EMERGING PAYMENTS ASSOCIATION

The fight against fraud and financial crime

The case for greater investment in technology and organisational change

Report from the EPA's Project Futures Workshop

MARCH 2020

Sponsored by

FICO Decisions

The purpose of Project Futures is to provide members of the Emerging Payments Association with insight and thought leadership on new innovations and technological developments, emerging market trends, and the prospective future regulatory landscape in payments.

The Project Futures workshop at Glaziers Hall, London Bridge in December 2019 focused on the case for greater investment in technology and the centralisation and consolidation of department responsibilities in order to improve the fight against fraud and financial crime.

The discussion focused on the following themes:

- Management of risk
- Fraud prevention
- Money laundering compliance
- KYC checking
- Cyber security defence

The workshop was structured around four interactive breakout sessions:

- The advantages and disadvantages of centralisation and consolidation
- The market trends and impact
- The opportunities, barriers and challenges
- Regulatory factors, technology and innovation

This report is part of a series produced by the Emerging Payments Association. It highlights the contents of the discussions, the insights derived and the conclusions drawn. These highlight the direction of travel for the payments industry as it develops and how the ecosystem may change in the light of new technologies and innovations. Previous reports are available from the EPA website www.emergingpayments.org, including: The impact of real-time on payments and data; new Credit and lending services; Data proliferation and using data to drive payments innovation; Monetisation of data; and Innovation in international trade.

Thank you to the Project Benefactor, FICO, the workshop moderator and report author, Mark McMurtrie, Director of Payments Consultancy Ltd and to the 15 workshop participants for their contributions to this insightful workshop.

EPA EMERGING PAYMENTS ASSOCIATION
INNOVATION IN INTERNATIONAL TRADE
Report from the EPA's Project Futures Workshop
December 2018
Sponsored by FICO Decisions
DATA PROLIFERATION AND USING DATA TO DRIVE PAYMENTS INNOVATION
REPORT FROM THE EPA'S PROJECT FUTURES WORKSHOP
APRIL 2019
The Impact of New Credit and Lending Services on Payment Service Providers
June 2019
Report from the EPA's Project Futures Workshop
The Impact of Realtime on Payments and Data
OCTOBER 2019
Report from the EPA's Project Futures Workshop

For more details and to join you should contact Nick May at nick.may@emergingpayments.org

Introduction

This report discusses the fight against fraud and financial crime. It makes the case for increased investment in technology systems and greater centralisation and consolidation of department responsibilities. The content of this report draws on discussions at a workshop organised by the EPA.

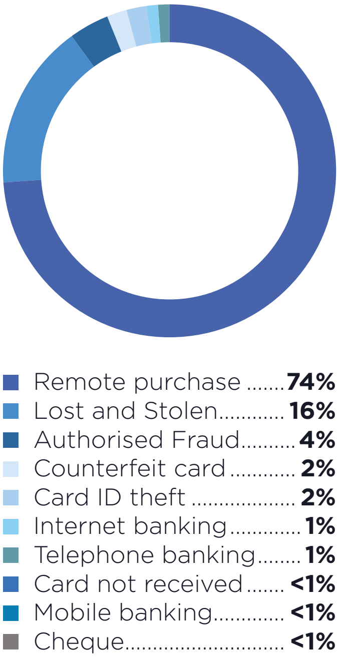
Financial crime includes the illicit payment flows from money laundering, bribery, tax evasion, fraud and corruption that support human abuses including modern slavery, drug trafficking and prostitution. Payment fraud refers to any false or illegal transaction, often involving credit and debit cards, remote banking and authorised push payments this increasingly occurs online. Cyber-criminals usually steal money, personal property, or sensitive information from an individual and then seek to monetise this.

The discussions explored how companies could consolidate departmental responsibilities in order to help prevent fraud, reduce business risk, ensure regulatory compliance, improve cyber security defences and stop criminal networks profiteering from financial crime. We primarily looked at the UK market but also considered trends from across continental Europe, North America, the Middle East and Asia, as the payments market is increasing global in nature and many of the workshop participants represented organisations with global operations and customers. This report focuses only on fiat currencies and not on cryptocurrencies or other types of unregulated payments.

Key Issues

Criminals are becoming increasingly organised and professional and attacks are becoming more diversified, sophisticated and frequent. Criminals are now far more connected and often work together to defraud companies and individuals. The impact of an attack has also escalated dramatically in the last decade, which is why most financial institutions (FIs) and regulators recognise that this topic deserves more attention. Card-based remote purchase fraud is by far the most common type of fraud with over 1 million instances reported in the first half of 2019.

Number of Fraud Cases in the UK 2019 H1



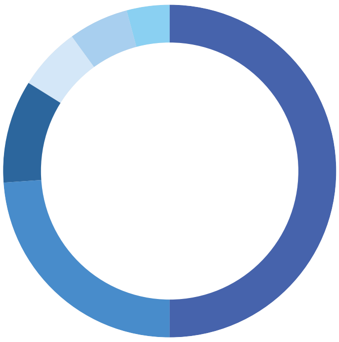
"In the UK fraud accounts for around one third of all crimes experienced by individuals."

Workshop participants felt that the direct financial losses to FIs from fraud were not their primary business concern but rather reputational damage and the impact of fraud on their customers. Attendees also recognised that the escalating penalties being imposed by regulators for failing to tackle financial crime encourage the industry to prioritise compliance over prevention and risk management. The ever-increasing operational costs of tackling financial crime call into question whether there are better ways to protect both businesses and customers. Greater investment in technology is felt to be critical as previous approaches cannot respond quickly enough or scale sufficiently to meet the attacks now happening.

