “who” and “what” is useful in discussing later in the paper how to combat various scams, as there are some mechanisms to confirm the identity of the payee account holder prior to making payment.

Scams involving misrepresenting **who** the payee is include:

- **Business Email Compromise:** The fraudster claims to be a senior business executive – typically via commandeered or disguised emails – and directs the company to pay the fraudster. Because it can involve very large payments, Business Email Compromise accounts for at least half of all payee scams in the US (estimated at \$2 billion in 2019, according to the FBI IC3 study).
- **Invoice/Mandate Scams:** The fraudster presents an invoice or bill that seems to be from a party that payer ordinarily deals with, but is actually being paid to the fraudster. Invoice and mandate scams were the second most common type of payee scam by loss seen in the UK in the first half of 2020 at £45.6 million, coming largely from business accounts.¹



Advance Fee Scams

The victim is scammed into paying a fee to release a higher value payment in return.



Romance Scams

The victim is scammed into paying funds to someone they met online, after being manipulated and lured into a false sense of security.



Investment Scams

The victim is scammed into investing in a fake investment scheme.



Purchase Scams

The victim is scammed into paying for non-existent goods.



Imposter Scams

The victim is duped by fraudsters pretending to be law enforcement or a bank security department. The victim believes they are sending money to a ‘safe account’.



Invoice/Mandate Scams

The victim is duped into paying an invoice or bill to a known 3rd party by posing as the 3rd party in an email communication.



Business Email Compromise

A fraudster gains access to a business email account and then impersonates an executive (or other person of authority), scamming an employee into issuing a payment to an account they control.



- **Imposter Scams:** The fraudster claims to be any of a variety of individuals or entities – law enforcement, the security unit of the payer’s bank, the government income tax authority, a charity, or just using a false name – and convinces the payer into direct a payment. Police/bank staff impersonation scams accounted for 12% of UK payee scams cases and 18% of payee scam losses. Another 10% of payee scam losses were from other forms of imposter scams.

Scams that involve misrepresenting what the payee will do include:

- **Purchase Scams:** The fraudster convinces the payee to make an irrevocable payment for goods or services that will never be delivered. Purchase scams were a very common form of payee scams in the UK, accounting for 57% of cases and 13% of losses.
- **Advanced Fee Scams:** The fraudster offers any number of benefits – a sweepstake prize, a too-good-to-be-true benefit, or a more modest payout – that requires an upfront payment to the fraudster. Advance fee scams were the fourth most common payee scam in the UK, with 9% of cases.
- **Investment Scams:** The fraudster (both with and without using a false identity) offers a false investment scheme that requires the payee to make a payment. UK investment scams were the largest payee scam category in terms of losses, at £55.2 million or 27% of losses.
- **Romance Scams:** The fraudster convinces the payee, often over the internet, that they are offering affection or should be trusted to help with financial matters. Romance scams accounted for only 2% of cases and 4% of losses in the UK, though this does not count any associated psychological damage involved.

Note that these “what will the payee do” scams may or may not also include the misrepresentation of “who” the payee is. Also note that this is not an exhaustive list of all scam types. Depending on region and terminology, other scam types or naming conventions could exist.

Liability For Payee Scams

Understanding the breadth of opportunity for fraudsters to dupe consumers, recognizing the savvy nature of those fraudsters, and respecting the value taken from consumers each year, the question shifts to liability – who bears liability and when?

Liability for an authorized consumer payment involving payee scams or misrepresentation has, until recently, largely remained with the payer that authorized the payment,

although in the new UK consumer protection rights have led to the creation of a Contingency Reimbursement Model placing liability firmly in the hands of payment service providers (primarily funded by the major UK retail banks if the payer has met certain requirements).²

In the United States, the laws governing ACH and debit transactions limit the liability for consumers when an unauthorized transaction occurs. In the case of scams, where the payer authorized the payment to the fraudster, liability has been left to the payer – the general *caveat emptor* approach when private parties deal with one another. As a result, the assignment of liability in the United States occurs via rules established by the payment card schemes or network owners/operators such as The Clearing House (with regard to its RTP® network).

