EMERGING PAYMENTS ASSOCIATION

# FACING UP TO FINANCIAL CRIME

Analysis of payments-related financial crime and how to minimise its impact on the UK

In association with Barclays, Refinitiv and a syndicate of EPA members


Sponsored by

BARCLAYS

REFINITIV

aimbrain simply smarter authentication

BANKING CIRCLE

Entersekt

NAPIER

Paysafe:

PXP | FINANCIAL

# Financial Crime Matters

Financial crime concerns every company in the payments industry. Because it affects everyone involved in moving money, whether consumers, businesses or governments. And it funds the activities of organised crime groups that seriously affect wider society, such as human trafficking, drug trafficking and terrorist financing.

But while there have been several coordinated attempts to decide what should be done about it, none have been on behalf of the emerging payments sector.

So the Emerging Payments Association has assembled a syndicate to address this. We have commissioned a specialist in payments and financial crime to carry out extensive research and analysis. We have identified what's really going on, by whom and at what cost. And we have developed a set of recommendations for action that are clear, timely and impactful.

Thank you to Barclays, Refinitiv and the other five syndicate members for investing time and resource to make this paper possible. It will enable the emerging payments industry to address the underlying causes of financial crime and protect everyone from the criminals behind it.

**Tony Craddock**
Director General
**Emerging Payments Association**

## About the EPA

The Emerging Payments Association (EPA), established in 2008, connects the payments ecosystem, encourages innovation and drives profitable business growth for payments companies. Its goals are to strengthen and expand the payments industry to the benefit of all stakeholders.

It achieves this by delivering a comprehensive programme of activities for members with help from an independent Advisory Board, which addresses key issues impacting the industry.

These activities include:

- A programme of 70 events annually
- Annual Black-Tie award ceremony
- Leading industry change projects
- Lobbying activities
- Training and development
- Research, reports and white papers

The EPA has over 130 members and is growing at 30% annually. Its members come from across the payments value chain; including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.

## About Huntswood

Huntswood, the commissioned producer of this white paper, aims to drive better outcomes - for its clients and their customers. Huntswood achieves this by combining people, process and technology to deliver practical solutions that help regulated firms deliver high quality services in a cost-efficient way, all while effectively mitigating business risk.

Huntswood is the partner of choice for:

- Resourcing - of the quality and level to get the job done
- Solutions - where they take responsibility for the outcome created

With centres of excellence in Reading and Liverpool, Huntswood is able to take on large-scale projects in-house or otherwise provide robust and tailored outsourced solutions.

This support is provided to firms within financial services, payments, utilities, travel, pharmaceuticals and gaming.

Its Payments subject matter experts bring with them a wealth of industry experience and in-depth knowledge of policies and regulation within the payments and financial services sectors. Huntswood is able to provide advice and support to firms on topics as wide-ranging as legislative change, PSD2, Open Banking, affordability, SM&CR and financial crime.

Firms of all sizes choose Huntswood because of its successful track record of balancing regulatory expertise with end-to-end operational support, backed by technology and service innovation. They value Huntswood's clear view of best practice and execution, drawn from their wide-ranging client exposure.

# Executive Summary

The Emerging Payments Association has produced this white paper to explain the nature of payments-related financial crime and to identify actions that should be taken, collectively by industry players or together with regulators and policy makers, in order to reduce the ability of criminals to exploit payments services and systems as part of their illegal activities.

Sponsored by a syndicate of EPA members led by Refinitiv and Barclays, the white paper addresses the ways that payments services and accounts are abused in order to carry out fraud and money laundering. From this understanding of the current situation, the white paper sets out proposed policy positions for the EPA to advocate for the payments industry and identifies areas for collective action by EPA members and the wider industry. These are summarised in **Table 1.**

| Ref | Theme(s) | Recommendations for EPA to progress |
|---|---|---|
| 1 | Training and Awareness | Promote training and awareness for financial crime staff across EPA membership to strengthen understanding of the importance of their role in tackling serious detriments in society. |
| 2 | Access to Banking | Collaborate with other trade associations to promote the adoption of best practice among PSPs for risk management to comply with financial crime legislation and thereby enable necessary access to banking. |
| 3 | Digital Identity | Engage with the wider payments industry, innovation hubs, government and regulators to play a part in creating a world-leading digital identity solution for the UK. |
| 4 | Transaction Analytics | Support and facilitate approaches within the industry for transaction monitoring analytics, extended across payment types and using a wider range of data sources and analytic techniques. |
| 5 | Information Sharing & Reporting of Financial Crime | Support sector-wide activity to determine the level and extent of information that can be shared by government, law enforcement, and payments companies for mutual benefit, through the use of a common platform and commercial model. |
| 6 | Know Your Customer | Engage with EPA members to create a shared position on developing the case for a global approach to KYC standards. |
| 7 | Know Your Customer | Support and facilitate a collaborative member-wide programme to create minimum standards for due diligence on suppliers of data services. |
| 8 | Know Your Customer | Support and facilitate a collaborative member-wide programme to share models and learnings from analysing customer behaviour that members can use with their own data. |
| 9 | Open Banking | Promote a shared, industry-wide voice, through collaborative training and education, to ensure the public is receiving coherent messages on the security of open banking. |
| 10 | Reporting of Financial Crime | Engage with National Economic Crime Centre and government to facilitate and reward reporting of financial crime by all parties via appropriate groups and channels, and to educate victims about how reporting helps reduce criminal activity. |
| 11 | Effective deployment of technology | Provide education and awareness to align firms' technology investment programmes with the concentrated programme of industry-wide regulatory, infrastructure and standardisation changes scheduled for 2019 and the following 3-5 years. |
| 12 | Effective deployment of technology, KYC & Digital Identity | Provide education and awareness on specialist technology areas through showcasing and collaborating with EPA members involved in those fields. |
| The EPA has set up a Financial Crime Working Group which is already addressing some of these recommendations, and which will track and advocate progress of those identified within this report throughout 2019–2022. The EPA can only do this with the active support and engagement of its existing members, and the wider industry. | | |

**Table 1:** Recommended actions for EPA to progress

## Understanding payments-related financial crime and how it's changing

The white paper analyses in detail the way that criminals use payment accounts in the UK for fraud and money laundering, explaining how payments are compromised across different payment types and channels, leading to a definition of eleven main clusters of the ways criminals exploit payments for crime.

Laundering is carried out through payments including bank transfers, cash and cheques, and transaction laundering via card payments. While estimates are difficult to produce, the National Crime Agency (NCA) recognises that the scale of money laundering through UK banks and their subsidiaries could be "in the hundreds of billions of pounds" each year.

Fraud in payments costs the UK economy over £2.4bn annually. This is £45 annually for every adult in the UK, and 2.0% of the financial services industry's total revenues. Methods of payments fraud include push payments by taking control of another person's account (£150m), tricking a genuine payer to send a payment to a fraudster's account (which could

**"The payments industry needs to use technology collaboratively to strengthen its fight against financial crime, including a common digital identity solution, and large-scale analytics of payments transactions"**

**Tony Craddock, Director General, Emerging Payments Association**

be over £1bn per annum, allowing for current under-reporting), and card-not-present fraud for remote purchases (£310m) in 2017.

Criminals continue to evolve their techniques in the fast-changing payments landscape, targeting the areas which are perceived to be weakest. In some cases, these weak links may be technologies, procedures, new businesses, outsourced services, or simply the customers. Financial crime as a whole changes slowly and tactics which are successful continue to be used and optimised; completely new methods appear rarely.

Many current trends use social engineering. Deceiving customers into making seemingly valid payments or tricking them into disclosing card or security details account for two thirds of payment fraud. To conceal proceeds of crime, money is laundered using multiple instruments for concealment including by mobile app, card and alternative payments. To further hide transactions, increasingly complicated company structures are set up using professional enabler and unverified persons, both in the UK and abroad.

The short-term outlook is unclear. On one hand the EU's revised Payment Services Directive (PSD2) brings in stronger systems of authentication for customers at the point of payment and account access. On the other, the opening up of payment services will introduce a number of other parties to the payments supply chain, thereby increasing the points of attack. This fragmentation is also occurring in the card acquiring and issuing market. Criminals will attempt to exploit any perceived weakness, so industry must find limitations in systems before they do.

## Payments industry structural changes and recommended industry response

Based on the analysis, the white paper makes a set of proposals across areas the EPA considers vital for strengthening the payments industry's approach to tackling fraud and money laundering, and the important role that the EPA can play in this.

The UK payments industry is moving through a period of structural change as a result of PSD2 which came into effect in January 2018. Open banking presents opportunity for further innovation through the introduction of new market entrants, but also presents challenges as market participants assess changing financial crime risks associated with the new environment. Furthermore, the Bank of England has announced its timeframes for adoption of international payment standard ISO20022 as part of its renewal of the UK Real Time Gross Settlement service (RTGS). RTGS renewal and the adoption of the ISO standard across the UK payment schemes represent a significant opportunity to ensure the UK is adhering to latest global standards, offering enhanced interoperability which will assist in more efficient payment transfers, as well as increased capacity to transfer data alongside a payment which will assist institutions in a number of areas including fighting financial crime.

The EPA sees it has an important role in providing know-how on these changes to emerging payments service providers to ensure they are involved in these initiatives. The EPA views that all payment providers have an obligation to maintain the integrity of the payment industry through compliance with relevant financial crime legislation, and this compliance is critical for payments providers to continue to have full access to banking facilities (see recommendation 2). The EPA also considers that payment providers and operators need to deploy up-to-date technology more extensively and collaboratively in defence of their services and customers, aligned with the judgment and knowledge of skilled staff. The EPA is going to be an advocate for members through this period of unprecedented change.

**Digital Identity:** Managing the authentication of users' identity is critical for electronic and digital payments, exploiting developments in biometrics and behavioural analytics. A digital identity in the UK is a core enabler for ongoing take-up of digital services, facilitating both convenience and security for users. The EPA advocates that the financial services industry could work collaboratively to drive a broad consortium of banks, payments providers and operators, innovation hubs, government and regulators to create a world-leading digital

1 National Strategic Assessment of Serious and Organised Crime 2018 - [NCA] 2018

2 Directive (EU) 2015/2366 of the European Parliament and of the Council – [European Parliament and Council] 2015

identity solution. The EPA will look to engage its members in developing a standardised approach that is pragmatic for all players. (See recommendations 3, 12)

**Transaction Analytics:** Machine learning and artificial intelligence techniques are increasingly being applied to payments systems to identify networks of criminals and suspicious payments or account behaviour. Initiatives are under way for analytics across central clearing systems, for example with Pay.UK targeting money-mule accounts for laundering. The EPA is supportive of the Pay.UK initiative and will engage with industry in developing opportunities where the analytical capability could be extended and diversified across payments types and analytical methods. (See recommendation 4)

**Financial crime information sharing:** Enhanced information sharing on known and suspected financial crime across the industry, and with law enforcement, would deliver benefits in enabling greater detection, prevention and prosecution of financial crime. The EPA supports initiatives to share information to tackle financial crime, where the sharing is inclusive of all regulated payments companies. The EPA also encourages its members to engage in the public/private partnership initiated by the Home Office with the industry as part of the SARs (suspicious activity reports) reform programme under way. Shared information services need to be cost-effective for smaller payments providers to ensure a level playing field. The EPA can engage its members in advising on requirements, and on practical operating principles and business models. (See recommendation 5)

**Really knowing your customer:** To really know your customer, companies need to go beyond document checking and analyse their behaviour. By preventing bad actors at account opening and performing ongoing monitoring of customers, payment companies will be better placed to prevent payments financial crime. Machine learning & behavioural analytics build up a model of expected patterns of legitimate payment behaviours and can uncover the increasingly complex networks where criminals hide. The EPA can help promote the appropriate use of their members' specialised technologies, and their members could collaborate to create a network of trusted data sources, shared behaviour models and broadcast events. A drive to develop the case for a global approach to KYC standards is also encouraged. (See recommendations 6,7,8,11)

**Addressing the threats in open banking:** The new environment of open banking offers potential targets for criminals. We highlight social engineering against consumers unfamiliar with 3rd-party providers (TPPs), and targeting of TPPs as aggregators of payments services, for hacking or mule accounts. The EPA's policy approach is to promote a shared, industry-wide voice through collaborative training and education, to ensure the public is receiving coherent messages on the security of open banking. (See recommendation 9)

**Improved Reporting of Financial Crime:** The reporting of cases of payment fraud is uneven and poorly enforced, resulting in a reduced and distorted picture of the impact on UK citizens, businesses and government. The newly formed National Economic Crime Centre will require good case information, data and statistics to fight financial crime effectively and the EPA believes this is critical to the correct focus and allocation of resources. It should be the responsibility of every PSP to encourage their customers to report fraud back to them and the correct authorities. Removal of the disincentives from reporting financial crime is also strongly recommended. This will ensure a comprehensive view of the problem and enable a swift response to changes in criminal behaviour. (See recommendations 5,10)

**Effective deployment of technology to fight financial crime:** In emphasising the role of technology, the report considers aspects of how technology can be effectively deployed. Companies need to invest smartly in technology, fully understanding the busy schedule of regulatory, legislative and industry-programme changes flowing over the next 3-5 years. The EPA could work with its members to provide training and support to promote that longer-term vision and strategic advice that companies require. The EPA can also provide training and awareness on the capabilities of specialist anti-crime technologies through showcasing and collaborating with EPA members involved in those fields. (See recommendations 11,12)

Enhanced technology capabilities need to be complemented by human experience and judgement to have the greatest impact on crime. In this way, payments companies have a vital role in society in tackling financial crime and the organised crime it funds. The EPA should engage with the industry to promote training and awareness for financial crime teams to strengthen understanding of the importance of their role in tackling serious detriments in society. (See recommendation 1). ■

## Call to Action

In recognition of the work already under way across the industry, the EPA, through its Financial Crime working group, with Refinitiv as the benefactor, will prioritise the recommendations that need EPA leadership to progress, and collaborate and engage with other initiatives which benefit the industry and customers by addressing challenges identified in this paper.