Anti-Money Laundering (AML)

Organised criminal gangs launder billions of pounds globally through payment systems every year. The scale of this is why governments are trying so hard to tackle these crimes and require FIs to strengthen their defences and prevent the illegal flow of money. The number of penalties issued by regulators for AML irregularities globally in 2019 increased by 100% to 58. The US had the most penalties applied with 25 cases, followed by the UK in 2nd place with 12 and India in third place with 5. ▸

Number of AML Penalties in 2019



■	US	25
■	UK	12
■	India	5
■	Belgium	3
■	Latvia	3
■	Norway	2

UK Fraud Data for Authorised Push Payment Scams in 2019 H1

2019 Ranking	Country	Total value ofAML penalties
1	France	$5,100,000,000
2	US	$2,286,531,383
3	UK	$388,396,000
4	Belgium	$336,779,000
5	Germany	$16,500,000
6	Latvia	$4,810,000
7	Hong Kong	$1,600,000
8	Norway	$1,003,532
9	Lithuania	$1,000,000
10	Bermuda	$500,000

The total amount of AML penalties issued came to $8 billion, a 90% increase over the previous year and second only to 2014 where the total figure was almost $11 billion. The average monetary fine was $145 million. The French regulator issued the largest fine to a single institution at $5.1 billion. The total of US penalties was $2.28 billion and, worryingly, the UK was in third place with fines of $388 million. It is noteworthy that only 48% of penalties were issued to banks compared with 69% in 2018. Four fines went to UK-based gambling/gaming organisations.

Other key themes raised included the industry-wide shortage of appropriately skilled resources to lead the fight against financial crime attacks and the opportunities available from improved technology platforms and greater systems integration. It is critical today for FIs to have teams of high quality data scientists available to help protect their organisation and customers.

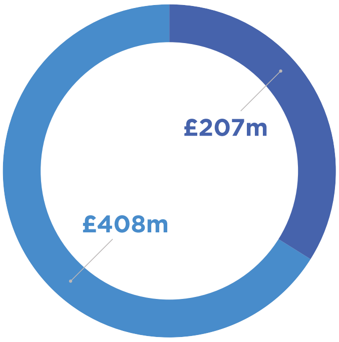
Some of the reasons shared for failing to effectively combat financial crime relate to the pressures within organisations of constantly growing company revenues, opening up new markets, corporate profit expectations and today's highly competitive marketplace. These at times appear to have a higher internal priority than preventing fraud and crime.

UK Statistics

While it is difficult to know exactly how much money is laundered through the UK, the FCA estimates that it costs the UK £37bn every year with the annual total cost of fraud standing at £190 billion.

> **"Since 2015, annual AML penalty figures have been steadily rising. Multi-million dollar fines have been commonplace for a while, but we are now seeing more penalties of one billion dollars and over."**

UK Payments Fraud 2019 H1



■	Authorised Fraud	34%
■	Unauthorised Fraud	66%

"UK estimates are that £37 billion is laundered annually and the cost of fraud is £190 billion." Financial Conduct Authority (FCA)

UK Finance data states that criminals stole £1.2 billion through payment fraud and scams in 2018. This can be divided into Authorised payment fraud, where the genuine customer is tricked into making a payment (now accounting for £207 million and 34% of the fraud in the first half of 2019) and Unauthorised payment, which is undertaken without the customer's knowledge or participation (accounting for £408 million and 66%). There were almost 1.5 million cases of fraud reported during the last 6 months.

The biggest proportion of Unauthorised payment fraud came from remote purchase (CNP), which increased to £237.4 million in 2019 H1 from 1,071,493 cases. Thanks to the introduction of Chip & PIN technology, Counterfeit card losses now total only £6.6 million in 2019 H1, a significant decrease when compared to the peak of £170 million annually in 2008. Losses due to lost and stolen card fraud rose to £48.3 million. Remote banking fraud totals £65.7 million with 74% of losses coming from internet banking, 17% from telephone banking and 8% from mobile banking.

Losses due to card ID theft were £18.5 million, a decrease on the £29.9 million figure from 2018 H2. Intelligence suggests that the main driver of card ID theft is data harvesting by criminals through methods including phishing emails, scam texts and the theft of mail from external mailboxes and multi-occupancy buildings. Card not received fraud losses, where a card is stolen in transit after the card issuer sends it and before the genuine cardholder receives it, fell to £2.5 million.

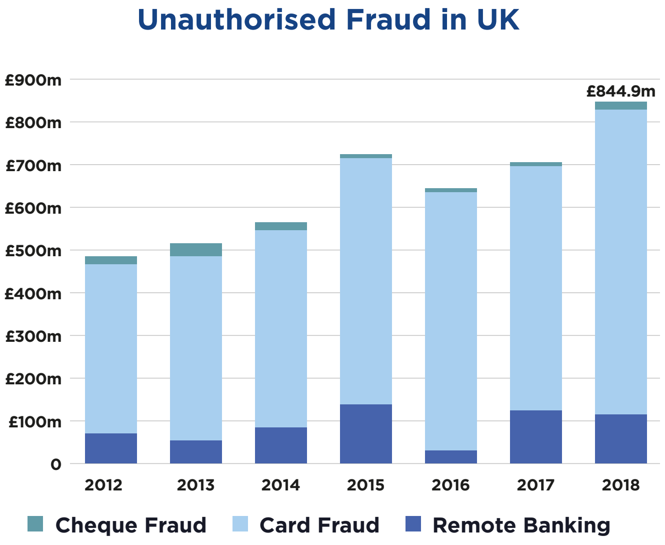
A total of £318 million of attempted remote banking fraud was stopped by bank security systems, which is equivalent to £6.75 in every £10 of fraud attempted being prevented. In addition, 15% (£22 million) of the losses across all remote-banking channels were recovered after the incident.

Fraud from cheques is £29 million, but represents a significant increase from £20.5 million in 2018. The introduction of digital cheque deposits may have made this a more attractive channel for criminals.

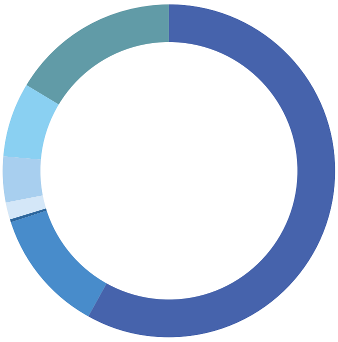
On a positive note, statistics indicate that bank systems are detecting fraudulent spending more quickly and the average loss per individual case is lower. Another industry report forecast, less optimistically, that payment card fraud globally was projected to grow to $35 billion in 2020 and that every dollar of fraud committed costs merchants $3.