² The Financial Ombudsman Service describes how they think about assigning liability for Authorised Push Payment scams <<https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams>>

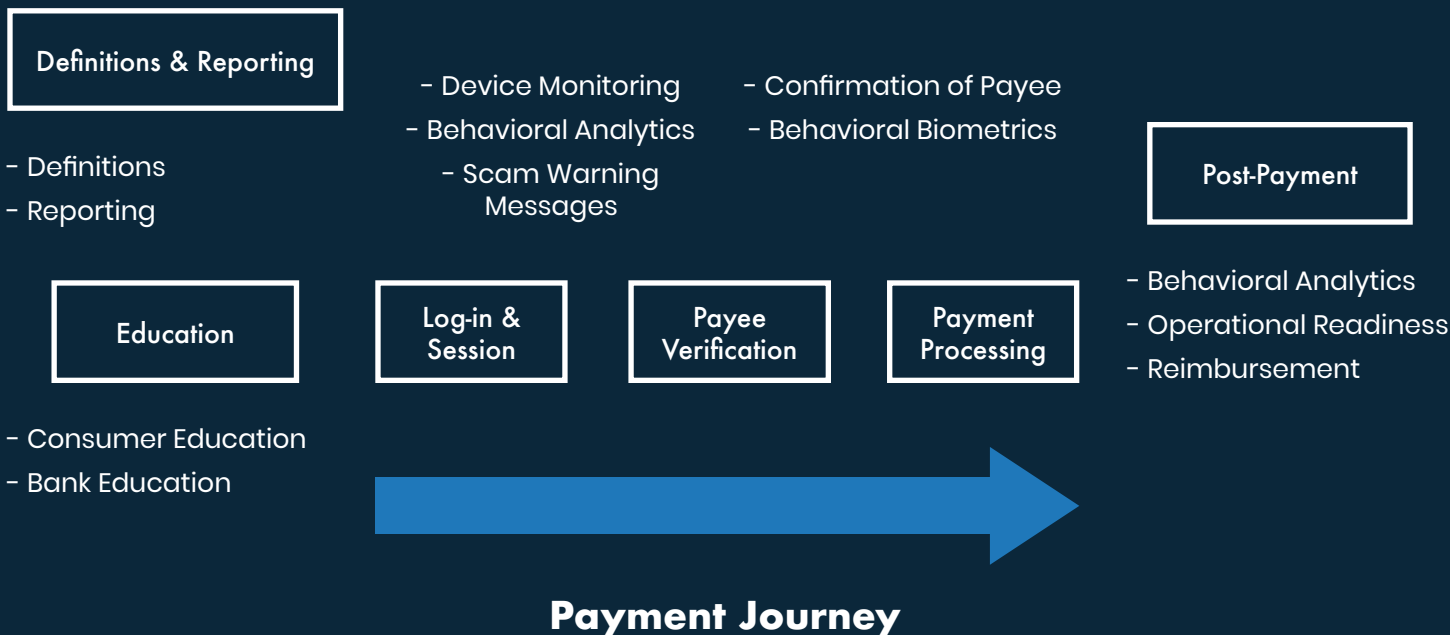
Deterring or Mitigating Payee Scams

Regardless of liability,

protecting customers against scams is good for business and can help avoid reputational risk.

Even more important, it protects people from significant financial loss and psychological damage.

There are several ways that payee scams can be mitigated. As the table below shows, it consists of a combination of definitions and reporting, consumer education, best practices by financial institution personnel in the case of payer present transactions and activities that payment service providers can take during and after a transaction is initiated.



Definitions & Reporting

If you can't measure a problem, how do you expect to stop it?