**To find out more information on the EPA Financial Crime Working Group and how to get involved, contact Thomas Connelly (thomas.connelly@emergingpayments.org)**

# 2. Contents



# 3. Syndicate Leads

## Barclays - Syndicate Lead

It has never been more important for industry bodies such as the EPA to assist their members in navigating this period of unprecedented regulatory and structural change for the payments industry. I am encouraged to see the EPA's focus on delivery of education, collaboration, and adoption of best practice for its members; all of which help to detect and prevent financial crime and to promote access to banking and the good functioning of the market.

The EPA's call for targeted investment in technology, supported by collaborative, member-wide, programmes that will share analytical models and will provide members with awareness of specialist technology areas is to be welcomed. Technology, supported and delivered through effective public-private partnership, is increasingly important in the fight against financial crime. More broadly the Home Office's review of the SAR regime, for example, will harness analytical technology to enhance the quality of financial intelligence available to competent authorities and the private sector. The launch of Pay. UK's Mule Insights Tactical Solution brings together payments data from multiple banks and overlays it with cutting-edge proprietary analytics and algorithms to build networks of suspected illegal activities, whilst the Bank of England's initiative to adopt international payment standard ISO20022 will deliver new opportunities to assess financial crime risk through by providing PSPs with improved structured payment data.

Barclays believes that Government and regulators should create a policy framework that incentivises all those in the economic crime ecosystem to work together, incentivising firms in the economic crime ecosystem to invest in solutions that protect their consumers from fraud by stopping the fraud occurring in the first place. Industry bodies such as the EPA will play a critical role in this policy effort, by firstly providing clear and consistent communications on the threat of financial crime to PSPs and consumers, and secondly by engaging their members in the successful delivery of initiatives such as the Contingent Reimbursement Model which will further incentivise Payment Service Providers to better protect consumers from Authorised Push Payment Scams. These strategic changes present significant opportunities for industry bodies to collaboratively drive effectiveness and to strengthen the UK's defences against economic crime. Barclays is, therefore, pleased to support this paper and the EPA's policy recommendations.

**Geraldine Lawlor**
Global Head of Financial Crime

**www.barclayscorporate.com**

## Refinitiv - Syndicate Lead

Welcome to this pivotal whitepaper on the changing nature of financial crime, delivered at a critical time of significant structural and regulatory change in the European payments market. In a global economy where less than 1% of the proceeds of financial crime are being identified and seized by law enforcement, it is very clear that the current approach to tackling financial crime needs to be more effective.

While banks and payment players continue to invest in technology to deliver groundbreaking digital products, services and channels, so are the criminals. They circumvent controls, defeat siloed defenses, and exploit vulnerabilities at an unprecedented scale. The problem is that the criminals don't sit through committees, governance processes, regulatory reviews and compliance reviews before they move. They innovate, adapt, replicate and scale at pace, behind (digital) masks, and profit from their actions very quickly, across borders and at massive scale. The aim of this paper is to highlight some of the traits of these digital criminals, and identify opportunities for the industry to work together to take meaningful action to tackle these changing patterns of behavior in an effort to tackle financial crime.

Refinitiv is leading the way in delivering solutions which help financial institutions to tackle money laundering, and financial crime, and we are passionate and vocal about the need for the industry to work together to tackle this abhorrent crime. Through global forums like the Coalition to Fight Financial Crime, launched with WEF and Europol at Davos in 2018, Refinitiv will continue to raise awareness of this issue, and will partner with the industry to solve it.

We hope you find value in reading this whitepaper and remain here to support you in your efforts to address this issue.

**James Mirfin**
Global Head of Digital Identity & Financial Crime Propositions

**Che Sidanius**
Global Head of Financial Crime & Industry Affairs

**www.refinitiv.com/en**

# 4. Syndicate Associates


## AimBrain

AimBrain is an award-winning Biometric Identity as-a-Service (BIDaaS) platform comprising five invisible and visible user authentication modules; 100% biometric, 100% proprietary. Our authentication engine is server-side and based on deep learning, which means that in just a few weeks, we capture 60% more manual fraud at the onboarding stage than an organisation can alone, all with zero changes to the user interface. Our multi-modal approach allows for unique configurations of our passive modules (AimAnomaly Detection and AimBehaviour) and active modules (AimFace, AimVoice and AimFace//LipSync) across any device and any channel. Authenticate the user, not the device.

**www.aimbrain.com**


## Banking Circle – Global Banking Services

Banking Circle is a next-generation provider of mission-critical financial services infrastructure leading the rise of a super-correspondent banking network. Banking Circle empowers financial institutions to support customers' trading ambitions – domestic and global - whilst reducing risk and the operational cost of transactions. By becoming a member of the Banking Circle, financial institutions can offer their customers banking services – from payments to loans – to help them trade domestically and globally, efficiently and at low cost. Importantly they can help their customers improve cash flow through enhanced speed of settlement whilst remaining fully compliant with financial regulation.

**www.bankingcircle.com**


## Entersekt

Entersekt is an innovator of mobile-first fintech solutions. Its goal is two-fold. Firstly, to help financial institutions and other large enterprises secure their customers' digital identities, so that end-users can make the most of the service channels available to them. Secondly, to confer on its customers a competitive edge as their industries transform. With Entersekt's platform in place, organizations can respond to change with agility by confidently launching exciting new digital experiences.

**www.entersekt.com**

## Napier

We are specialists in building Intelligent Compliance Solutions that make it easier and more cost effective for organisations to meet their regulatory requirements. Our cutting-edge solutions for Anti-Money Laundering (AML) and Trade Compliance are used by both financial services firms, and the broader industry sectors. We use AI and Machine Learning (ML) developed in conjunction with academic research that focuses solely on the compliance problems that our applications solve. Using ML in conjunction with user definable rules give the best of both worlds in detection rates, whilst satisfying regulatory requirements. Using both AI and rule based system means that we can significantly reduce false positives whilst increasing the detection rates of false negatives, all in a way that is fully auditable and transparent to the regulator. We provide an Out of the Box end-to-end AML Solution that can be used to augment or completely replace legacy systems.

**www.napier.ai**

## Paysafe

Paysafe is a leading global provider of end-to-end payment solutions. Its core purpose is to enable businesses and consumers to connect and transact seamlessly through industry-leading capabilities in payment processing, digital wallet and online cash solutions. Delivered through an integrated platform, Paysafe solutions are geared toward mobile-initiated transactions, real-time analytics and the convergence between brick-and-mortar and online payments. With over 20 years of online payment experience, a combined transactional volume of US $56 billion in 2017 and approximately 3,000 employees located in 12+ global locations. Paysafe connects businesses and consumers across 200 payment types in over 40 currencies around the world.

**www.paysafe.com**

## PXP Financial

PXP Financial is a complete, omni-channel payment provider that helps businesses to accept payments online and on-premise globally. It offers an online and POS solution, alternative payments, collection services, card acquiring, risk management as well as variety of value-added services: payment pages, reporting, conversion improvement, tokenisation, dynamic currency conversion, instalments and recurring payments across multiple channels.

PXP Financial has many years of experience in the payment business and holds an FCA license in the UK, passported to all EU countries, a Money Transmitter license in the US as well as Mastercard and Visa acquiring licenses. The company processes transactions worth €16bn for more than 1000 merchants annually. PXP Financial has offices in the UK, Austria, Bulgaria, India, Australia and in the US with 250 employees from 25 nations

**www.pxpfinancial.com**

# 5. Introduction

The Emerging Payments Association has produced this white paper to set out the nature of payments-related financial crime in the UK and to identify actions that should be taken, collectively by industry players or together with regulators and policy makers, to reduce criminals' ability to exploit payments services and systems as part of their illegal activities.

## Definition of financial crime

Why are we addressing financial crime and what do we mean by financial crime overall? Financial crime over the last two to three decades has become a significant concern to governments across world. This stems from the direct losses incurred, the serious detriments for individuals and society for example through human trafficking or terrorist financing, and the impact on economic development of societies and on the rule of law. According to a survey in 2018 by Refinitiv, "$1.45 trillion is the estimated aggregate lost turnover as a result of financial crimes, according to the organizations surveyed around the world, representing 3.5% of their global turnover."[3]

According to the International Compliance Association[4], financial crime can be divided into two distinct, though related, areas of activity. Firstly, there are activities that dishonestly generate wealth for those engaged in the financial crime. Secondly, there are the crimes that protect illegal wealth once it has been acquired, for example through laundering.

## Aims and scope for the report

Addressing the payments environment, this report focuses in on the ways that payments services and systems can be abused in order to carry out fraud and money laundering. Payments fraud enables the generation of wealth for criminals by stealing money from the victim. Money laundering across the payment systems, together with breaches of sanctions or ignoring the risks of PEPs (Politically Exposed Persons), enables the movement of illicit funds. The report also addresses customer due diligence activities that should give companies high confidence they understand the nature of their customers' activities and payments.

**Section 6** of the report addresses how payment services and operations are targeted by criminals and the current scale and level of impact. The analysis highlights particular areas where the nature of criminal threats to payment services is changing in the current timeframe.

**"The serious types of detriment include terrorist financing and drug, sex and human trafficking."**

The impacts and implications for tackling these threats are addressed for providers and operators of payments services and payments accounts, firms who provide services to payments institutions to combat financial crime, and for the end users of payments.

**Section 7** presents the key findings of the white paper, across seven key areas of activity vital for strengthening the payments industry's approach approach to tackling payments financial crime. In these findings the white paper sets out proposed policy positions for the EPA to advocate for the payments industry and identifies areas for collective action by EPA members and the wider industry.

Other important considerations in respect of scope for the white paper are:

- It addresses retail and small-to-medium business payment services, meaning all transactions involving consumers or SMEs and the corporates that they transact with
- The analysis includes card-based payments, bank transfer payments, and electronic money (e-money) services. In these we consider the roles for criminals acting either as end-users or as intermediaries (for example as merchants) in the payments journey
- We approach this from the perspective of UK payments service providers, primarily addressing payments which start and/or end in the UK. Nevertheless, as organised crime activity spans countries, we consider where actions on some issues need to be co-ordinated with other jurisdictions
- This report focuses only on fiat currency, not crypto-currencies or other unregulated electronic funds (such as Linden dollars or ISK in Eve Online). We note that further work on payments financial crime could address these stores of value which are not related to fiat currency.

## Importance to society of tackling financial crime

Organised crime groups use fraud and money laundering to fund and facilitate activities which create the most serious types of detriment for society that run opposite to anyone's idea of a just world for all people. These include terrorist financing, drug trafficking, sex trafficking, and human trafficking. (In a worst kind of example, children are being separated from their families and sold to other parties who carry out persistent abuse of them).

**"Payments providers and operators can play a vital role in making financial crime harder to carry out."**

Within the wider financial services industry, payments providers and operators can play a vital role in making financial crime harder to carry out. This mission should be set out clearly and reinforced frequently within payments companies. Hard work to prevent financial crime is not driven primarily by regulatory compliance or by managing to a commercially-driven 'fraud loss' budget. It should be driven by payments providers' responsibility to disrupt, reduce or prevent the fraud and laundering activity that funds serious and organised crime. In the payments industry, this mission can be achieved by co-ordinated activity across payment service providers and system operators, payment scheme, regulators, government and law enforcement. Ongoing training and awareness-raising of the impact of this activity, done well, is essential across these players. ■

**Footnotes:**

3 The true cost of financial crime - a global report [Refinitiv] 2018

4 What is financial crime? - [International Compliance Association]

### ICA (International Compliance Association) definition of 'Financial Crime'

"First, there are those activities that dishonestly generate wealth for those engaged in the conduct in question. For example, the exploitation of insider information or the acquisition of another person's property by deceit will invariably be done with the intention of securing a material benefit. Alternatively, a person may engage in deceit to secure material benefit for another.

Second, there are also financial crimes that do not involve the dishonest taking of a benefit, but that protect a benefit that has already been obtained or to facilitate the taking of such benefit. An example of such conduct is where someone attempts to launder criminal proceeds of another offence in order to place the proceeds beyond the reach of the law."

Source: 'What is financial crime?' International Compliance Association

# 6. Understanding payments-related financial crime and how it's changing

Broadly, financial fraud generates proceeds of crime, and money laundering conceals, moves and manages them. This report focusses on the financial crimes where payments services are abused in order to carry out fraud and money laundering.