Authorised Push Payment Fraud

The second most worrying area of payment fraud relates to Authorised Push Payments. The latest UK Finance fraud statistics for the first half of 2019 show that £207 million was lost, a 40% increase over 2018 H1. ▸



UK Payments Unauthorised Fraud 2019 H1 in £



■	Remote purchase	237.4
■	Lost & Stolen	48.3
■	Card not received	1.4
■	Counterfeit card	6.6
■	Card ID theft	18.5
■	Cheque	29.4
■	Remote banking	65.7

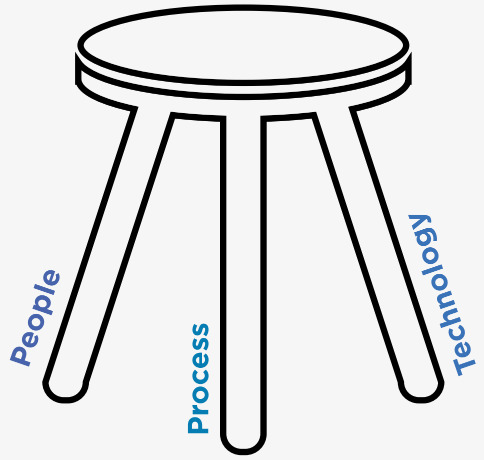
The table highlights the most common scams, the number of fraudulent payments, the value of losses and how much was ultimately returned to the customer.

Data Breaches

Criminals continue to attack businesses that sell online, seeking to steal payment card details that they can monetise and use to commit fraud. With more businesses selling online, we can see the volume of security breaches increasing as well as the number of records captured. This is despite the fact that the Payment Card Industry Data Security Standards (PCI DSS) have been in existence for over 15 years. The UK remains a very popular country for criminals due to the maturity of the eCommerce marketplace and the high number of payments taking place. Some successes have been achieved but defences must be strengthened and further investments in security technologies are required.

> ***"Almost two thirds of medium and large sized UK businesses identified a cyber security breach or attack in the last 12 months." Department for Digital, Culture Media and Sport***

The cost of a data breach is very high, with businesses incurring costs for forensic investigations, system upgrades, fines from payment schemes, card replacement costs, compensation claims and penalties imposed by regulators. In 2019, British Airways received a £183 million fine following a major data breach where 380,000 customer records were compromised, highlighting how GDPR regulations are now working in parallel with PCI when a data breach happens. Businesses that suffer a data breach will also experience big revenue losses as customers lose trust and move their spending to competitors.



Pillars of Fraud Prevention

> ***"Almost 50% of customers will stop using a business following a data breach with a third unlikely to ever return."***

Effective defence strategies are supported by three equally-important pillars – people, process and technology. Employees are thought to have been involved in half of all attacks. While technology generally requires the greatest investment, this should not be at the exclusion of process and people improvements.

> ***"Around 50% of all reported cases of fraud and attacks include inside involvement."***

Participants felt that all fraud losses are generally under-recorded in

UK Fraud data for Authorised Push Payment Scams in 2019 H1

Scam category	Number of Payments	Value of losses	% Increase in losses	Amount recovered
Purchase	44,252	£27.9 million	+43%	£2.7 million
Investment	7,126	£43.4 million	+108%	£2.9 million
Romance	4,388	£7.9 million	+50%	£0.5 million
Advance Fee	7,345	£8.2 million	+38%	£0.7 million
Invoice/Mandate	6,195	£55.9 million	+7%	£13.5 million
CEO	487	£7.9 million	-1%	£2.1 million
Police/Bank	10,056	£35.4 million	+60%	£11.2 million
Other impersonation	6,317	£20.9 million	+45%	£5.5 million
TOTAL	86,077	£207.5 million	+40%	£39.3 million

published statistics as many companies fear reputational damage and risk to third party relationships if they reported all incidents and published the full financial costs.

Organisational Structures

Responsibility for fighting financial crime for most large FIs tends to sit across multiple departments and teams, such as risk, fraud, compliance and IT. Additional specialist teams are often formed when new threats emerge. Several positive examples were given of departments starting to work more closely together thanks to threats now crossing classic boundaries. Cyber and data security is mainly the responsibility of IT departments, based on the perspective of it as a largely internal issue, rather than one that impacts customers and broader stakeholder groups. This may explain why there is less evidence of close co-operation between IT and other crime-fighting/fraud prevention departments. This is despite the evidence from multiple research studies that insiders are involved in more than 50% of attacks and fraud cases.

"Strong Customer Authentication spans multiple departments including compliance, risk management, fraud prevention, security, IT, operations and customer support."

"Organisational structures have evolved over time and largely been reactionary to new threats and regulatory demands rather than strategic choices."