An adage as old as time, but very relevant when discussing payee scams in certain regions of the world. Historically, the United States has not distinguished between unauthorized fraud and payee scams when labeling their overall fraud losses. In order to best address and quantify the problem it's important to have more granular definitions of payment fraud. The U.S. is taking steps to better define payment fraud through the "FraudClassifier Model" developed by the Federal Reserve. The model was introduced in 2020 and will take time to mature into industry wide adoption.

Until then, you can look to regions like the U.K. as an example of stronger reporting around payee scams. UK Finance began reporting on payee scams in 2017 and the quantification and resulting actions have already paid dividends. No matter the reporting mechanisms in place, there is still progress to be made, but it is clear that granular fraud labels and accurate reporting is an important first step in addressing payee scams.

Consumer Education

In an increasingly connected world and an environment where more and more payments are taking place online,

criminals employ a variety of methods to defraud consumers and businesses. Highlighting these approaches to consumers is a vital preventative tool.

In order for fraudsters to perpetrate these crimes, a number of scams are deployed to trick individuals into sending money to the perpetrators. These payee scams are similar to those that trick victims into divulging their financial account information, or providing personal data that enables criminals to open bogus accounts and conduct illegal activities.

Generally, while the messaging for these scams is different, what payee scams have in common are the instructions that are provided for how to send money to the fraudster. Because scammers want the money as fast as possible and in a way that is less traceable and harder to claw back, fraudsters will encourage consumers to wire money using a retail remittance service, or they may ask for funds

² The Financial Ombudsman Service describes how they think about assigning liability for Authorised Push Payment scams <<https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams>>

to be put onto a reloadable prepaid card and provide the card's registration or card account number. Increasingly this practice is passing over to instant account to account payment solutions, where the beneficiary account can be a mule account.

In the UK, *Take Five* is a national campaign led by UK Finance and supported by payment and financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organizations. Its aim is to provide straight-forward and impartial advice to help people and businesses protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organizations.

Its key themes are:

- **Stop** – Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge** – Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect** – Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

The UK's National Trading Standards Body's initiative *Friends Against Scams* also aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams. Its focus is community action through awareness raising about the postal, telephone and doorstep scams which often target specifically at disadvantaged consumers or those in periods of vulnerability.

The Society of Citizens Against Relationship Scams (SCARS™) is a Worldwide Nonprofit Nongovernmental Incorporated Cybercrime Victims' Assistance Support & Advocacy Organization focused on the detection, deterrence, and eventual elimination on global online scams in all its forms, and the assistance and education of scam victims in their recovery and avoidance of future victimization. Their principal goal is the assistance of traumatized scam victims to aid in their recovery and avoidance of future victimization and to educate the public about socially engineered cyber-enabled crimes in all of their forms to prevent further cybercrime.

Bank Education

In the United States, several state legislatures have passed laws in recent years requiring qualified representatives of financial institutions, such as a tellers or financial advisors, to report situations when the qualified representative reasonably believes that

financial exploitation of a financially endangered adult may have occurred, may have been attempted, or is being attempted. The reporting can occur to a family member, legal guardian, account trustee, or state official, such as a representative in an adult protective services or Social Security division. Financial institutions provide annual training to staff that educates them on the warning signs of financial exploitation.

In the United Kingdom, the Banking Protocol is an initiative between the police, banking institutions and Trading Standards, which is designed to provide a standardized method to stop multiple victimization. Its aim is to identify at the earliest opportunity vulnerable victims who are in the process of being defrauded of funds from their bank accounts by criminals and to intervene to prevent these crimes.

Victims, particularly elderly and other vulnerable people are targeted by suspects for a range of fraud offences,

including courier fraud and bogus worker offences.

These crimes often involve the perpetrator encouraging the victim to attend their bank, post office or other financial services provider in person and withdraw or transfer cash.

If bank staff think the transaction is out of character, they will ask the customer questions such as:

- What is the money going to be used for?
- Who are you giving the money to?
- Was this withdrawal or transaction planned or unexpected?
- Have you had a call or been approached, claiming you have been a victim of fraud or offered an investment?
- Have you been contacted by someone claiming they are Police, bank staff or a trader?