Conceptually there are three processes of financial crime related to payments: generation and capture of the proceeds of crime, management of criminal funds, and extraction or re-investment. **Figure 1** below shows that, just like many businesses, cash management is important for criminal organisations

## 6.1 Analysis: "Follow the Money"

Using the investigative principle of tracing money movements, the analysis here focusses on obtaining or moving money in support of financial crime, with transactions which start and/or ends in the UK, in a recognised fiat currency. Criminals take advantage of payments by exploiting one of the elements of trust about a given transaction. These assumptions are that a payment is:

a) authorised by the payer
b) initiated from the correct payer to the correct recipient
c) for a legal purpose
d) not modified after initiation
e) not subject to an incorrect refund or return request and in addition, that systems are secure and operate reliably.

Criminals can attack payment accounts across multiple payment initiation channels, some which are not in the control of any payment provider such as retailer websites and apps.

By analysing payment initiation channels, payment instruments and types of attack **(see Table 2)**, it is then possible to see patterns of common attacks across channels and similar attacks across payment instruments. Grouping these combinations by similarity results in eleven clusters shown in **(see Table 3)**. For

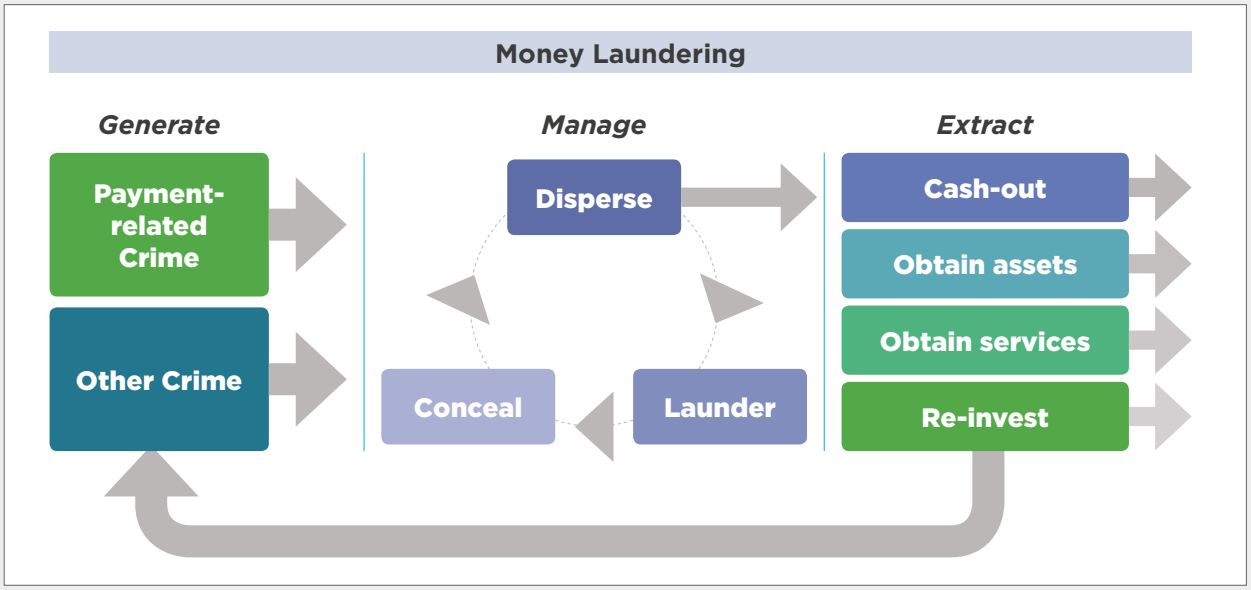



**Figure 1:** The cycle of financial crime

example, money laundering by credit transfers, cheques and cash is broadly similar across all channels. We have therefore grouped these together as "money laundering", whereas illegal payments by payment card is classified as "transaction laundering" as it uses a different method. These eleven clusters of payments-related financial crime are unrelated to any technical considerations.

## 6.2 Counting the Cost of Financial Crime

With many types of crime, it is difficult to estimate the impact, however with payment-related crime there is always a value associated with each payment. This analysis focusses on totalling these transaction values.

While it is worth noting that fraud is not generally disclosed, nor extensively reported to the police, some estimates do exist. This subsection uses data from a number of sources, subsequently verified with financial crime prevention and payment practitioners. In some cases, data sources are unavailable, incomplete or are known to be inaccurate.

In addition, where funds are transferred through multiple transactions, as happens in money laundering and especially money mule networks, it is difficult to understand the figure reported. For example, if £100 is laundered through six sequential payment transactions, is that £100 or £600 of money laundering? And if only two of those transactions are identified as money laundering, the reported figure might be £200.

Better and more consistent reporting will make statistics like these more reliable and ensure that any changes year-on-year are not merely consequences of improvement in the process of capturing data.

| Attack | When | Examples |
|---|---|---|
| **The identity associated with the payment account is false** | Before authorisation | Fake account, synthetic identities, fraudulent account opening |
| **The payment account has been taken over** | Before authorisation | Hacking online banking, phishing via email and SMS |
| **The payment instrument has been abused** | At authorisation | Online card fraud, counterfeit cards, direct debit fraud, subscription fraud |
| **The payment is intentionally misdirected** | At authorisation | Invoice or supplier fraud, director or CEO fraud |
| **The payment is illegal** | At authorisation | Money laundering, terrorist financing, sanctions-breaches, sales of illegal goods |
| **The payment details have been modified** | After authorisation | Cheque interception or modification |
| **The payment account facilities have been abused** | After authorisation | Re-charge fraud, direct debit indemnity fraud, cash withdrawal fraud |

**Table 2:** Examining seven potential routes for attack

### Money laundering and illegal payments

The category of illegal payments covers two distinct clusters: transaction laundering (which uses a card payment to clean money paid from a card account to a merchant, both under criminal control) and other money laundering. These clusters will include payments made from the proceeds of crime to support terrorists, for bribes and making other corrupt payments, and breaching sanctions.

These groups are subject to a requirement on PSPs at least to report any suspicious activity, however it is unclear how the total value of suspicious activity reports (SARs) raised relates to the total value of illegal payments. The National Crime Agency recognises the problem of estimating money laundering:

*"There is no reliable estimate of the total value of laundered funds that impacts on the UK. However, given the volume of financial transactions transiting the UK, there is a realistic possibility the scale of money laundering impacting the UK annually is in the hundreds of billions of pounds"* - National Strategic Assessment, NCA, 2018

**"There is no reliable estimate of the total value of laundered funds that impacts on the UK. However, given the volume of financial transactions transiting the UK, there is a realistic possibility the scale of money laundering impacting the UK annually is in the hundreds of billions of pounds."**

| Cluster | Method |
|---|---|
| **Money Laundering** | Illegal dealing with the proceeds of crime including making payments using credit transfer, cash, direct debit, cheques and transaction laundering |
| **Abuse of payment card** | Abuse payment card, card data or counterfeit cards to make payments |
| **Push payment fraud** | Convince payer to pay an account under criminal control |
| **Transaction laundering** | Criminal merchant and cardholder transactions to wash proceeds of crime or conceal seller |
| **Takeover of bank account** | Takeover account to make a credit transfer (e.g. Direct Credit/SEPA Credit Transfer) |
| **First-party payment fraud** | Dispute payment fraudulently (aka 'friendly fraud') via card, credit transfer, direct debit |
| **Direct debit fraud** | Abuse a 3rd party account to make a direct debit payment |
| **Merchant fraud** | Accept card payments fraudulently (merchant fraud) |
| **Cash** | ATM skimming, intercept cash in post, dispute ATM withdrawal |
| **e-Wallet payment fraud** | Abuse e-Wallet (stored value, not card) for criminal purposes |
| **Cheque fraud** | Modify cheque, intercept cheque, issue cheque, takeover account to issue chequebook, kite cheque |

**Table 3:** Eleven clusters of payments-related financial crime

NCA recognised in 2017 that its previous estimate from 2016 of up to £90 billion is a "significant underestimate"[5].

Transaction laundering[6 7 8], the use of card payments to handle payments for a third party or to transfer and wash the proceeds of crime, is estimated[9] to have been $159 billion in the US in 2016 of total card spend of $3,340billion.

Assuming that proportion is also correct for the UK, that would relate to almost £46 billion of transaction laundering; this is likely to be a high estimate for the real figure but is the only estimate available.

## Card Payments

In addition to general cybersecurity improvements, payment cards have broadly been the focus of industry effort for over 25 years. The Chip and PIN programme was introduced to stem counterfeit card and some lost/stolen card crime, the cards industry has progressively introduced security measures such as the code printed on the reverse of the card to crack down on online card fraud. However, since payment cards can be used globally, these initiatives are partially dependent on the speed of the slowest region. For this reason counterfeit card crime against UK-issued cards was still being undertaken ten years after the Chip and PIN programme had successfully completed in the UK.

Whilst the card schemes record disputes about transactions as "chargebacks", the underlying cause is not always clear. An example is merchant fraud, where an individual sets up a merchant account to receive payment for goods and services they do not deliver. In these cases, the merchant acquirer may be left with a debt[10]. These figures are generally not published by the merchant acquirers and are invisible to card schemes.

Furthermore, some disputes are brought by cardholders fraudulently and in some cases may be successful in obtaining refunds to which they are not entitled. This is known as first-party card fraud.

## Push Payment Fraud

Generally, there are two types of crime related to push payments:

- Hacking into or taking control of an account, then initiating payments
- Using social engineering or other mechanisms to persuade a real payer to make a payment to an account in the control of the fraudster

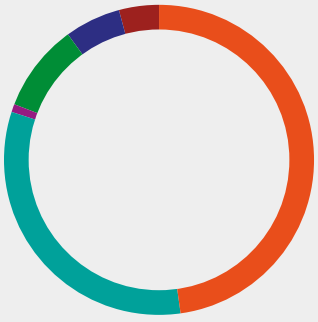



**Figure 3:** Breakdown of goods sold via transaction laundering [Mastercard] 2015

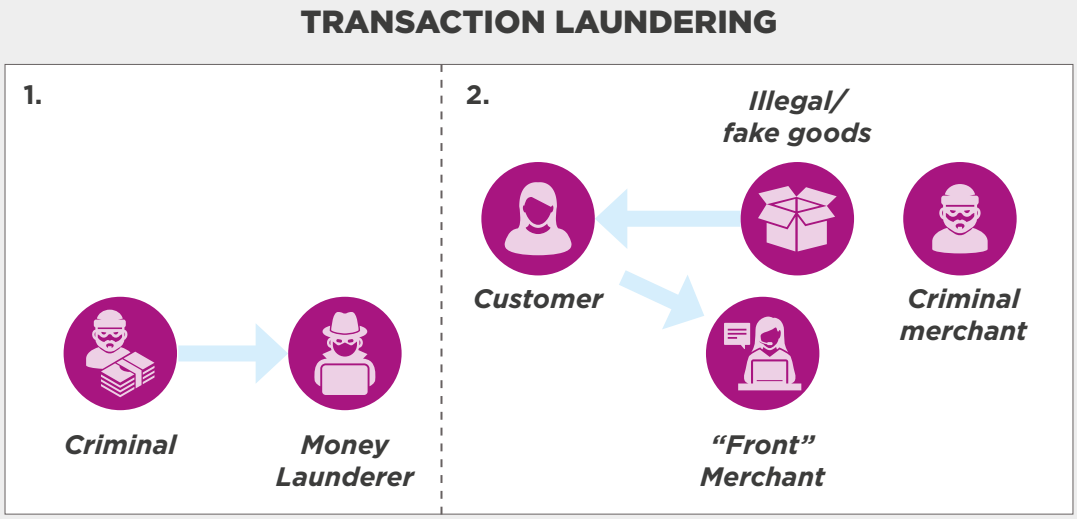



**Figure 2:** The two main types of transaction laundering

Whether the payment is authorised by the account-holder or someone purporting to be them, the account-holder is the victim and may be unwilling to report the fraud, especially if it is a business.

For this reason, the scale of this type of attack has gone unrecognised for many years

### Direct Debit Fraud

The strengths of the Bacs Direct Debit scheme are that it's both easy to use and protects payers in the case of error or fraud. A typical fraud would be for a criminal to obtain a new smartphone handset contract backed by a direct debit for which the fraudster gives a victim's account number and possibly name.

Losses for this fraud are not counted by the industry and the Direct Debit scheme does not measure the volume or value of losses. In financial institutions these claims under the direct debit indemnity are, in general, not handled or reviewed by the financial crime or fraud teams.

The most recent research was a survey conducted back in 2010 by CEBR which estimated the annual losses at £40m. With better reporting, as required of PSPs by PSD2 from January 2019, the industry could soon know the actual losses.

### Cash

Despite the move of consumers to electronic payments, cash remains important in financial crime due to its anonymity. There are a number of cash-payment-related crimes including ATM skimming, false claims of notes not dispensed, recording of a PIN followed by retention or acquisition of the related card, and interception of cash payments made in the post. Cash is still used frequently for money laundering despite being bulky, and large-denomination notes facilitate this.

In addition, the point of transfer from electronic payment systems to physical notes is critical. This area is targeted by criminals who use technology to copy or intercept card information at ATMs. This is also the point where physical attacks on the ATM itself are increasing, such as violent attacks on the machine using explosives or cutting torches[11].

## 6.3 Scale of Payments-related Financial Crime

Financial crime is widely unreported and undetected; as such, metrics for loss and incidence are generally inaccurate and unreliable. The following **Table 4** summarises estimates based on the financial crime clusters.