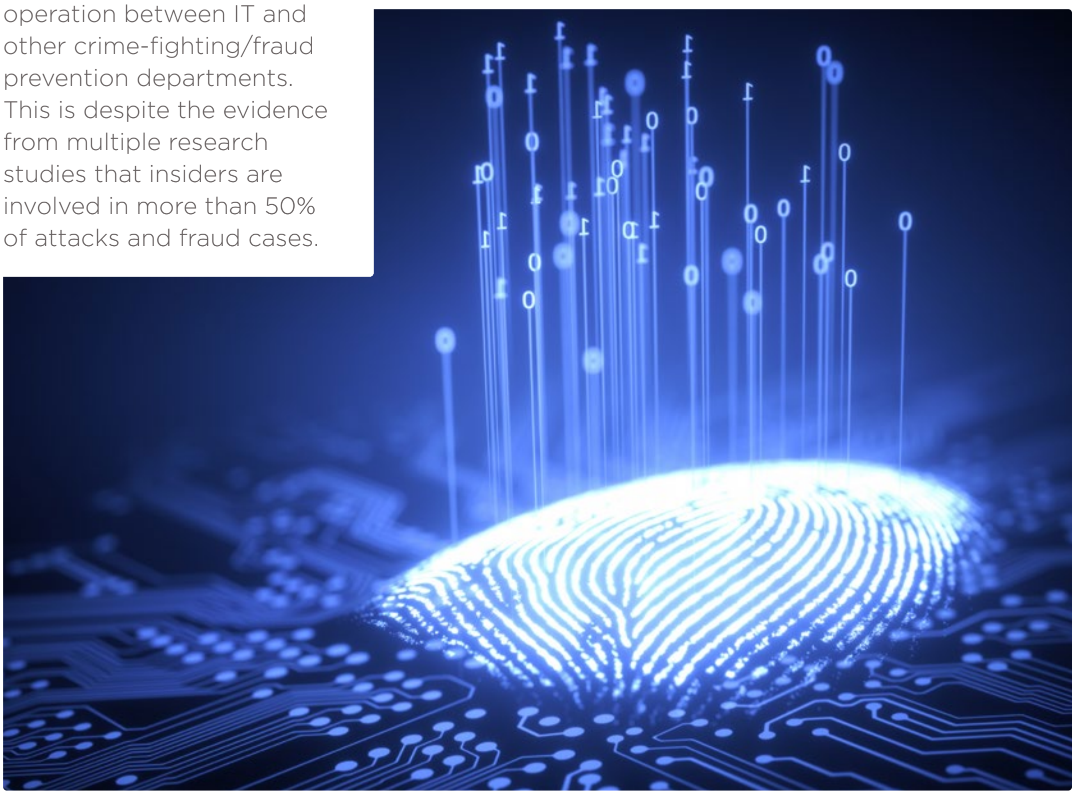
Some large FIs have established 'Shared Services' functions for many organisational responsibilities including risk, fraud and financial crime. This model has merits but its implementation needs to avoid the recreation of silos so it can address the whole picture. The European PSD2 regulation, for example, has brought the need for Strong Customer Authentication, but this responsibility lacks a natural home within many FI organisational structures as it impacts multiple departments.

From the outset, Fintechs have looked more holistically than the large established FIs at fraud and crime prevention and they have not been burdened by legacy systems or historic departmental structures. This may simply be because Fintechs often have fewer resources and require an individual to fulfil multiple roles which, within a larger FI, would have resided in different departments. One of the key barriers to greater departmental co-operation and consolidation is from compliance teams who frequently have a single-minded focus on achieving/maintaining regulatory compliance, often at the expense of wider organisational benefits.

"We are tasked with ensuring regulatory compliance and discouraged from looking more broadly."

Organisational structures are already starting to change and this trend is expected to accelerate over the next three years. This report helps articulate some of the advantages, barriers and challenges that apply.

"Criminals don't worry about departmental structures; they simply look for the weakest link." ■



Advantages and Disadvantages of Centralisation and Consolidation

Advantages

Greater centralisation and consolidation of department responsibilities and investment in new technology platforms offer many advantages to FIs. This is increasingly being considered by organisations, but the rate of adoption varies considerably and for many organisations requires acceleration.

"A converged financial crime operating model is the next logical step."

Cost Savings

The main advantage relates to the potential cost savings, both in employee costs and technology costs. A single pool of resources allows efficiency savings to be realised, greater flexibility and improved productivity. Having a single data science team was one example where cost savings could be achieved at the same time as strengthening protection levels and reducing business risk. Currently the majority of large FIs have multiple technology systems in place, many of which have overlapping functionality, provide poor data-sharing and require dedicated specialists to manage day-to-day operations. Over time, these departments frequently become silos and fail to work effectively together. System consolidation should result in both CAPEX and OPEX savings.

Better Decision-making

A key aspect of the consolidation of financial crime prevention systems is the creation of a single enlarged data pool. This allows enhanced detection of attacks, improved risk management and better decision-making. Artificial Intelligence (AI) and Machine Learning (ML) are increasingly important but these rely on access to consolidated data. This allows the identification of patterns and behaviours that would otherwise remain hidden.

"Access to more data allows better decisions to be taken."