If bank staff suspect a customer is being coerced or the transaction is a as a result of fraud, the police are contacted. The scheme also ensures extra support is provided to those customers affected to help prevent them falling victim to similar scams in the future, including through referrals to social services, expert fraud prevention advice and additional checks on future transactions.

Industry Measures

While consumer and bank educational measures can help mitigate payee scams, where the customer is tricked into authorizing a payment from their account, and that payment is executed in accordance with the customer's specific instructions, these are not foolproof mechanisms, as consumers may be unwilling to believe they are being duped. As a result,

it is incumbent on payment service providers to take additional steps to protect customers.

The growth in these types of fraud and the perceived gap in customer protection has led the UK Payment Systems Regulator and the FCA to require the industry to establish an industry code of practice for this type of payee scam. The resulting Contingent Reimbursement Model Code for Authorized Push Payments scams (the “CRM”) is a voluntary code overseen by the Lending Standards Board to which subscribers sign up to:

- Protect consumers with procedures to detect, prevent and respond to APP scams, providing a greater level of protection for customers considered to be vulnerable to this type of fraud; and
- Greater prevention of accounts being used to launder the proceeds of APP scams, including procedures to prevent, detect and respond to the receipt of funds from this type of fraud.

Importantly, any customer of a payment service provider that has signed up to the code can expect to be reimbursed without undue delay, and within 15 days at the latest (unless there are special circumstances in which case this can be extended to 35 days), where they were not to blame for the success of a scam.

Standards that firms are expected to adhere to include:

- On the send side:
 - Educating customers about the risks and types of scams (e.g. using customer accounts as “mule” accounts).
 - Taking steps to identify customers and payment authorizations that run a higher risk of being associated with this type of push payment scam.
 - Adding appropriate warnings to the customer journey.
 - Implementing a confirmation of payee solution to reduce the incidence of this type of fraud by enabling customers making a credit transfer to check that the name of the payee matches the account details at the payee’s bank.
 - Taking steps to protect customers who are particularly vulnerable to this type of scam and payments that appear at risk of being connected with such fraud.
 - Delaying payments suspected of being connected to a scam to the extent possible under a risk-based approach while it investigates the payment.

- On the receive side:
 - Identifying accounts that may be being used for such a scam or to launder proceeds.
 - Opening accounts in accordance with anti-money laundering requirements and industry recommendations.
 - Using and sharing available intelligence.
 - Freezing accounts and seeking to repatriate funds to the extent possible.

The scheme establishes a reimbursement model that participating firms should follow in determining whether to reimburse, which allows firms to consider the extent to which the customer is vulnerable or whether the customer has been grossly negligent.

Vulnerable customers will be refunded in full. In other cases, where a refund is determined as appropriate, the level of customer reimbursement depends on the extent to which the banks involved, and the customer, are found to be at fault.

Where neither firm involved has been found to be at fault, or a participating bank must provide a refund because a non-participating fund does not, the reimbursing bank can recoup their loss from a “no-blame fund” set up under the scheme.

However,

the approach regulators have adopted is slightly patchwork in nature, reflecting the continual evolution of payments fraud and the difficulty that regulation has in keeping up with it. As previous weaknesses are closed, fraudsters identify new weaknesses that can be exploited.

As a result, legislation and industry measures to bolster consumer protection have tended to advance in a somewhat piece-meal fashion, addressing specific issues to reflect concerns as and when they emerge. For example, the CRM is currently being reviewed by the UK regulator, with one of the issues under consideration being the extent to which participation should become mandatory for all payment service providers.

The Payment Systems Regulator (the PSR) has found that the existing CRM Code has improved outcomes for customers but is still leading to less than 50% of losses assessed under the code being repatriated. The main reasons for this being that the code is open to interpretation (especially around the exceptions that apply e.g. what constitutes an effective warning given by the sending payment services provider (PSPs), whether the customer has with a reasonable belief, and if the customer has acted with gross negligence) and does not protect customers of non-signatories.