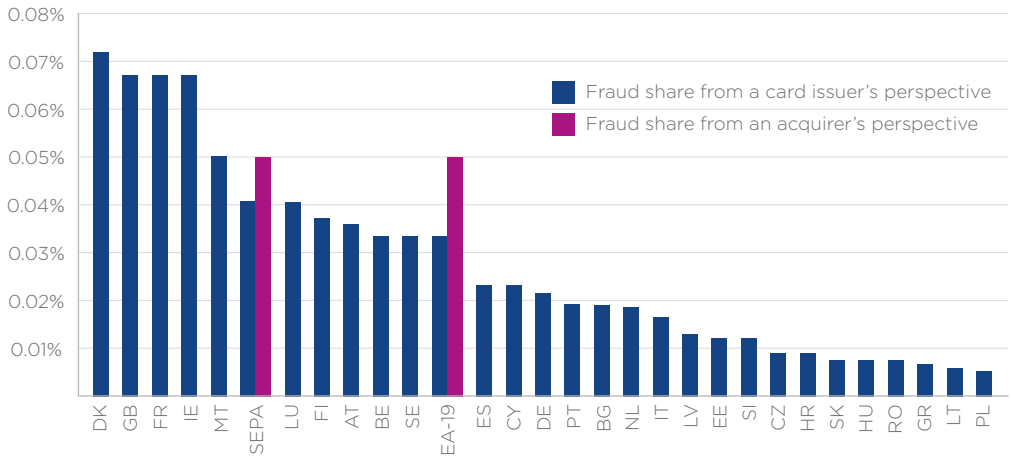



**Figure 4:** The UK has one of the highest loss rates to card fraud in the EU, driven by online fraud. Source: Fifth report on card fraud – [European Central Bank] 2018

| | Cluster | Estimated size £million | Growth indications[12] |
|---|---|---|---|
| **Money Laundering** | Money laundering (including transaction laundering) | 90,000-200,000[13] | → |
| | Transaction laundering | up to 44,100[14] | → |
| **Fraud** | Push payment fraud | 1,200-1,500[15] | ↗ |
| | Payment card abuse | 630[16] | → |
| | First-party payment fraud | c163[17] | ↗ |
| | Takeover of payment account | 150[18] | → |
| | Merchant fraud | 74[19] | → |
| | Direct debit fraud | c40[20] | → |
| | Cash | 19[21] | ↗ |
| | e-Wallet payment fraud | n/a[22] | n/a |
| | Cheque fraud | 9.6[23] | ↘ |

**Table 4:** Estimated scale of payments financial crime

| Type of Financial Crime | Refinitiv Global Estimate for Loss as % of turnover | UK estimated loss as % of turnover | UK estimates £ billion |
|---|---|---|---|
| **Fraud** | 2.5% | 1.9% | 87[27] |
| **Bribery and Corruption** | 3.2% | 2.9 - 5.3% | 136 - 246[28] |
| **Money laundering** | 3% | | |

**Table 5:** Losses due to financial crime extrapolated from Refinitiv's report 'The True Cost of Financial Crime'

## 6.4 Comparison with global rates of losses to financial crime

Payments-related financial crime is a proportion of all financial crime and there are variable estimates. In Refinitiv's study[24] "The True Cost of Financial Crime", the survey establishes general loss rates as a percentage of turnover globally for fraud, bribery/corruption and money laundering which are given below.

The total turnover for businesses in the UK is £3,861 billion[25] and public sector spending is estimated at £800.4 billion[26], giving an estimate of £4,661 billion total UK turnover.

Comparing these UK estimates of loss with the Refinitiv global estimates, see Table 5 suggests the UK may be doing a little better (as much as 20% smaller losses). However, tackling incompleteness and inconsistency of detection and reporting is required for better and more robust statistics.

**"The total turnover for businesses in the UK is £3,861 billion and public sector spending is estimated at £800.4 billion, giving an estimate of £4,661 billion total UK turnover."**

## 6.5 The changing nature of payment-related financial crime

Criminals are strongly motivated to adapt their methods and targets for fraud and money laundering. This section considers these changes in addition to the impact of payment industry initiatives, with further analysis and recommended actions outlined in **section 7.**

Industry experts and practitioners are clear on two points: criminals exploit what is perceived as the easiest to exploit - the "path of least resistance" - and never stop creating new ways to develop current methods. Social engineering, one of the techniques used to circumvent security, is used to bypass technological measures, educating customers and staff on whom to trust is therefore vital. Regulation has a role to play in driving up standards and mandating good practice, but industry-originated initiatives are important, built on consensus and collaboration. The EPA can play a vital role in lobbying for, shaping and delivering

some of these proposals, which are described and listed in **section 7.**

A number of significant trends are explored in the rest of the section.

- **Authorised push payment scams**
- **Mobile app-based laundering**
- **Social engineering**
- **Threats in the Open Banking environment**
- **PSD2 Strong Customer Authentication**
- **Ultimate Beneficial Owner Concealment**
- **Fragmentation in the payment card value chain**

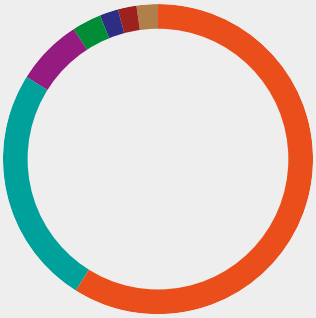
## Authorised push payment scams

One disturbing trend is the growth of fraud by persuading consumers or businesses to make payments directly to criminal accounts. This has existed for at least ten years, certainly since a fraudster convinced Condé Nast to pay bills of $8m from their printer to an unrelated account in 2011[29]. This set of scams may be known as invoice fraud, CEO fraud, supplier fraud and many others, and is frequently enabled by social engineering across mainstream digital communications platforms and financial services channels (see social engineering section, below). The problem was becoming sufficiently acute that the consumer association Which? raised a super-complaint with the Payment Systems Regulator (PSR) in 2016.

Industry reports[30] put losses to this second type of crime at £236 million per annum in 2017, the first year for which a figure was reported. Because banking providers typically report only fraud which is compensated, these figures are widely believed to be an underestimate and may not contain unreported fraud affecting some consumers, SME and corporate customers. It is widely believed that the true figure is over £1 billion, with a sizeable proportion lost in the corporate or government sector.

Indications are that this crime is increasing, but the industry is taking action. An operational code of practice[31] which has been developed has stopped at least £25m of fraud losses according to the City of London Police, but there is a way to go yet. Similar to commercial solutions[32] launched over eleven years ago to tackle an almost identical problem in Direct Debit, Pay.UK is developing a new Confirmation of Payee service to tackle the problem. This is intended for launch in mid-2019 and should have an almost immediate effect on this type of fraud. However, some industry professionals believe that the protection the new service offers may be only short-lived as criminals could work out how to avoid being detected and further measures may need to be taken. In a further measure to tackle push payment fraud, the FCA and industry have been working via the PSR's 'Authorised Push Payment (APP) Scams Steering Group' to introduce a contingent reimbursement model to aid in resolving cases where customers have been victims of push payment scams, which will exist alongside the dispute resolution approach set up for open banking.

### Breakdown of losses to payments financial crime not related to money laundering



| | |
|---|---|
| Push payment fraud | 59% |
| Payment card adbuse | 25% |
| Takeover of payment account | 7% |
| Merchant fraud | 3% |
| First-party payment fraud | 2% |
| Direct debit fraud | 2% |
| Cash | 2% |

### Increasingly sophisticated attacks on PSPs

- A digital bank described a recent fraud attack it had suffered, demonstrating the high level of organisation and capability of the financial crime group.
- The fraudsters set up a copy of the bank's website and online banking login screen, using a website name very similar to the bank's genuine name. This required them to set up a web site with an Internet Service Provider with a domain name from a registrar.
- A user's login credentials were recorded on their site, before the user was redirected seamlessly to the genuine bank website.
- The fraudsters could then login to the user's account minutes or hours later, and initiate payments to accounts in their control. For security, these payments triggered a one-time password to the user's phone; the criminals phoned the user and duped them into revealing the password on the pretext of verifying their identity.
- To drive traffic to their site, the criminal group paid for key-word search results for the bank's name, which required the group to operate an AdWords account with Google.
- Sophisticated criminal projects, such as this one utilising multiple service providers to deliver seemingly genuine services, are on the rise.

## Mobile app-based laundering

Transaction laundering, used to launder the proceeds of crime or conceal the seller, has been in existence for many years. The emerging trend is for this to be done via criminally developed apps on mobile devices where in-app purchases, purporting to be additional content, options or functionality, are used instead of goods. The increased difficulty for fraud prevention is that the criminal behaviour may be almost indistinguishable from users of genuine apps. The weak link is the ability to obtain a merchant facility, directly or indirectly, which calls for good implementation of merchant due diligence[33] which is addressed in **section 7.5.**

## Social engineering

Persuading people to bypass processes or disclose information is not new but the term social engineering is recent. In addition to the social engineering used to facilitate authorised push payment scams, the technique is also being used in increasingly sophisticated ways to take over payment accounts, obtain bank account credentials and abuse payment cards. Paradoxically, the increase of payment card security in the US, which has meant the decrease in counterfeit card fraud, has resulted in increased online card fraud in both the US and the UK.

Social engineering is also increasingly used to compromise security measures introduced to keep payment accounts safe. One-Time Passwords sent via mobile devices are a major target and it is not just payment providers that criminals attack. Social engineering is used with mobile operators' customer support systems online, in-store and over the telephone to perform a "SIM swap"[34] or account takeover in order to intercept SMS messages sent by banks. This is forecast to increase even further as these security measures become more prevalent. One aggravating factor is that consumers are poorly educated on security and tend to trust without thinking. A number of social engineering methods require the credibility or access that large-scale social media firms, search firms, and telecoms providers can provide. This enables fraudsters to make their scam convincing enough that it will dupe a majority of customers. This might include setting up close copies of a bank's website, accessing data via social media accounts, or diverting online search results to a fraudulent website. The ecosystem for payments financial crime includes major technology providers. The industry along with government and regulators could explore further how technology providers might be included in activities and regulatory requirements for tackling payments crime.

## Threats in the Open Banking environment

The UK's open banking environment[35] has a central aim to open up the market for new payment services and a wider range of providers. New categories of regulated payment providers (AISP & PISP[36]) allow fintechs, established banks and other players to create new value propositions for customers. They do this by combining their own technology with customer data and payment services from existing current account providers.

It is up to the payments industry to ensure that criminals do not exploit the open nature of the platform, by considering both regulatory and technology aspects. Even if open banking and its rails may have the necessary protection, external vulnerabilities may move across to open banking as it provides access to existing services. Consumers may also be more easily exploited because the facility is new and unfamiliar.

One potential example of this is social engineering consumers' account credentials. Consumers who have been conditioned to share sensitive account information only with their bank, are now being allowed to disclose it to some third parties.

Whilst the open banking workflow is to provide your credentials on your own bank's website, consumers will get used to having third parties acting on their behalf and having their data, so these TPPs have to be trusted.

With the TPPs as aggregators of payment services, cybercriminals and launderers are likely to be attracted. Hackers will see them as a single point of information rather than attacking the bank directly, and criminals looking to distribute proceeds of crime will be attracted to the ease of connectivity and access to many accounts.

In light of these threats, there may need to be more discussion about how the contingent reimbursement model (see section on Authorised push payment scams, above) addresses sharing of liability with third-parties such as payment initiators (PISPs).

We acknowledge this requires a balance to be struck between having low barriers to entry to enable small or new-entrant PISPs to launch services, and on the other hand protecting ASPSPs from losses that could come from payments initiated through PISPs without ASPSP involvement.

We address the above concerns in **section 7.6** which touches upon education, technical standards and collaboration.

## PSD2 Strong Customer Authentication

A development that is expected to reduce fraud losses is the introduction of Strong Customer Authentication by September 2019. This is the enforcement of multi-factor authentication for many payment-related transactions including logging into accounts, initiating payments and most remote account actions. Some payment providers have already been trialling multi-factor and biometric technologies with success to authenticate their customers, although earlier iterations led to abandoned transactions as was seen when 3-D Secure was introduced. Industry and the regulators are awaiting eagerly the



**"Hackers will see them as a single point of information rather than attacking the bank directly, and criminals looking to distribute proceeds of crime will be attracted to the ease of connectivity and access to many accounts."**



**"Even if open banking and its rails may have the necessary protection, external vulnerabilities may move across to open banking as it provides access to existing services. Consumers may also be more easily exploited because the facility is new and unfamiliar."**

outcome of this legislative approach to security and the adoption of new standards. The payment card schemes, participating through EMVCo, have updated the 3-D Secure specification, used to secure e-commerce payments, to enable card payments to meet the requirements of Strong Customer Authentication. Support for 3-D Secure 2 will be mandated for EU PSPs in 2019 to support biometric and multi-factor authentication and fight fraud in the web and mobile environment.

## Concealment of Ultimate Beneficial Owner

With increasing international collaboration, criminals are becoming more adept at concealing the real controller of assets and money, the Ultimate Beneficial Owner (UBO). As part of its Mutual Evaluation Report (MER), FATF rated the UK as partially compliant[37] in being able to produce adequate and timely records that identify UBOs.

Making opening a business simpler has allowed criminals to conceal their identities and create complex structures via fiduciary services, nominee shareholders and shadow directors. These practices are identified as problematic in a different FATF report from this year[38] which focussed specially on UBO concealment.