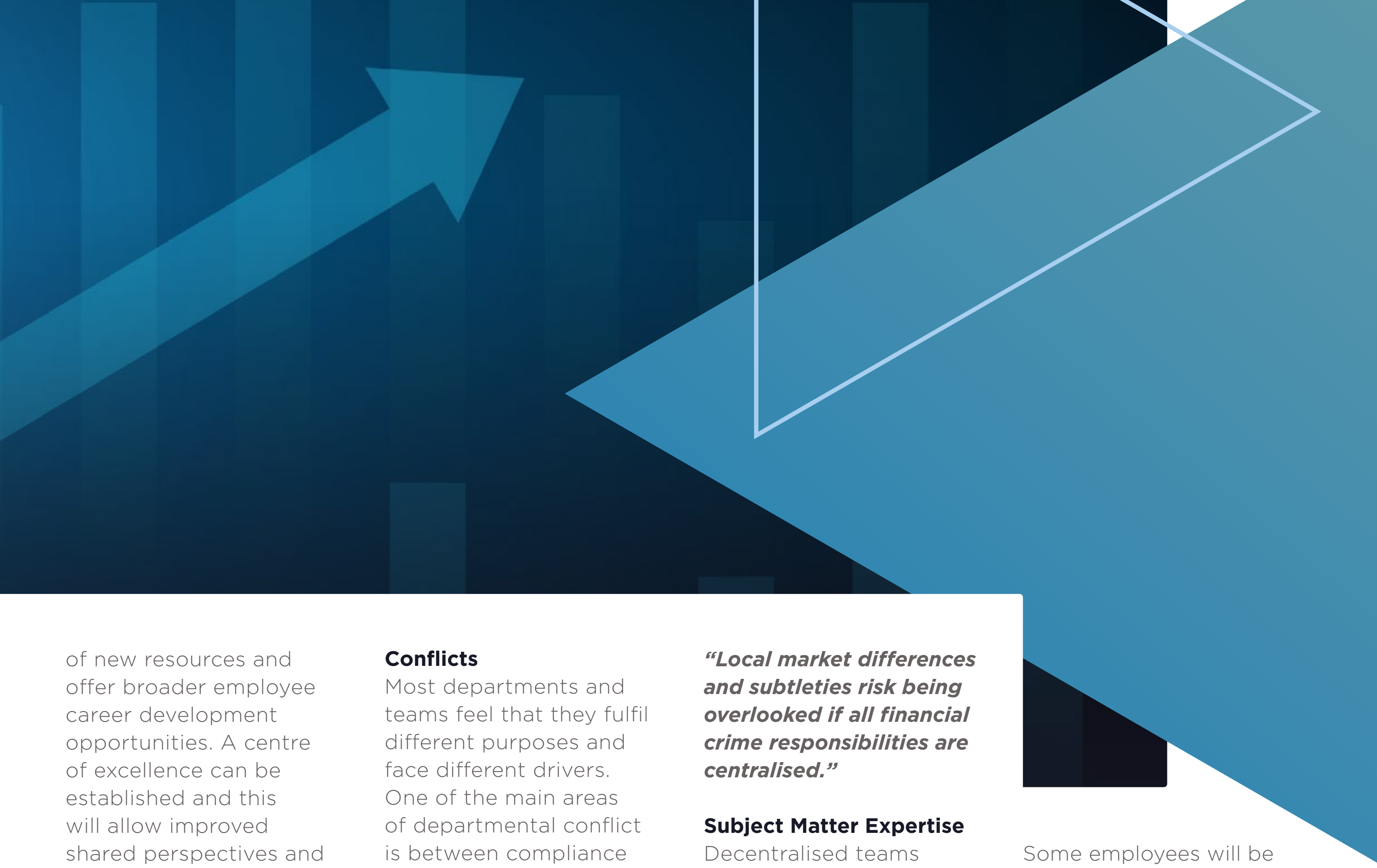
Accountability

If all resources focussed on fighting financial crime report into a single senior executive, this will bring increased visibility and accountability. Today, many firms have more than one fraud team and these may take too narrow a view. Most FIs recognise the growing synergies between functions but organisational structures and conflicting departmental objectives often hinder cooperation.

"Consolidation of responsibilities would prevent 'finger-pointing' between departments and provide 'one throat to choke'."

Resource Flexibility

There is an industry-wide shortage of the highly skilled individuals needed to protect, detect and prevent financial crime. An enlarged team structure will help in the recruitment



of new resources and offer broader employee career development opportunities. A centre of excellence can be established and this will allow improved shared perspectives and understanding. It will also help minimise the impact of resource shortages that currently exist within teams.

Easier to Manage

If responsibility is consolidated then it will be easier to manage resources and ensure greater alignment with the top priorities. A unified team will also result in more cross-pollination of ideas. Greater transparency will also be achieved as well as improved consistency in communications.

"The realisation of these advantages relies on execution excellence and strong leadership."

Disadvantages

There are also disadvantages and risks to centralising systems and consolidating departmental responsibilities.
The following are particularly important.

Conflicts

Most departments and teams feel that they fulfil different purposes and face different drivers. One of the main areas of departmental conflict is between compliance and risk teams. Where team priorities differ, consolidation may not be straightforward. The differing points of view from diverse roles are valuable and these remain important, even when those responsibilities are centralised.

"Conflicts between departments can be reduced through aligned priorities, joint objectives, better communications and stronger leadership."

Local Market Needs

Many FIs serve multiple international markets. Local teams understand the subtle differences of each, but these might be missed after centralisation and compliance to local regulations may be harder if managed centrally.
As the styles of criminal attack vary by geographic region, so different defence strategies may also be necessary.

"Local market differences and subtleties risk being overlooked if all financial crime responsibilities are centralised."

Subject Matter Expertise

Decentralised teams build up deep specialisms and subject matter expertise. Organisational changes typically unsettle some individuals, with some fearing that the value of their specialist skills may be reduced. They may not like the sound of departmental consolidation and start investigating other career opportunities. These concerns need to be considered before any changes are implemented.

"Organisational change may cause short-term disruption and some loss of key staff."

Leadership

The success of departmental consolidation requires strong leadership to be in place as it is easier to manage small teams rather than very large ones. Appropriate leaders will need to be identified or recruited before embarking on any reorganisation.

Some employees will be resistant to change and will need to be convinced as to the advantages. This could result in some short-term staff attrition but this should be outweighed by greater resource flexibility, simplified recruitment and other long-term benefits.

Learning Slows

Decentralised departments are thought to respond to traditional attacks more quickly. However, thanks to adaptive technology solutions, new types of attack can be identified faster and new prevention strategies agreed more quickly where there is a consolidated department and unified platform.

Cost

Reorganisations may have a negative short-term cost impact and may disrupt current operational activities; the benefits, however, are expected to far outweigh these costs in the medium-term. ■

Market Trends

One of the notable trends is the ever-increasing volume of regulations being introduced and their increasing scope of these continues. Considering several of the key European and Global initiatives, reporting requirements seem to have significantly increased as have the penalties for non-compliance. Importantly, local variances need to be managed and some regulatory demands can even prevent consolidation happening. These enhanced regulatory requirements are also making it more challenging for FIs to outsource some activities.

"Each year we need to spend more and allocate additional resources to comply with regulatory demands."

Financial crime and the perpetrators behind it do not respect borders – their operations are truly transnational and highly professional. They shift their attention to the weakest link.

FATF

One of the most significant global initiatives is co-ordinated by the Financial Action Task Force (FATF), an inter-governmental body focusing on tackling money laundering, terrorist financing and other related threats to the international financial system. FATP publishes a series of recommendations and provides a consistent framework of measures for countries and FIs to follow. These international standards acknowledge that measures can be adapted to suit particular circumstances.

Intelligence Networks

National Financial Intelligence Units (FIUs) are increasingly collaborating to improve their effectiveness in fighting financial crime and stopping cross-border fraud. These include the Financial Crime Enforcement Network (FCEN) and the Finance Fraud Enforcement Taskforce in the US. Another group is the Global Financial Innovation Network (GFIN), which includes representations from 38 nations including the UK.