The PSR have suggested the following measures to reduce scam losses:

- Improving transparency on outcomes – by requiring PSPs to publish their APP scam, reimbursement and repatriation levels.
- Greater collaboration to share information about suspect transactions – by requiring PSPs to adopt a standardized approach to risk-rating transactions and to share the risk scores with other PSPs involved in the transaction.
- Introducing mandatory protection of customers – by changing industry rules so that all payment firms are required to reimburse victims of APP scams who have acted appropriately.

Digital - Account Log-in & Session

Payments across digital channels have risen steadily over the last couple decades, with consumers flocking to a simpler, faster and more convenient way to move money. Unfortunately, along with speed and convenience comes different fraud challenges. This is particularly true in a real-time payments environment where the funds are immediately accessible and irrevocable. Increasingly,

many firms consider it important to deploy fraud prevention before the monetary payment.

Customer identity may be verified and monitored through ongoing KYC processes and customer behavior monitored at the point of log-in all the way through the online banking session.

Fraud practitioners deploy different types of technology and methodologies to combat payee scams. Here, we will highlight some of the approaches currently being used throughout the user journey.

Device Monitoring

This refers to the data and analytics associated with a specific device (often a device ID). There are technology solutions that leverage consortium level data and device profiles to understand device risk. The strength of this technology often depends on the strength of the data and insight into device behavior across various institutions and industries. While traditionally used to detect unauthorized fraud, it can be leveraged to monitor risky devices and target specific fraud MOs such as payee scams. Device monitoring can also help identify remote access and pre-scam activity which are common in some payee scams. To enrich their digital understanding, device monitoring technology will often layer in things like location, credentials, and other digital data of value. Some device monitoring solutions build a session profile for each customer and detect anomalies that may indicate someone is being scammed.

Behavioral Biometrics

This technology analyzes how a human interacts with a device, whether that be a computer or mobile device. Behavioral biometrics captures session data such as mouse clicks, scrolling patterns, and tap gestures, and alerts to anomalous behavior and/or common fraudulent behavior.

This pivots from the standard device data to the session data on how the individual is interacting with the device. Here are some examples of good behaviors to track.

- Session length is interesting as it is quite common for customers to have long sessions when they are being persuaded and manipulated by fraudsters.
- Using an accelerometer, financial institutions can determine if a tap gesture is light/steady v. strong/shaky, which can be useful when detecting if a genuine customer is operating under duress.
- Monitoring remote access is particularly useful when detecting payee scams.

Note, this is just a subset of the many behaviors you can track. A single behavioral biometrics signal is generally not enough to produce significant risk insight. However, combined together and layered with the previously discussed device intelligence, you can build strong risk-based intelligence.

Behavioral Analytics

This is a broader categorization and includes the analysis of monetary, non-monetary, and digital data to produce a predictive risk score. This expands on the previous two methodologies to include the robust profiling of digital, device, payment and non-monetary data.

As we move more broadly into behavioral analytics, the ability to profile across diverse data streams allows for multiple different profiling options. Now, the strength and sophistication of the profiling will depend heavily on the strength of the data and technology performing the analysis. The non-monetary and digital events are of the greatest interest when discussing log-in and session activity. These include things like channel data, beneficiary changes, two factor authentication responses, device ID amongst other events. Data can be leveraged to develop behavioral profiles and alert financial institutions to anomalous and risky behavior. Payments that are processed in real-time require behavioral analytics that can ingest this data and output an actionable risk score in real-time as well. An automated decisioning strategy where financial institutions can block, approve, or refer payments/accounts based on a variety of inputs will become increasingly important.

Analytics are more challenging when the genuine user is the one accessing the account and making the payment. Some important principles of behavioral analytics for payee scams are:

- The ability to profile both the sending account and the beneficiary account to get a holistic view. Is this the first-time sending money to this beneficiary? Is the beneficiary bank also new and known to have issues with money mules?
- The application of vulnerability markers to effectively profile sending accounts at a higher risk of falling victim to scams. Information as simple as customer age combined with other factors like channel usage can be flagged and serve as one indicator to feed into the overall analysis.