In the UK, there is also concern over the amount of due diligence Companies House does before registering a new business. Indeed, the MER also recommended that Companies House should screen for sanctioned entities and individuals and share this information as appropriate. (The use of digital ID in tackling this is touched upon in **section 7.2**). Cross-border relationships can also be problematic with other countries having a similar lack of integrity in their data.

Additionally, when businesses open payment accounts, the payment service providers are responsible for complying with AML/CTF guidelines, but where a PSP's controls are insufficient, highly complex ownership hierarchies can hide criminal activity.

Being able to verify the UBO through links in the chain of companies is vital to the fight against financial crime and PSPs are obligated to understand a company structure before approving it. We also explore solutions in **section 7.5** where technology-driven KYC solutions can apply equally to consumers and businesses.

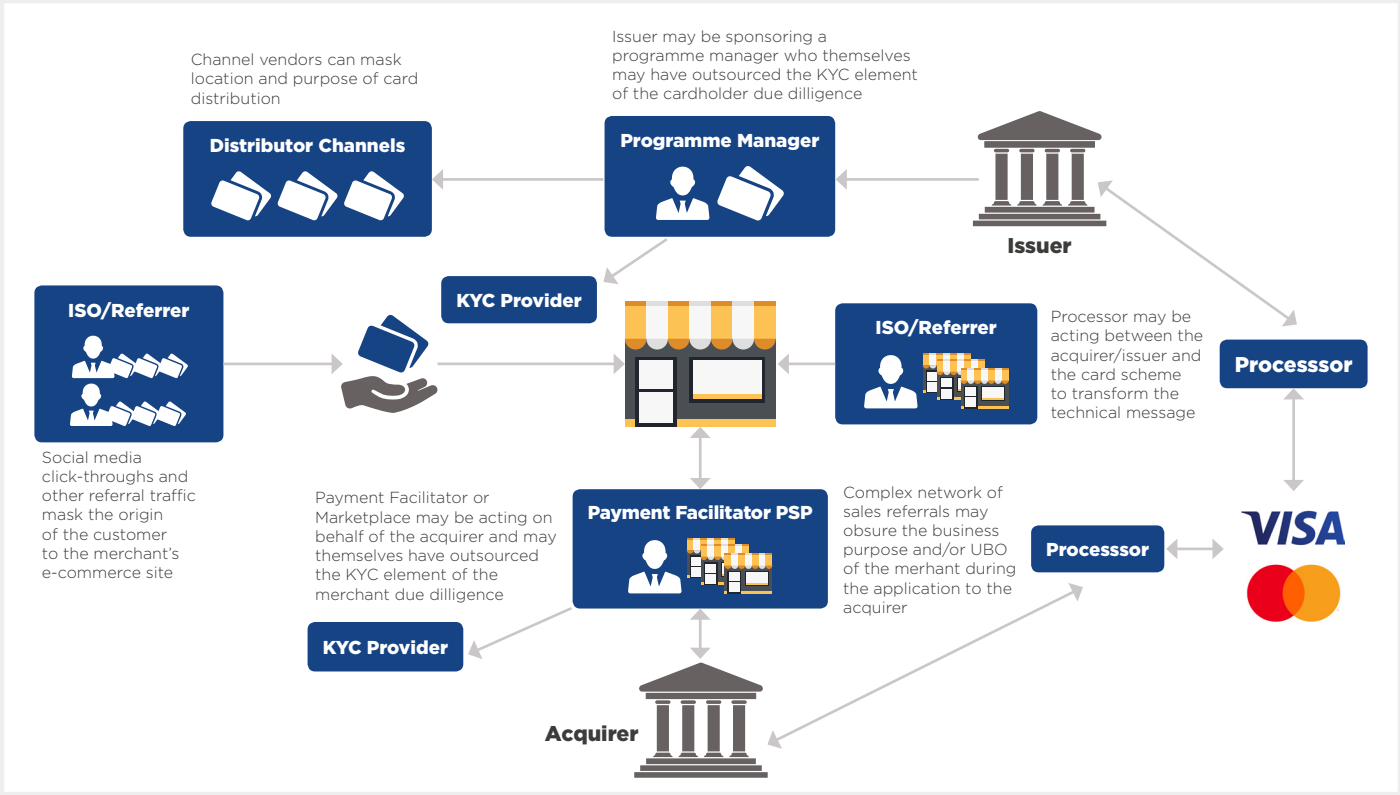
Regulation will still continue to play its part though; the EU's Fourth Anti Money Laundering Directive (AMLD) introduced a central UBO register to identify UBOs of companies and trusts, which will be made public with the 5th AMLD, subject to legitimate interest. The 5th AMLD will also extend beneficial ownership reporting requirements to any legal arrangement that is similar to a trust, although this is not due to come into force until January 2020.

## Fragmentation in the payment card value chain

Criminals continue to target the weakest links in the chain. In many cases these are the consumer and businesses who use payment products, but in some cases these weaknesses are in the value chain of payment services, notably in the card payments arena. Over the last decade a number of additional organisations have inserted themselves into payment processing, both on the acquiring and issuing sides (see figure 6). These potentially introduce weaknesses, for example data not being made available to other parties, transactions being manipulated so as to be approved or due diligence being obstructed.

There are three weak points being increasingly compromised, where improved KYC (addressed in **section 7.5**) can improve matters greatly:

- Independent sales operations: Businesses which assist in onboarding merchants may fail to disclose relevant information to the acquirer or facilitate multiple applications across the same or different acquirers, known as load-balancing;




- Payment Facilitators and Marketplaces: Businesses which collect card payments on behalf of multiple sub-merchants whose details may not be adequately checked. These can also conceal load-balancing;
- Programme managers: Sub-issuers that offer branded cards in conjunction with a real issuer. These cards may be distributed in unapproved countries and with poor processes to check customers' details, meaning that card fall into the hands of criminals who are able to obscure their location.

Involving other parties means that due diligence on their operations is required. The trend to involve more organisations in the commercial and technical relationships increases the risk and burden of regulatory compliance. This is an area of growth and acquirers and issuers should continue to keep standards high. ■

**Figure 6:** Parties in the increasingly fragmented cards ecosystem

**Footnotes:**

5 National Strategic Assessment of Serious and Organised Crime - [NCA] 2017

6 Transaction Laundering is the New, Advanced form of Money Laundering - [Evercompliant] 2018

7 The growing threat of transaction laundering - [Thomson Reuters] 2018

8 Why transaction laundering is turning into a huge financial blindspot? - [FT Alphaville] 2018

9 What is transaction laundering and what is the Industry doing about it? - [Payment Cards and Mobile] 2018

10 As an example, like many merchant acquirers, WorldPay states "Fraud by merchants or others could have a material adverse effect on our business". 2017 Annual Report and Account - [Worldpay] 2017

11 Victimless Crime - The true impact of ATM crime on UK communities - [Cardtronics] 2018

12 Interviews with practitioners in financial crime prevention as part of this white paper [©EPA] 2018

13 EPA estimate based on National Strategic Assessment of Serious and Organised Crime - [NCA] 2017, 2018

14 Estimate based on US proportion of e-commerce [© EPA] 2018

15 Research interviews as part of this white paper [© EPA] 2018

16 Fifth Card Fraud Report - [European Central Bank (ECB)], 2018

17 Estimated from data provided by payment scheme and Fifth Card Fraud Report - [ECB] 2018. Note this value is included in the abuse of payment card estimate above.

18 Fraud, the Facts - [UKFinance] 2018

19 Estimate extrapolated from Fifth Card Fraud Report - [ECB] 2018. Estimate based on average merchant acquirer incremental fraud rates for SEPA zone of 0.008%

20 CEBR research, 2010, informal industry estimates, 2018.

21 Fifth Card Fraud Report - [ECB] 2018

22 E-Wallet fraud is generally handled internally by the e-money provider and therefore unreported.

23 Fraud, the Facts - [UKFinance] 2018

24 The true cost of financial crime – a global report - [Refinitiv] 2018

25 Annual Business Population Estimates for the UK and Regions in 2018 - [UK Department for Business, Energy and Industrial Strategy] 2018

26 Public Spending Details for 2018 - [UK Public Spending] 2018

27 Annual Fraud Indicator [UK National Fraud authority] 2012. The £73 billion loss to fraud in 2012 has been increased in line with total UK spending increases.

28 Money Laundering and Transaction laundering. See Table 3.

29 Supplier Payment Fraud: How it Happens And How to Avoid it - [Sarah Fane, SharedServicesLink] 2016

30 Fraud the Facts - [UK Finance] 2018

31 Banking Protocol Prevents £25m in Fraud and Leads to 197 Arrests - [City of London Police] 2018

32 Bacs lists approved solutions that prove ownership of account, for the purposes of setting up a Direct Debit.

33 Three Types of Merchant Fraud: A Guide For Merchant Acquirers - [Finextra] 2017

34 SIM Swap is the practice of persuading a mobile operator to issue a new, duplicate SIM card for an existing phone to an address in criminal control.

35 What is Open Banking? [Open Banking Ltd]

36 Glossary of Open Banking terms [Open Banking Ltd]

37 Recommendations 24 and 25, Mutual Evaluation Report of the UK, 2018 [FATF]

38 Report into Concealment of UBOs [FATF]

# 7. EPA recommendations for industry action to tackle financial crime

## 7.1 Introduction

Building on the research and analysis in **section 6**, this section sets out seven priority areas for action by regulators and government, by the whole payments industry, or collaboratively by the EPA members. These recommendations and industry initiatives will strengthen the capabilities of payments companies to reduce payments-related financial crime.

It is clear from research for this report that payments service providers and payments systems operators are positioned to play critical roles in the fight against financial crime. They can directly stop fraudulent and laundering transactions from being executed across the services they provide.

Secondly, they have direct information on the nature of payments activities being carried out and can use advanced analytics to drive insights from this data, which can be shared across industry and with law enforcement.

Thirdly, providers can engage actively with law enforcement to assist in pursuit of wider networks of criminals rather than focus just on stopping the rogue activity inside their own operation.

Many of the ways criminals abuse payments services depend on exploiting advanced technologies, for example targeting the digital channels for remote interaction, or by understanding the complexity of the payments supply chain across many companies' systems. In return, the industry needs to use technological capabilities more extensively in defence of its services and customers, aligned with good judgement by staff to make the right decisions on how to deal with suspected criminals.

As a major theme, the report proposes that the industry should collaborate in deploying technology that can play a strong role in fighting fraud and laundering, allied to the right staff capabilities and judgement:

- digital identity and biometrics, to provide identity verification and authentication for customer on-boarding, customer authentication and transaction authorisation;
- transaction monitoring and analytics to identify and monitor suspicious or rogue transaction activity or behavioural changes throughout a user's session;
- sharing of financial crime information on known and suspicious

activities, within the industry and with law enforcement;

- enhanced customer due diligence to really know your customer, to understand in depth the nature of a customer's activities and their source of funds;

- effective protection in the open banking environment, with an extended range of parties involved in mainstream payment services;

- improvements in reporting of financial crime, to provide a true and comprehensive view of the current situation and trends.

Supporting all the specific proposals in this section, there is a clear theme for closer collaboration between payments companies, and closer engagement between the payments industry and law enforcement.

Payments companies and their services are a core target for serious and organised crime groups. A payment provider acting alone can focus on stopping suspicious transactions as they occur or focus on one particular customer's activities. Closer engagement with law enforcement would enable broader and forensic assessment of a wider network of activities, in turn enabling a larger set of criminal players or activities to be monitored and dealt with, based on strong evidence.

The introduction section of this report describes the vital role that payments providers and operators should play in protecting society from financial crime and its wider implications, for example, in human trafficking, drug trafficking and terrorist financing. Payment service providers therefore have an obligation to maintain the integrity of the payment industry through compliance with all relevant financial crime regulations – both for their own systems and knowing their own customers, and related to the financial services they consume, such as banking facilities, from other providers. (This aligns with the EPA's objectives for enabling access to banking facilities through its Project Banking Access).
More broadly for payments companies, the commitment to tackling financial crime is about fulfilling their role in society, and not solely about regulatory compliance or managing to a commercially-driven 'fraud loss' budget. Ongoing training and awareness-raising of the societal importance of this activity, done well, is essential across all payment organisations.

**EPA Recommendation:**
*Promote training and awareness for financial crime staff to strengthen understanding of the importance of their role in tackling serious detriments in society.*

**"A final underpinning theme is the need for ongoing targeted education and awareness for customers."**

**EPA Recommendation:**
*Collaborate with other trade associations to promote the adoption of best practice among PSPs for risk management to comply with financial crime legislation and thereby enable continued access to banking facilities..*

A final underpinning theme is the need for ongoing targeted education and awareness for customers. The methods criminals use for fraud attacks and money laundering change continuously, and customers need frequent repetition of messages to achieve high-levels of awareness. In addition, there is a demographic flow of new payments users into the market each year as young people start to manage their own finances. Despite the competitive pressures for customer experience and convenience, it is essential that users know how to protect themselves. Customers need to appreciate that payments providers put in place anti-fraud measures for their customers' own good, despite the additional checks and friction these may introduce.