"We make the UK a hostile environment for money laundering by targeting individuals, disrupting their techniques, recovering and confiscating assets, and making it harder to abuse our financial systems." National Crime Agency

BREXIT

The UK's decision to leave the European Union (EU) will have significant impact on financial crime prevention departments. This will result in FIs needing to think and act more locally unless regulatory alignment and data-sharing is agreed. Organisations are busy implementing Brexit plans and this is expected to add cost and is seen as an argument against greater centralisation and consolidation of responsibilities.

"Consolidating our data, adopting structured messages and investing in new platforms and technologies, like AI and ML, will allow us to better protect our customers and ourselves."

"Brexit will require us to decentralise operations and create separate teams."

Geographical Trends

Although the payments industry is increasingly global in nature, some geographical variations should be given particular consideration. Under the current US administration, that market has become increasingly isolationist and this is filtering down to FI strategies. Conversely, many Asian markets are now more comfortable with adopting a global view and are looking more positively at international standards, regulations and opportunities to collaborate.

Benefits of Data

FIs understand the growing importance data can play in fighting financial crime. They are looking to make existing data more widely available for analysis and are creating large data pools that AI and ML can utilise. The shift to structured data through the adoption of new international

standards such as ISO 20022 is seen as a further positive move. Superior fraud detection is achieved by analysing an abundance of transactional data in order to effectively understand behaviour and assess risk, at an individual level.

Maturity

The level of maturity in moving to an integrated, centralised organisational model appears to vary considerably by geography. Canada is considered the most ambitious country, reflected in the number of initiatives currently underway both nationally and at an institutional level. The major US banks are also early adopters. The large UK and Nordic FIs are slightly behind, but these are significantly ahead of FIs from the German, Austrian, Swiss (DACH) region.

"The Canadian banks are seen to be exhibiting the greatest maturity and ambition in their thinking and approach."

Know Your Customer

FIs are required to conduct detailed KYC due diligence checks on their customers which address the need to verify identities, reveal the ultimate beneficiary ownership of companies (UBO), identify Politically Exposed People (PEP) and monitor and report on suspicious activity (SARs). A key market trend is the adoption of next generation screening tools and services that allow fully digital identify checking including by age and location. The reliance on paper-based identity documents is steadily being replaced by digital. These new tools allow enhanced due diligence to be undertaken and are a critical element in delivering AML compliance and fraud reduction. ■

> "Digital KYC checking is improving the accuracy, speed and cost of verifying customers, and is key to delivering AML compliance and fraud prevention."

Impact

As a result of the increase in number of regulations, we are seeing less innovation from established FIs. Brexit is also creating significant new demands and uncertainty for organisations. There are simply fewer resources and budgets remaining to be invested on innovation. The cost of change is also increasing due to increasing complexity.

"Brexit uncertainty is stifling innovation and slowing down resource consolidation and investment in new platforms."

This reduction in innovation is in direct contrast to Fintechs who are continually delivering new services and capabilities and, as a result, are starting to grow their market share. Fintechs typically favour in-house technology development over the licensing of commercial platforms. Some of the losses being incurred by Fintechs, however, could perhaps be attributed to their inexperience and lack of fraud and crime prevention system capabilities.

Collaboration

There has been a noticeable increase in cross-industry collaboration rather than competition between institutions on crime and fraud prevention. A good example of this is the increased engagement between trade associations including Pay.UK, UK Finance and the Emerging Payments Association.

The UK Payment Strategy Forum report advocated the need for greater collaboration and it is gratifying to see that this is now taking place through bodies such as the Financial Fraud Bureau (FBB), the Fraud Intelligence Sharing System (FISS), Action Fraud and the FinTech FinCrime Exchange (FFE). Another positive initiative is the work of the Dedicated Card and Payment Crime Unit (DCPU), which is a collaboration between the police and UK Finance. In the first half of 2019 the DCPU prevented £7 million of fraud, secured 39 convictions and disrupted 13 organised crime groups. This brings the total savings from reduced fraud activity to £600 million since the DCPU was set up in 2002. The main areas of recent success relate to stopping money mules, courier scams, fireplace fraudsters and fake ID fraudsters. Greater community intelligence derived from the strategic aggregation of data is a further benefit from the increase industry collaboration happening.

"Greater collaboration will continue to be a high priority if the battle against the criminals is to be won and customer confidence is to be maintained."

Complexity

Increased investment in defence mechanisms is needed in order to keep pace with the criminals. Attacks have become far more sophisticated and this has resulted in the need for the recruitment of more qualified resources. As these resources are scarce, FIs will need to rely more on AI and ML.

FIs will look for the optimal blend of supervised and unsupervised AI technologies and the combination of ML and fraud rules.

Changing Regulation

Regulations need to change over time in order to stay relevant and effective, as seen by the launch of AML5, PSD2 and PCI DSS4. Long-term commitment and investment are required, as crime and fraud prevention must become a business as usual activity rather than be treated as a one-time compliance project. ■

Opportunities, barriers and Challenges

Opportunities

Centralisation of resources and consolidation of systems can create many opportunities for FIs. Some of these have been explained above (see Advantages section). Others are described below.

"Investment in tech platforms helps stop fraud and criminal activity at the same time as improving the customer experience."

Fraud Detection

New technology platforms have been shown to improve fraud detection rates and reduce the number of false positives. Continual improvements in AI and ML will deliver greater accuracy and faster decision-making. ML helps data scientists determine which transactions are most likely to be fraudulent and reduce the number of false positives.

Customer Experience

Early adopters of the latest fraud platforms have been able to deliver a better experience to their customers. This can be achieved in a number of ways but results from having access to more data, a better understanding of the customer behaviour, the ability to communicate more proactively and the removal of unnecessary friction. Maintaining the right balance between providing a strong customer experience and regulatory compliance is critical. Delivering a great customer experience is so important because of customer expectations and competition levels being at record heights.

Risk-based

Partly as a result of the global shift to Risk Based Accountancy standards (RBA), FIs are seeking to invest in technology solutions that can help departments demonstrate regulatory compliance.