Teams that have a strong understanding of payee scam MOs and the appropriate data and fields to leverage can really add significant value. Also, more robust analytics that deliver truly differentiating machine learning technology will help financial institutions make the best use of the subtle behavior changes.

Scam Warning Messages

While digital journeys present risks, they also present an excellent opportunity to warn vulnerable customers. By leveraging behavioral analytics, financial institutions can send targeted scam warning messages to customers navigating through their online banking sessions. These messages come in many varieties, but the purpose is the same: to alert the consumer of a potential scam. Financial institutions should be careful not to send blanket warning messages as this could have a reverse effect and become white noise to the customer. Disrupting customers unnecessarily with inappropriate warning messages will add friction to the customer journey. In the same way that multi-factor authentication are risk based, so should scam warning messages. Therefore, financial institutions must underpin their scam warning messages with the same behavioral analytics that fuel their fraud alerts. This is the most effective way to leverage your risk insight and interdict in the customer journey at multiple touchpoints.

Payment Processing

Monetary events are probably the most obvious thing to profile in payment fraud prevention. However, it is important not to analyze these events in isolation. The previous log-in, session and confirmation of payee activity will provide substantial context and insight to the monetary events and should be performed as a holistic analysis. This is particularly true when addressing scams.

As with previous stages of detection, risk analysis for payment processing is easier for instances of unauthorized fraud. That said, subtle anomalies can be detected with the right technology and knowledge of scam behavior. And just like with non-monetary events,

it is important to profile both the sending account and beneficiary account to get a holistic view.

This might require increasing levels of co-operation, between payment service providers as regards the exchange of information on customer behavior.

For example, when profiling the beneficiary, it's often helpful to understand whether the beneficiary has received payments of this size and nature before. Also, different scams types can have different payments profiles, such as large one-off payments or smaller payments that gradually increase. Account loading is a common practice for some scams, where the fraudster will send funds to the victims account in advance of the scam. It's important for financial institutions to understand this data and behavior, and then layer some of the common trends back into their analytics.

Post-Payment Measures

The need to increase defenses to combat payee scams also extends beyond the payment into post-payment analysis.

Data sharing can enhance the ability to analyze payments activity, and is an important tool for banks and payment service providers to use when fighting payee scams.

Similar approaches and techniques that have proven effective in identifying and preventing these attacks from occurring in the first place can successfully be applied to improve outcomes after the payment has been made. The benefit of post payment analysis is the ability to incorporate more data into the decisions, as well as employ strategies that are more tailored to a human analyst making final decisions.

With the growth in payee scam attacks in the UK and US, there is a need for fraudsters to move the proceeds of these attacks through various payments systems to obscure the source of funds and enable a higher probability of a successful extraction or so called 'cash out'. As the proceeds of a payee scam are initially moved from the victim account to a beneficiary account (known as a money mule) there is an opportunity for a beneficiary bank to analyze the incoming payment to identify potentially suspicious activity that may indicate the beneficiary account is receiving stolen funds.