## 7.2 Digital Identity: an industry approach

Compromise of identity is a central factor in many types of payments financial crime, which allows criminals to misuse payment services to obtain funds, goods or services fraudulently, to deposit or move illicit funds, or to evade sanctions. Identity-based payments fraud include card-not-present e-commerce transactions (£310m losses in 2017[39]), direct debit mandate fraud (both target the identity of the payer) and push payment scams (£236m losses in 2017[40]) which target the recipient's identity. With laundering, the difficulty of identifying either the payer or recipient is a weakness that launderers exploit.

The UK is world-leading in financial services, and in fintech innovation. The payments industry itself innovates ambitiously in electronic/ digital payment services, providing greater speed and convenience for users.

The industry also needs to innovate to keep customers safe, delivering secure payments. At present customers are exposed to risks of identity abuse without having the tools to protect themselves fully.

The UK risks falling behind other countries in its limited and fragmented approach to digital identity. A coherent approach to managing digital identity is required across the payments industry (and financial services) to provide a fully digital approach for identifying and authenticating customers throughout their lifecycle. This is a particular need for remote or digital channels, but should apply across all payment channels.

The financial services industry should work collaboratively to drive a broad consortium of banks, payments providers and operators, innovation hubs, government and regulators to create a world-leading open digital identity solution.

This would define and build on agreed industry standards[41], together with defining operating models and codes of practice, for how payments providers manage digital identity verification and authentication for customer on-boarding, customer authentication and transaction authorisation. Government support would underpin this as a vital area for facilitating the digital economy.

Payments firms would be responsible for meeting the standards, deciding on their own operational approach. The EPA could engage through its members to advise on a standard approach that is appropriate and pragmatic for firms of different sizes and roles across the supply chain

**EPA Recommendation:** *Engage with the wider payments industry, innovation hubs, government and regulators to play a part in creating a world-leading digital identity solution for the UK.*

Different potential architectural approaches and business models exist. In one example, specialist providers of digital identity could then establish themselves, whose role is to assure the authentication of a service user to payments providers as their client.

### The common components of identity management, irrespective of company, customer-type or payment service/channel

- Identity information gathering: the user asserts an identity based on a set of identity-related attributes
- Identity proofing: independent checking of identity attributes to establish that an asserted identity is valid
- Identity verification: connecting the validated identity to the user claiming it
- Identity assurance: establish a usage profile of the identity
- Authentication: risk-based mechanisms for the user of an assured identity to authorise transactions (or other account activity) securely
- Secure transmission and storage of identity attributes

The successful approach needs to be based on a commercially viable model for digital identity services, designed around compelling consumer use-cases, enabling widespread take up. Payments & financial services providers need to be at the forefront of defining the requirement, while ensuring the approach is valid for other key sectors, for example healthcare and aviation. Interoperability at domestic and international levels is a key consideration.

There should be proportionate regulation of identity providers, reflecting the vital nature of the service and building close co-operation with law enforcement and legal sectors.

We support the industry's goal to confirm payee details more strongly in electronic payments.

**"The financial services industry could work collaboratively to drive a broad consortium of banks, payments providers and operators, innovation hubs, government and regulators to create a world-leading digital identity solution."**

The commitment to 'confirmation of payee' (CoP) capability is a valuable step forward to be introduced in mid-2019 to protect customers against mis-directions and push-payment scams. Looking ahead, as open banking services grow, there need to be measures to give customers confidence that the receiving account is the correct one when triggering a bank-transfer payment to a merchant on an app or website.

For businesses using payments services, there are initiatives to make more extensive use of Legal Entity Identifiers (LEIs) in transactions between companies, to reduce the opportunity for payments to be fraudulent. Furthermore, following the FATF evaluation of the UK's anti-money laundering regime, the Government's recent Serious and Organised Crime Strategy[42] publication commits to improving the accuracy and integrity of the register held by Companies House, building on steps already taken to improve sharing between Companies House and law enforcement.

We acknowledge that initiatives on digital identity need to be addressed in ways that are aligned with cultural, societal and political attitudes, for example concerning the relationship between citizens and government, and the protection of personally identifiable information (PII).. The emphasis is to facilitate the digital economy by improving convenience and security for service users.


## BankID in Scandinavia

BankID is an electronic identification ('eID') issued by banks in Norway, Sweden and Finland which can be used for payment authorisation, and more broadly by banks, government agencies and other providers to confirm agreements with individuals via digital channels. In Sweden 8 million people use BankID, and over 95% of Swedes aged 21-50 have a BankID[44]. In Norway, 4 million people have BankID.

BankID is deployed primarily on smartphones, but also works on a card, or on a PC disk. The smartphone BankID enables the smartphone to be used as a standalone authentication device for accessing apps and browser-based websites. Instead of having to remember numerous usernames and passwords, it means users only need to remember one password to access all (participating) services.

### SAR definition

A Suspicious Activity Report (SAR) is a piece of information which alerts law enforcement that certain client or customer activity is in some way suspicious and might indicate money laundering or terrorist financing. The submission of SARs is a legislative requirement in relation to anti-money laundering and combating the financing of terrorism.

The UK Financial Intelligence Unit (UKFIU) has national responsibility for receiving, analysing and disseminating financial intelligence submitted through the SARs regime. The UKFIU provides the gateway to reporters and a repository of data to inform law enforcement.

Suspicious Activity Reports - Annual Report 2017 (NCA, 2017)

### Biometrics and behavioural analytics

Effective management of digital identity is inherently a technology-led capability, where biometrics and behavioural analytics can have a huge impact in disrupting the current methods that criminals use. Biometric recognition is defined by the International Standards Organisation as the "automated recognition of individuals based on their biological and behavioural characteristics"[43], and is centred on inherent personal characteristics for an individual. Consumer services today widely use facial images or videos, voice or fingerprints to provide greater confidence in authenticating users.

Furthermore, behavioural analytics can include assessing how the customer is moving through the screens of an app and comparing to other authenticated customers, or to known characteristics of criminal usage. These can be combined with other data points from the phone on battery life, location, or angle of tilt during usage.

Multi-modal biometrics is a further advance, whereby authentication systems are based on a combination of different biometric measures. This could be the capture of two individual factors, such as a fingerprint and face or voice, but technology is evolving to combine multiple biometrics into single authentication stages, such as 'face plus audio' with random challenges and lip synchronisation analysis to confirm it's a real person. This is harder to compromise at authentication, though a critical requirement to avoid compromise is to capture the different biometrics at one stage during on-boarding.

Inclusivity is an important consideration, allowing all users to benefit from this convenience and protection. With multi-modal biometrics, the user can have choice of biometric features that she/he wishes to use, extending applicability to people with different or restricted physical capabilities.

The EPA will establish a member-led working group to showcase developments in biometric and behavioural analytics technologies, and advocate its members to understand fully the operational approaches and benefits available in tackling payments crime. (This policy recommendation is covered in **section 7.8**)

## 7.3 Transaction Analytics

Machine learning and artificial intelligence techniques are increasingly being applied to large, complex datasets to solve problems in many fields. Some of these tools have been used to predict payer behaviour for over 20 years, but with the increase in computing power and storage these are now being applied to ever larger databases. Identifying networks of criminals and irregular payments is a suitable application, however each PSP is limited to its own narrow view of the whole set of transactions.

The Payment Strategy Forum, formed by the PSR, recognised in its Strategy in November 2016[45] that analysing payments transactions between all PSPs across a time period would be a powerful tool in the detection and prevention of financial crime. For the first stage of implementation, Pay.UK worked with infrastructure supplier Vocalink, a Mastercard company, to provide an innovative network-level anti-money laundering and mule account detection service. This service (Mule Insights Tactical Solution) enables suspicious payments to be tracked as they move between payment provider accounts. This is irrespective of whether the payment amount is split between multiple accounts, or if those accounts belong to the same or different financial institutions. This service creates a visual map (dispersion tree) of where and when money has moved, providing data-driven insights and new intelligence for financial institutions to act on quicker than ever before.

The EPA is supportive of this initiative and will engage with industry in developing opportunities where the analytical capability could be extended and diversified across payments types. Criminals who find their inter-bank payments are tracked will use transfers using other payment mechanisms to conceal the flow of funds. In addition, with one analytic approach in place they may be able to develop measures to conceal some of their transactions.

It is therefore suggested that broader data sets should be sourced from multiple payment instruments (including cross-border payments, to or from Europe and beyond) and analytic capability extended to support the development of innovative techniques by multiple providers of analytics. This will avoid a systemic risk and will prevent criminals gaming the analytics system. The approach of bringing together data and analytics to a secure, central set of resources, is one model that the EPA believes would ensure both continued progress and reliability.

**EPA Recommendation:**
*Support and facilitate approaches within the industry for transaction monitoring analytics, extended across payment types and using a wider range of data sources and analytic techniques.*

## 7.4 Financial Crime Information Sharing

The opportunity exists for enhanced information sharing on known and suspected financial crime, supporting closer working between industry, law enforcement and government. This would include more payments providers outside credit institutions, and would deliver benefits in enabling greater prevention, detection and prosecution of financial crime. Furthermore, legitimate customers would experience less friction in carrying out their payments; and society overall would benefit from more effective prevention. For tackling payments fraud, some parts of the industry have in place mechanisms for sharing information, for example through CIFAS and UK Finance. These have typically been constrained to confirmed cases and held in separate databases to protect data access, and participation is restricted to members paying a subscription. For sharing information on money laundering, the industry is required to submit suspicious activity reports (SARs) to the National Crime Agency (NCA) and currently receives limited feedback on the value or effectiveness of SARs raised. The SARs reform programme under way seeks to enable more information to be shared with law enforcement, developing the sharing model produced by the JMLIT[46]. SARs reform is an opportunity to revolutionise the financial control framework in both effectiveness and efficiency, increasing the quality and enhancing the analytical capability while also achieving the right quantity of SARs.

The EPA encourages its members to engage in the public/private partnership initiated by the Home Office with the banking industry to strengthen its impact in reducing financial crime. We welcome initiatives that address the concerns of FATF in relation to the UKFIU[47].

Across law enforcement, industry, government and regulators, there is recognition that further work is required to establish a more effective legal framework for sharing of financial crime information (across known crime and credible allegations).


### SARs reform

"We will reform the Suspicious Activity Reports (SARs) regime through a public-private partnership. SARs are submitted by the regulated sector to alert law enforcement, at all levels, to activity that might indicate money laundering or terrorist financing. The number of SARs has doubled over the last ten years, and the efficiency of the SARs regime could be substantially enhanced"

"The reform programme will enhance the way that SARs intelligence is used by law enforcement and will produce clearer and better guidance to the regulated sector, allowing their very significant resources to be better targeted to have the most effect. In support of this, the NCA will increase the size of the UK Financial Intelligence Unit (UKFIU) which receives, analyses and disseminates intelligence submitted through the SARs regime."

HM Government's "Serious and Organised Crime Strategy – Nov 2018"[48]


"Researchers have long realised that annotated data (labelled data, for example onboarding records known to be fraudulent) cannot be scaled. Because of this, we expect to see a lot more effort put into unsupervised learning (where algorithms draw inferences from datasets comprising input data without labels), self-supervised learning (a form of unsupervised learning in which some part of the data is withheld and models trained to predict) and transfer learning (one approach in machine learning where models are trained on one task and then reused as a starting point for a different task usually harder to learn, or has less data available)."

**Stathis Vafeias, Head of Machine Learning at AimBrain**

This would need to adhere with data protection and client confidentiality and have clear framework for liabilities. The Criminal Finances Act (CFA) 2017 contributed to moving this forward - for example enabling information sharing on a voluntary basis where there is suspicion of money laundering, generating better intelligence for law enforcement agencies, and helping firms better protect themselves.

However, the CFA is seen as not sufficiently incentivising institutions to share money laundering intelligence, and its complexity prevents wide usage. Further work is under way to develop the necessary legal framework. The UK also is engaged in driving changes internationally through FATF requirements to enable greater sharing.

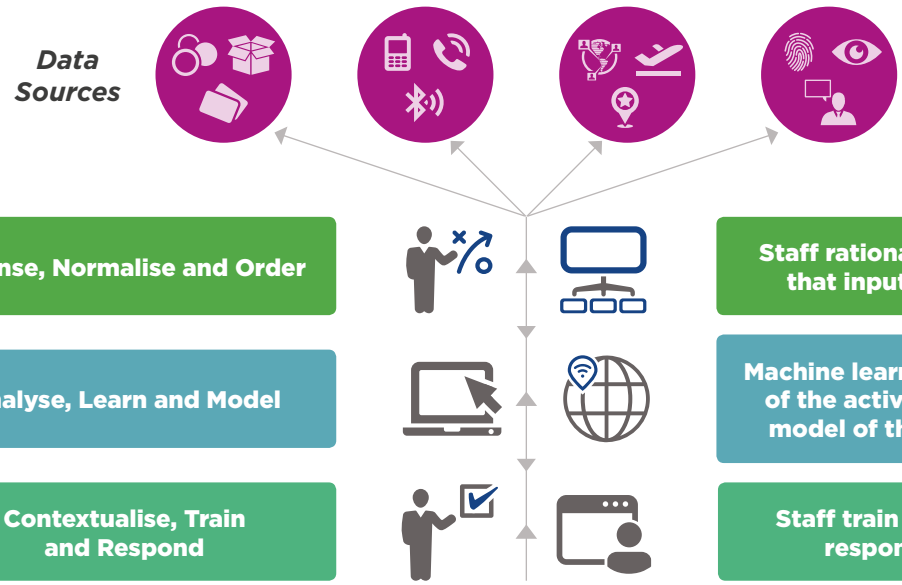
Developments in information sharing can be between all payments-regulated and AML-regulated entities within the industry, and between industry and law enforcement. Payment service providers and operators are well placed to identify suspicious activities related to individual payments or account behaviours over time. With the growth in payment providers due to innovation and open banking standards, approaches to information sharing will need to encompass a wider range of payments providers. Otherwise the criminals will be able to switch their activity to providers outside the sharing network.