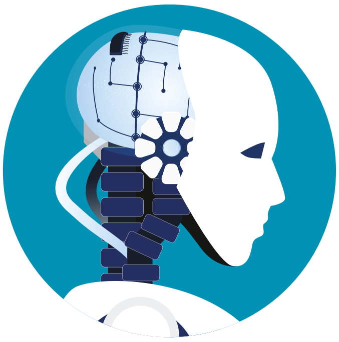
"There is an overlap of more than 50% of software functionality between legacy fraud and AML systems."

Barriers

There are many barriers to overcome before investing in new platforms and reorganising staff. Some of the more significant include the following.

Inertia

Many large FIs suffer from the problem of inertia. They are too often happy to retain the 'status quo', which is felt to be unthreatening. New platforms require significant investment and incur upfront costs, which cannot deliver the immediate payback that institutions frequently demand. And the consequences of poorly-managed platform migration are very high.



"Financial institutions and Fintechs are heavily investing in machine-learning analytics to help balance risk mitigation with the customer experience"

Risk

Large financial services companies have become increasingly risk averse through the fear of things going wrong and the high costs when things do. Many managers and employees are also resistant to change and there is a lack of cultural openness to there being a problem and learning from it. Too many managers don't wish to 'rock the boat' and risk 'being at the helm' when something goes wrong'. They are risk averse. Organisational culture and business risk appetite are also barriers that have to overcome.

"All change brings inherent risk and many FI executives fear the consequences if things go wrong on their watch."

Leadership

High quality leaders are needed to manage a reorganisation and ensure it is successfully. Managing larger teams, looking after more functions and implementing new enterprise tech platforms is a very demanding task and takes a highly capable leader. Strong executive sponsorship is also very important. ▸

Alignment

Frequently departmental objectives are not sufficiently aligned which can lead to a lack of co-operation and support for others, with disagreement over who as higher priorities, as has been seen with compliance teams. This may be due to inflexible operational procedures being in place. All of these barriers need to be overcome and buy-in achieved before the implementation of a new technology platform or organisational restructure.

Challenges

FIs face many challenges in preventing fraud and financial crime. In the UK, they are already spending over £1 billion annually in this fight but, beyond just spending more, how can effectiveness be improved? The following are just some of the challenges.

"The collective resourcing cost of the fight against financial crime among UK regulated firms now comes to over £1 billion each year."

Resource Shortages

Most organisations are struggling to recruit and retain the specialist resources they need. There tends to be permanent shortages in each department and it is particularly difficult to resource compliance departments. As threats continue to evolve, FIs need to continually invest in staff training to ensure they can counter criminal action.

Outdated Systems

Many organisations rely on out-dated fragmented technology systems, which lack today's required functionality and have poor data-sharing capability. Some of these may well have come through M&A activity. Old IT systems tend to be inflexible, are difficult to integrate and poor at delivering reports and management information. Technical constraints make it slow to implement system changes and performance tends to reduce over time.

Alerts

Each system triggers multiple alerts if attacks or unexpected events are noticed. As organisations typically operate multiple systems, the number of alerts quickly becomes unmanageable. The high level of false positives and false negatives are both particularly problematic. Greater use of behavioural intelligence technologies can be helpful to warn of abnormal employee behaviours and thus can stop more attacks originating from inside the organisation.

Analogue

Many organisations have failed to fully embrace the digitisation of data and legal documents and also suffer from the lack of structured data. For example, the digitisation of documents aids the identification of fake photographs on identification documents when accounts are being opened.

"Digital approaches and structured data need to be adopted to prevent fraud and financial crime." ■

Regulation, Technology & Innovation

Regulation

There are a very large number of regulations that apply to the provision of payment and financial services, which apply on a national, regional and global basis. It is impossible to cover all of these in this report but the some of the most significant to the fight against crime and fraud include the following.

AML

In Europe the 5th Anti Money Laundering (AML) Directive came into effect on the 10th January 2020. The main changes focus on enhanced powers for direct access to information and increased transparency around beneficial ownership, information and trusts. The regulation now covers virtual currencies and prepaid cards (with a new €150 limit) to help prevent these being used for terrorist financing purposes; improving safeguards for financial transactions to and from high risk countries; and ensuring national registers are accessible in all member states. The directive additionally strengthens requirements related to high value goods and reporting on politically exposed persons (PEP).

SARs

Suspicious Activity Reports (SARs) alert law enforcement to potential instances of money laundering or terrorist financing. The latest annual figures show that over 460,000 SARs were reported by FIs and other professionals to the UK Financial Intelligence Unit which, in turn, works with the National Crime Agency to assess the threat and take appropriate action.

"In the UK over 460,000 SARS were reported with each of these needing to be assessed."

PEPs

FATF and AML regulations require FIs to identify Politically Exposed Persons as part of their KYC customer due diligence processes. These individuals represent a higher risk as they are more likely than other clients to become involved in financial crimes like money laundering or the financing of terrorism. Around 120,000 PEPs have currently been identified.

PSD2

Within Europe the PSD2 regulations are having a major impact on all payment industry stakeholders including crime prevention teams. The PSD2 Regulatory Technical Standards (RTS) require the introduction of Strong Customer Authentication (SCA) in order to reduce fraud. A key focus is to tackle the £237 million of remote purchase card fraud that happened in the UK in the first half of 2019.

GDPR

FIs operating in Europe must comply with the General Data Protection Regulation (GDPR). This covers the use of personal information and requires transparency and customer consent. The processing of personal data for the purposes of fraud prevention is allowed, as it constitutes a legitimate interest of the data controller. But FIs must not fall into the trap of storing unnecessary data and then using it for other business purposes. Any breach of GDPR can incur very high penalties and so needs to be taken seriously.