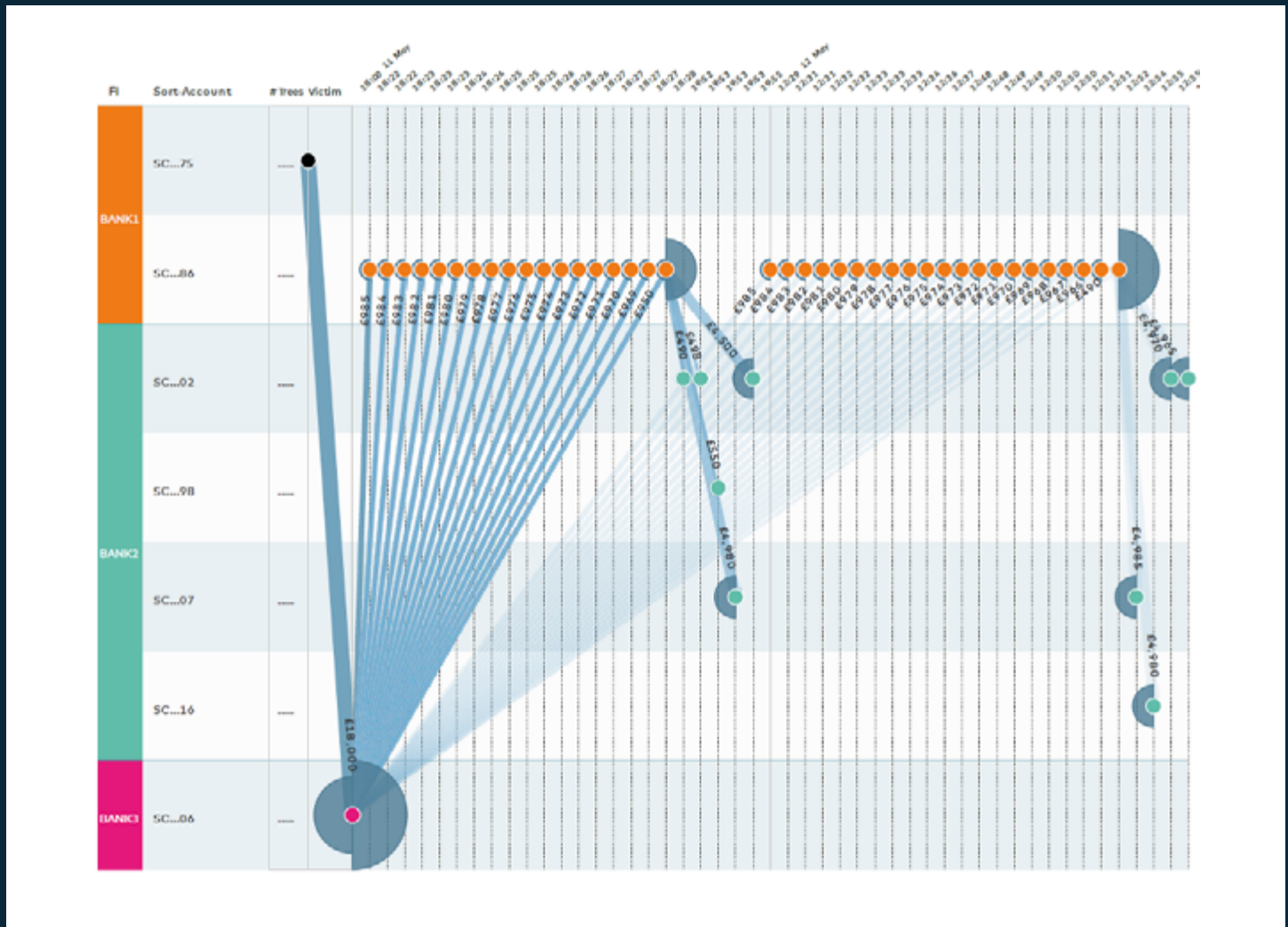
The use of behavioral profiling and analytics applied to incoming payments and beneficiary accounts is proven increasingly effective in identifying the type of anomalous behavior that may indicate incoming funds are the proceeds of fraud. For example, large funds transfers arriving into a newly created account, or one that has been open for some time but with little activity, may be an indicator that this account may have been created for the express purpose of being a money mule.

A system designed to enable fast and automated collaboration, as well as integration into the individual fraud systems within each bank, enables banks to rapidly work together to detect and prevent funds related to frauds from getting into the hands of the criminals.

Beating The Criminals

Analytics in isolation will not solve the problem; there needs to be collaboration and communication between the originating and receiving banks to make the intelligence actionable and effective in improving customer outcomes. While many banks have a loosely established relationship with colleagues across fraud departments, much of the collaboration happens over telephone or email, which isn't fast enough to keep up with the fraudsters.