Many RegTech companies to whom regulated entities could outsource are unable to obtain approval to hold the information. A mechanism for RegTechs to be certified to participate could transform the effectiveness of shared information.

The EPA is an advocate of initiatives to share financial crime information in order to manage financial crime risks in the industry, where the sharing needs to be inclusive of all regulated payments companies irrespective of size. It needs to go beyond banks/credit institutions to include authorised payment institutions, electronic money institutions, the newly regulated 3rd-party providers, and RegTech suppliers of data.

The set-up and ongoing costs for smaller payments firms to access information sharing services must be set at a level to allow fair competition in capabilities to tackle financial crime.

Following publication of the Government's updated Serious and Organised Crime Strategy (November 2018), the




EPA's policy should be to support sector-wide activity to determine the level and extent of information that can be shared by government and law enforcement, and between industry players, for the benefit of regulated payments entities.

The EPA with its members could explore how to develop clear principles for depositing and receiving information via a sharing mechanism in ways that are viable for payments providers and operators across the spectrum.

**EPA Recommendation:**
*Support sector-wide activity to determine the level and extent of information that can be shared by government, law enforcement, and payments companies for mutual benefit, through the use of a common platform and commercial model.*

**"Customers now demand a frictionless journey, but the digital-led world has provided criminals with more tools to open accounts and easily make payments."**

## 7.5 Really knowing who the customer is

Validating static identity documents like government IDs and passports against your name and date of birth, is no longer enough to understand your customer. Location data, social interactions, phone habits, spending patterns, and a variety of other attributes are now at the disposal of service providers, from within and outside the payments space.

To really know your customer, firms have to monitor behaviour. A step towards preventing fraud and money laundering is to prevent bad actors from initially entering the system, but this isn't something done only at on-boarding. Ongoing behavioural monitoring is essential to knowing not only your customer, but their motivations, and the whole network. Firms getting this overall view are understanding how criminals operate, identifying rogue participants and stopping the problem at source.

A combination of Big Data, Machine Learning, and Human Intervention is key to making sense of the criminal world. A wider variety of data points is being taken, from phone characteristics to spending habits and a variety of other public and private sector sources to build up a picture of how a typical customer acts, how you as an individual act, and crucially, how the network interacts.

Machine learning and behavioural analytics create a model of the world and can then identify anomalies; spreadsheets should be obsolete when it comes to the scale required to uncover the increasingly complex networks where criminals hide. (Figure 10 depicts the interaction between staff and technology in the cycle of machine learning.)

But what is normal? Customers now demand a frictionless journey, but the digital-led world has provided criminals

with more tools to open accounts and easily make payments. APIs, scripts, bots and other technology are allowing the creation of essentially false environments that interact for some time, until the illegal funds are ready to be moved. Then when it happens, it's not unusual because the framework has already been created. The industry now understands this practice, but it highlights not only the balance required between friction and security, but the level of sophistication required to identify sources of wealth coming into the system and then follow the money.

Even with all this automation, computers alone aren't enough. The modern world still needs that human touch to decipher it. Context, feedback and fine-tuning are essential to training these models, to determine whether a trend is relevant. Secondly, a system will only be as good as the data fed into it, so when combining multiple sources, a data cleansing stage is also essential to reduce false positives. Finally, following up alerts by making a phone call or some other contact with the customer, will always require human involvement.

The above principles apply whether the customer is a consumer or a business. Specialised KYC analysts are still needed, as the fragmentation and UBO concealment discussed earlier in **section 6.5** highlights the need to make sense of these layered referral models, especially in how merchants are approved for accepting card payments. Indeed, while machine learning can uncover patterns without any preconceptions, PSPs should still use a risk-based approach using known indicators when deciding whether to apply additional scrutiny for a customer. Sometimes, human intuition is required to validate any red flags[49] arising from an alert or risk assessment[50], or to personally visit company locations, which may belong to a fiduciary or incorporation service, or a generic rentable office, rather than the principal place of business[51]. Lines can be blurred as top companies increasingly recognise the benefits of co-location spaces like WeWork[52].

Machine learning technology has been around for some years now, but the EPA can help promote its appropriate use. This policy is called out in **section 7.8**. Duplication in validating customers and modelling data sources is inefficient and with the increased burden of compliance put on financial services firms, resource available to innovate is at a premium. The EPA can encourage members to share data sources within their own network, so that data only needs obtaining and sanitising once, to an agreed format.

EPA members can decide on minimum supplier standards within their group so that vendors used amongst members are effectively endorsed. Economies of scale could also be leveraged when seeking new data sources. Indeed, as part of its commitment to reducing corporate fraud, the EPA is already in discussions to promote a global company database where subscriber fees will be reduced based on the amount of fraudulent activity reported.

**"To address the issue of transaction monitoring, shared and transferrable behavioural modelling is equally valid here, especially to assist new services where there is no previous activity to analyse."**

**"The EPA can encourage members to share data sources within their own network, so that data only needs obtaining and sanitising once, to an agreed format."**

The lack of a harmonised global approach to KYC standards is also seen as a barrier to conducting effective compliance. The EPA can support members in raising the profile of this issue by developing and projecting a consistent message from its members, for engaging with regulators.

**EPA Recommendation:**
*Engage with EPA members to create a shared position on developing the case for a global approach to KYC standards.*

**EPA Recommendation:**
*Support and facilitate a collaborative member-wide programme to create minimum standards for due diligence on suppliers of data services.*

Simply using more data sources is not the complete story, because of the difficulty in scaling labelled data. Instead, the predictive nature of machine learning will need to be exploited to determine how customer behaviour will evolve.

Transfer learning allows the creation of behaviour models which can then be used elsewhere, so EPA members could fine-tune those models with their data and directly benefit from them. We also support peer recommendations to broadcast trend activity (such as new methods of fraud) in an anonymous manner to alert members to active threats, in line with the information sharing policy in **section 7.4**.

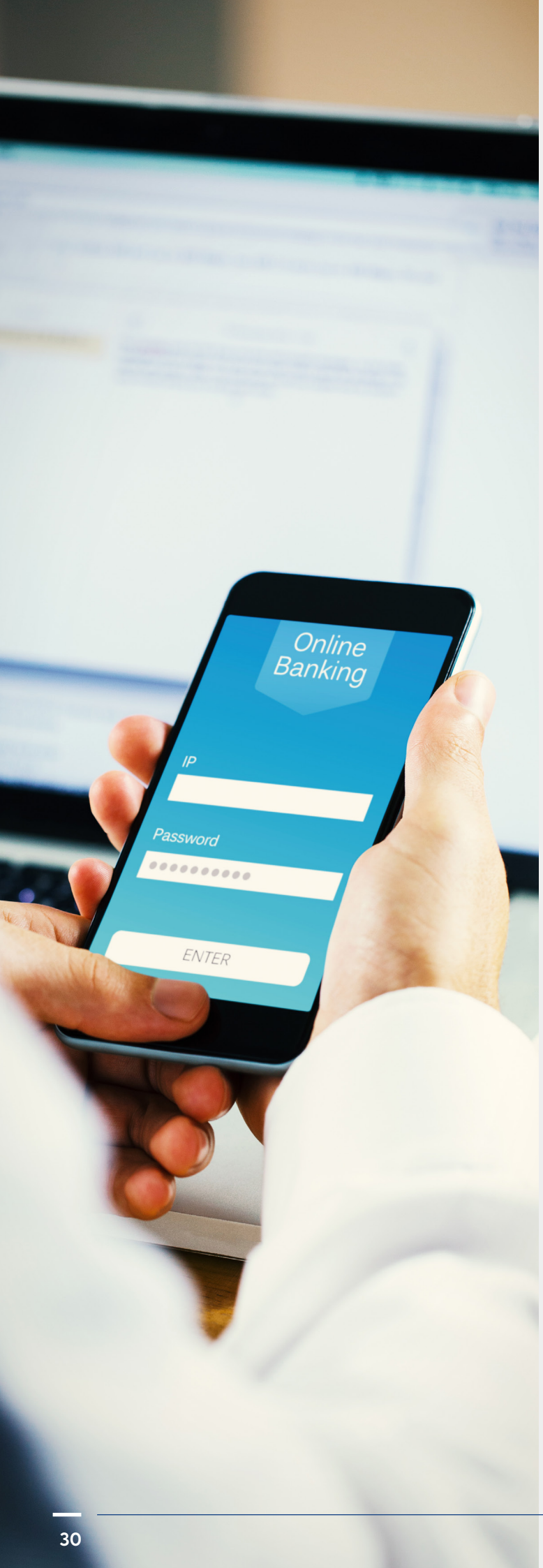
This must be done in a way that does not jeopardise commercial information or liability. We consider that blockchain solutions having the potential to record incorrect outcomes permanently need further legislation to resolve liability concerns.

**EPA Recommendation:**
*Support and facilitate a collaborative member-wide programme to share models and learnings from analysing customer behaviour that members can use with their own data.*

"Machine learning (ML) should not be seen as the panacea to solve the conundrum of anti-money laundering within client transactional data. Rather, it should be seen as an aid to the subject-matter expert (SME).

ML should work in conjunction with risk-based rules and aid the SMEs by removing false positives and indicating false negatives. ML should, when deployed correctly, help focus on the data that needs thorough and urgent investigation, and therefore remove the time-wasting element of looking at dead-end scenarios."

**Julian Dixon, CEO at Napier**




## 7.6 Addressing Threats in the Open Banking Environment

The new environment of open banking is discussed earlier (see **section 6.4**) as being a potential target for criminals. For example, social engineering through consumers being unfamiliar with 3rd-party providers (TPPs), and TPPs as an aggregator of payment services being a target for hacking or mule accounts.

The EPA can play a vital educational role in providing training to its members, advocating a common voice to prepare the consumer to expect entities other than their banks to be part of the authentication and information-sharing journey.

The open banking environment is still at an early stage, where all participants need to remain vigilant on emerging financial crime threats and to enhance existing security processes as required. For example, to mitigate cyber threats the industry could pursue a PCI-type model for TPPs, where different categories of certification are required dependent on the service offered.

**EPA Recommendation:** *Promote a shared, industry-wide voice, through collaborative training and education, to ensure the public is receiving coherent messages on the security of open banking.*

To address the issue of transaction monitoring, shared and transferrable behavioural modelling (as described in **section 7.5**) is equally valid here, especially to assist new services where there is no previous activity to analyse.

**"Our understanding of fraud in the UK is seriously hampered by under-reporting with less than 20% of incidents believed to be reported to the police."**


## 7.7 Improved Reporting of Financial Crime

While the payments industry is required to flag suspected instances of money laundering and terrorist financing, the reporting of cases of fraud is less controlled. This gives a reduced and distorted picture of where losses to UK citizens, businesses and government are occurring and results in a focus on crime methods which are recorded rather than those which are unrecognised, such as authorised push payment fraud until recently.

To ensure better intelligence is available, the regime of Suspicious Activity Reports is being improved, the Payment Services Regulations 2017 oblige PSPs to report statistics concerning payment fraud to the FCA on at least an annual basis.

This transparency is welcome however it is likely to underestimate the true losses; customers and especially businesses, do not report all fraud consistently to their payment provider.

The ability of government, law enforcement and industry to prioritise which financial crimes to tackle is therefore diminished by lack of reliable data and perceptions that the problem is not as big as it is. Furthermore, with no consistent reporting mechanism, the same fraud might be reported by the victim and the sending and receiving PSPs.

Searching for financial crime groups relies on being able to piece together a jigsaw of their activity: with too many missing data points, links may be missed, investigative resources wasted and prosecutions undermined. Analytics may be able to help, but good training and corroborative data is key to many machine learning techniques.

While the money laundering reporting system is widely known, the corresponding system for fraud is less well used. The UK has a single reporting point for all fraud, Action Fraud, however many cases go unreported as only a proportion of cases can be investigated. This reduces the value of the database.

The National Crime Agency states in the National Strategic Assessment 2018:

*"Our understanding of fraud in the UK is seriously hampered by under-reporting with less than 20% of incidents believed to be reported to the police."*

Reporting of cases of fraud by business customers to police, financial institutions and fraud prevention services – such as CIFAS and National Hunter – is inconsistent and results in untrustworthy statistics. While listed companies may have obligations to inform some third parties[53] even this does not include their PSPs. Fraud professionals in banks consulted for this report said that businesses rarely report fraud to them, especially where internal staff were involved.

In addition, there are disincentives for business


**"In doing so, technology deployments need to complement the need for human experience and judgement for effective and compliant decision-making which will deliver real improvements to business outcomes and the customer experience. Furthermore, technology investments and deployment need to fit with external strategic developments, allow good control of the new business risks introduced (and avoid unintended consequences), and deliver benefits inclusively across the widest range of user groups."**

customers to recognise fraud as such. A business may claim back VAT on good or services which are stolen, but the business is defrauded, VAT may not be reclaimed. This practice creates a financial incentive to classify the crime as theft rather than fraud.