Fraudsters have realized that the faster they move the proceeds of payee scams from the original beneficiary or money mule account onto other accounts, the more difficult it becomes for banks to trace and recover the funds. So fraudsters utilize coordinated networks of money mule accounts, and the speed of payments systems, to quickly move the proceeds of fraud using a complex web of transactions spanning multiple banks. This also serves to make identifying mule accounts on their books more difficult, as they appear normal to the typical analytical tools as they are no longer directly connected to the original fraud. The Exhibit below illustrates the complexity of these networks. The proceeds of a fraud from Bank 1 are rapidly dispersed from an account at Bank 3 and sent to a different account at Bank 1.



Examples of the interconnectivity of fraud victims and mules

It shouldn't be underestimated that the complexity of executing these transactions requires significant collaboration and communication between the fraudsters as well. Therefore, it's clear that to adequately address this problem, banks and payment system operators need to match the level of sophistication, collaboration and communication exhibited by the fraudsters. In the UK, Pay.UK, Mastercard and participating banks have successfully proven that applying collaborative systems, beneficiary profiling and large-scale artificial intelligence to interbank payments data can enable participating banks to accurately trace the proceeds of payee scams and shut down the networks of money mules being used to steal consumers' money. Supported by a strong collaboration framework and open communication amongst participants, the intelligence provided to banks enables them to identify the movement of stolen funds as well as the suspect money mule accounts with greater accuracy and efficiency. Banks have been able to enhance their existing strategies with this new intelligence to find mule accounts that were previously hidden, get to other mule accounts sooner in their lifecycle and add an extra component of evidence to their investigations, thus suffocating the mule networks and making the job of the fraudsters that much more difficult and expensive.

Conclusion And Recommendations

Ever since the creation of money, there have been criminals intent on stealing it. Payee scams are currently a preferred method for fraudsters. They often exploit the most vulnerable members of society, but scams have become increasingly sophisticated, capable of duping even experienced businesspeople and investors.

It may not be possible to eradicate fraud completely, and no single solution is likely to prevent payee scams. Instead, P20 recommends payment service providers implement a layered defense. As a first step, a payment service provider should make every effort to understand the problem. The approach to addressing the problem will include:

- implementing accurate, timely reporting;
- educating consumers and businesspeople about scams and how to avoid becoming victims;
- better training for bank employees to help spot potential scams against their customers;
- incorporating user prompts and suspect transaction screens into the payment initiation process; and
- after the transaction, using powerful analytics to trace the proceeds of scams and to identify the accounts of fraudsters.

As long as there are criminals intent on defrauding consumers and businesses, scams will persist. Payment service providers can, however, make a difference. The tools and practices described in this paper, together with our specific Best Practice Recommendations, can help prevent and deter fraud, reducing the pain it inflicts on its victims.

Report Contributors

Working Group Chair: Steve Ledford, The Clearing House

Thomas Aiello, The Clearing House

James Barclay, J.P. Morgan

Jane Barber, NatWest

Liam Cooney, Mastercard

Charles Elliott, Hogan Lovells

Kimberly Ford, Fiserv

Lee Kyriacou, The Clearing House

Emily Reid, Hogan Lovells

Kate Robu, McKinsey & Co

PJ Rohall, Featurespace


About P20

P20 brings together industry leaders, government and regulators to collaborate on and develop solutions to non-competitive issues in the payments industry. 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's key areas of focus are combating fraud & criminal transactions, cyber security and financial inclusion - and on a regular basis, we publish thought leadership and best practice reports on these issues.

Every September, P20 hosts its Global Payments Conference and brings together industry leaders, politicians, government officials, regulators, thought leaders and others to highlight trends, debate industry priorities and shape the future.



 payments20.com

 [P20 - Payments 20](#)

 [@P20payments](#)