Ultimately, statistics on cases and losses are incomplete, which therefore makes it difficult to quantify the scale of the problem for the industry. The recently-formed National Economic Crime Centre (NECC) will require good data and statistics which the EPA believes are critical to the successful detection, prevention and prosecution of financial crime.

The EPA will engage with the NECC to help create an intelligence sharing, operational group with broader membership – including EPA members both large and small – similar to JMLIT but with a focus on payments-related financial crime.

The NECC may well be the correct point of engagement for other EPA initiatives in this section. EPA members and other PSPs should encourage customers to report all fraud both to them and, currently, via Action Fraud website.

This will ensure as complete a view of the problem as possible and facilitate budgetary justifications and development of solutions. In addition to payment schemes. EPA could lobby Government to remove legislative and procedural disincentives from reporting financial crime.

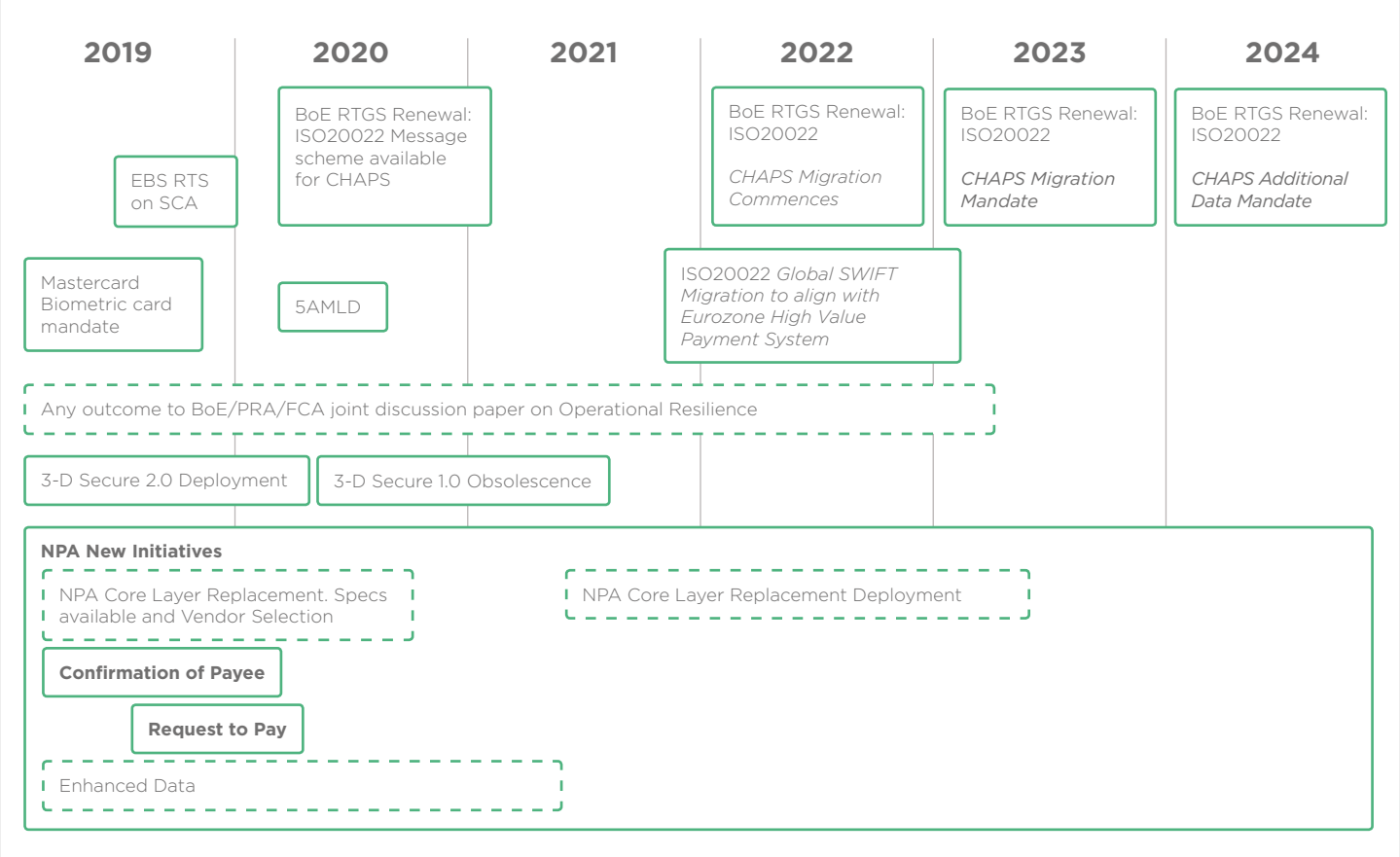



**Figure 7:** Timeline of Industry, Regulatory and Legislative Initiatives/ Milestones

**EPA Recommendation:**
*Engage with National Economic Crime Centre and government to facilitate and reward reporting of financial crime by all parties via appropriate groups and channels, and to educate victims about how reporting helps reduce criminal activity.*

## 7.8 Effective deployment of technology to fight financial crime.

This section of the report has advocated priority areas where an ambitious approach to using latest technology capabilities can have a strong impact on fighting financial crime in payments. Critically, these technologies need to be deployed on a timely basis – investing in updating or extending defence capabilities to keep pace with the criminals.

In doing so, technology deployments need to complement the need for human experience and judgement for effective and compliant decision-making which will deliver real improvements to business outcomes and the customer experience. Furthermore, technology investments and deployment need to fit with external strategic developments, allow good control of the new business risks introduced (and avoid unintended consequences), and deliver benefits inclusively across the widest range of user groups.

### Ongoing Investment in technology

Criminals will always be up-to-date on the latest technology trends and will exploit the weakest link in the chain; however, throwing money at the latest tech is not necessarily the way forward, especially in the fraud and payments space. Whilst regular investment in IT and eliminating obsolete infrastructure would seem obvious, a constant eye on regulation and ensuring technology is appropriate, are factors in determining which companies come out on top.

Companies need to act smartly when it comes to developing financial services technology, fully understanding the busy schedule of regulatory, legislative and industry-programme changes flowing over the next 3-5 years (see figure 7). Companies should invest resources in horizon scanning and collaboration to enable investments in new systems to align strategically with this timetable of changes. For example, Pay.UK's new payment architecture programme and the Bank of England's RTGS renewal programme, and with both adopting the ISO20022 standard, provide once-in-a-generation opportunities for systems renewal. The Bank of England ran a valuable consultation earlier this year on adopting this standard for payments in the UK[54].

Technology needs to be relevant to meet specific requirements and contexts; there are nuances between concepts and products, between fraud and AML, between closed-loop gift cards and open-loop prepaid cards, between machine

learning and deep learning. To the uninitiated, these differences may be subtle but have big implications; but for those prepared to invest, the rewards can be reaped. The EPA could work with its members to provide training and support to promote that longer-term vision and strategic advice that companies require. EPA also has a variety of specialist members who support different niche areas, so that technology opportunities can be understood and well- targeted, according to each target company's requirements.

**EPA Recommendation:**
*Provide education and awareness to align firms' technology investment programmes with the concentrated programme of industry-wide regulatory, infrastructure and standardisation changes scheduled for 2019 and the following 3-5 years.*

**EPA Recommendation:**
*Provide education and awareness on specialist technology areas through showcasing and collaborating with EPA members involved in those fields.*

## Balance of Technology and Human judgement

In the field of artificial intelligence and machine learning, for example in transaction analytics, providers need the right human involvement for judging context and evidence, and for taking important decisions to address suspicious transactions or customers. There is a requirement in GDPR (Chapter 3, Section 4, Article 22.1) that gives data subjects the right to not be subjected to decisions solely based on automated processing that produces 'legal effects' or other significant effects.

## Creatively challenge underlying assumptions

Another important challenge for deployment of technology in customer products and services is to adequately assess how the new technology-enabled service could be abused by criminals for fraud or laundering.

When banks first offered services on the internet, they replicated some of the services in-branch, however the detached nature of electronic banking allowed actions that were not possible in the physical world and criminals have exploited these differences. For example, a criminal could not physically go to five tellers in a branch at once, but online a criminal could open as many banking connections as feasible. Also, if a criminal was unsuccessful in a branch with one set of credentials, he/she would be recognised coming back into the same branch with a different set; these restrictions are not present online.

These unintended consequences can be reduced by carrying out stronger scrutiny of usage assumptions, and risk assessments of fraud opportunities from a fraudster's viewpoint.

## Services and their benefits must be widely available

A further consideration is to avoid a 'digital divide', where services based on advanced technology capabilities can deliver real benefits for certain user groups but risk disadvantaging other user groups. Political and societal support is dependent on a clear path to enabling these benefits across society, for different socio-economic groups, different education levels, and different levels of physical capability. In deploying technology, firms and regulators need to consider the take-up of the required devices across user groups, the levels of training and awareness required for different customer groups, and access by people of different capabilities and ages.

This area of analysis has been a primary consideration, for example, in the recent interim report by the Access to Cash Review[55], which highlights that 8 million people in the UK say cash plays an important part in their lives. The same rigorous analysis is required for technology-based tools to prevent fraud. The benefits of technology need to be spread evenly across the population, and in particular not disadvantage lower-income or vulnerable customer groups. ■

**Footnotes:**

**39** Fraud the Facts - [UKFinance] 2018

**40** Fraud the Facts - [UKFinance] 2018

**41** UK Finance adopted the British Standard in Digital Identification and Authentication (PAS499) as meeting their PSR obligations in October 2018. Digital Identity in the UK Financial Services Sector – [UK Finance] 2018

**42** Serious and Organised Crime Strategy 2018 - [UK Home Office] 2018

**43** ISO/IEC 2382-37. Information technology (Vocabulary, Part 37): Biometrics - [ISO]

**44** Delivering Digital Identity – Why banks should act now - [Consult Hyperion / Gemalto] 2018

**45** A Payments Strategy for the 21st Century - [Payments Strategy Forum] 2016

**46** Joint Money Laundering Intelligence Taskforce. Anti-money laundering taskforce unveiled – [UK Home Office] 2015

**47** Immediate Outcome 6, United Kingdom Mutual Evaluation Report - [FATF] 2018

**48** Serious and Organised Crime Strategy 2018 - [UK Home Office] 2018

**49** Concealment of Beneficial Ownership - Indicators of Concealed Beneficial Ownership - [FATF] 2018

**50** Finalised Guidance - FG 18/5: Guidance on financial crime systems and controls: insider dealing and market manipulation (page 31 provides good practice recommendations for risk assessments as required by Regulation 18 of the Money Laundering Regulations) - [FCA] 2018

**51** Card schemes have strict rules on defining the correct location of a merchant's principle place of business: Visa Core Rules and Visa Product and Service Rules [Section 1.5.1.2] - [Visa] October 2018 edition. Mastercard Rules [Section 5.4] – [Mastercard] 28 June 2018 edition.

**52** WeWork becomes central London's biggest office occupier - [FT.com] 2018

**53** Fraud reporting in listed companies: A shared responsibility -[Fraud Advisory Panel] 2010

**54** [Bank of England] 2018

**55** Is Britain ready to go cashless? - [Access to cash] 2018

# 8. Conclusions

Across the payments industry the threats faced from financial crime are varied, large scale and continually evolving. The industry has done much in recent years to tackle this, for example Chip and PIN, tokenisation of card details, and currently Confirmation of Payee and strong customer authentication.

However, there is widespread acceptance that much more needs to be done. This needs to encompass prevention, reduction of impact, detection and prosecution, based on robust understanding and evidence of the nature and scale of threats faced today.

The report has set out approaches based on ambitious use of technology in tackling the criminal threat, together with enhanced information sharing and more comprehensive and consistent reporting of the fraud and laundering activity seen currently.

A number of parties need to collaborate to make this happen:

- The EPA, as a voice for industry, can stimulate debate across its members and with all payments stakeholders
- EPA members, as payments operators and payments providers, can educate their own customers and engage actively in collaborative industry initiatives
- Law enforcement, working closely with industry, can decide on the most effective actions to take to disrupt the criminal groups, based on the insights, suspicions and evidence that industry provides
- Government can allocate resources to law enforcement with near-term impact, and introduce new or updated legislation to drive change in the medium term – for example to enable wider information sharing to tackle crime.
- Regulators can set priorities for compliance with risk management and reporting requirements, and can allow and encourage the use of new technology as a key capability for the industry

The key requirement is collective action involving all parties in the payments supply chain. Going beyond the industry, there should be active collaboration across stakeholders including customer groups, law enforcement, government and regulators. As a trade association, the EPA can play a leading role in articulating a balanced view, across many payment companies, of the challenges faced from payments financial crime, and opportunities to conquer them. ■

**“As a trade association, the EPA can play a leading role in articulating a balanced view, across many payment companies, of the challenges faced from payments financial crime, and opportunities to conquer them.”**

# Notes

# Notes


**Emerging Payments Association**
London, SE1 2SX, UK
Tel: +44 (0) 20 7378 9890
Web: emergingpayments.org
Email: info@emergingpayments.org
@EPAssoc
Emerging Payments Association