Technology

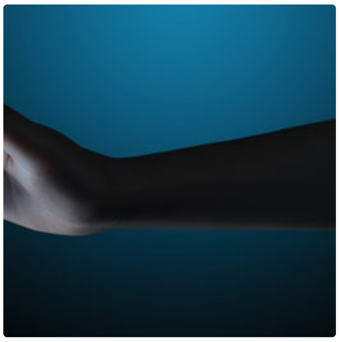
Most financial services professionals believe that technology is the most important factor in financial crime prevention. It should, however, be recognised that no 'silver bullet' exists and that is why investment in multiple technologies is required. Bringing together ML models, contextual data and expert workflows will aid detection and investigation of both fraud and financial crime.

"Investment in technology is critical if FIs are to win the battle against criminals."

Artificial Intelligence

AI has a critical role to play in the future and ML technology is rapidly improving, with the ability to detect fraud patterns before being identifiable by humans. ▸

"Compliance needs to be treated as a critical business-as-usual activity rather than a one-time project."



This is seen as the best chance for organisations to control losses and allow attacks to be shut down more quickly thereby limiting their impact. ML involves running complex algorithms that require significant volumes of reliable data, with poor data quality identified as a key obstacle to progress in this area.

"Artificial Intelligence must be understood properly and used effectively if the maximum benefits are to be realised."

FIs should be seeking to blend open source ML libraries with ML techniques in order to more accurately detect criminal activity.

Biometrics

The accurate confirmation of the identity of a customer is a critical aspect in stopping fraudsters. Biometrics is expected to play an increasingly important role in this new decade and we will see greater use of facial recognition technology, fingerprints, voice patterns and IRIS scans. Biometrics is the strategic options for most banks in delivering Strong Customer Authentication. This will largely be implemented through smartphone technology, which is now being used by the majority of customers.

Cloud

Additionally, cloud based data and technologies have great potential in financial crime prevention. This is an area where FIs are looking to invest in order to improve results at the same time as reducing costs. Some FIs have previously expressed concerns about greater adoption of cloud services for security reasons, but these could be addressed if best implementation and security practices are followed.

Card Payment Security

Technology has a major role to play in preventing payment card fraud. Tokenisation of card details is a high priority for online businesses and Point-to-Point Encryption (P2PE) for merchants selling from physical premises; both of these help stop card details being used after a data breach. PCI DSS compliance remains the best defence for all retailers and merchants. This year, most online businesses will be adopting the second version of 3DSecure in order to become compliant with the PSD2 Strong Customer Authentication.

"Merchants will be adopting 3DS v2 before March 2021 in order to achieve Strong Customer Authentication, otherwise transactions will be declined."

Emerging Technologies

There are many other technologies currently being evaluated by FIs which include: robotic process automation, natural language processing (to help manage high volumes of cases) and distributed ledger technology (DLT). Greater adoption of these emerging technologies is expected in the next few years.

"Technology can detect suspicious behaviours for review, then automate manual tasks within a flexible, unified case manager to helps stop fraud and criminal activity at the same time as improving the customer experience."

"Current Tech platforms have real limitations and that is why investment in unified platforms and emerging technologies is required."

Unified Fraud and Crime Platforms

Around the globe, regulators are encouraging organisations to develop and embrace enterprise platforms that unify fraud and compliance. This allows FIs to complement existing AML capabilities with complex variables and aggregations, profiling of any entity including beneficiaries, use ML models with explainable AI, real-time screening and alerting, unified alert and case management. A robust enterprise fraud solution combines a range of analytic models and behavioural profiles in order to understand evolving transaction patterns

Fraud Models

Black boxes are increasingly being used to create, test and decide on optimal fraud models. It is important that these are then moved into production faster. A dilemma, however, is that a model seen to be the most accurate may be the hardest to explain to others. Providing regulators with practical experience will help enhance their understanding of these models.

"The best outcomes are likely if regulators are approachable and FIs take an embracing and collaborative approach."

Drivers for Adopting Technology

Strengthening regulatory compliance, reducing crime levels, improving the efficiency of current processes and, of course, reducing costs are some of the main drivers for adopting technology. New technology also helps prevent payments fraud and financial crime by allowing banks to design, simulate, and implement new strategies that work across all digital banking interactions and cover customer authentication, payments, and account maintenance. Behavioural analytics based fraud management solutions can leverage the power of ML and AI.

"Greater use of technology and adoption at an enterprise level is key to reducing levels of fraud and financial crime."

Whether the threat comes from social engineering, phishing or other sophisticated fraud techniques, the latest technology solutions deliver the profiling and historical context needed to protect against account takeover associated with credit transfers, P2P transfers and mobile payments.

"We must not forget the advantages of new technologies are also available to criminals."

Innovation

Emerging technologies and new collaborations are helping to turn the tide on fighting financial crime. Innovations are being applied in the following ways.

"We all need to experiment with new technology, and together see how we can tackle criminals who want to exploit the financial system." FCA

Trusted Data

Clean, complete and reliable data is the foundation of effective technological innovation. Fuelled by trusted data, technology can help organizations in numerous ways, from reducing the burden on compliance teams, to pinpointing potential risk; from uncovering hidden networks of potential financial crime activity to improving the customer experience.

Digital Onboarding

There is plenty of innovation in the area of customer on-boarding, allowing FIs to carry out more effective KYC checking. This includes the accurate identification of clients, the verification of customer data and the screening against sanctions databases. The digitisation of data is a key element of this. Challenger banks are often at the forefront, using scanned document, video and voice clips, plus other forms of biometrics.

Mule Accounts

In 2019 Pay.UK introduced the Mule Insights Tactical Solution (MITS), a new technology that helps track suspicious payments and identify money mule accounts. This enables suspicious payments to be tracked as they move between bank accounts, regardless of whether the payment amount is split between multiple accounts, and if those accounts belong to the same or different financial institutions. MITS creates a visual map of when and where money has moved, providing data-driven insights and new intelligence which allows fraud teams to take action. By bringing together payments data from multiple banks and overlaying it with analytics and algorithms, MITS can accurately pinpoint individual mule accounts involved in suspected illegal activities. This system has the potential to disrupt fraud and money laundering worth millions annually.

Confirmation of Payee

Authorised Push Payment (APP) scams have become a major area of fraud, particularly in the UK, where there were 84,624 reported incidents annually, which resulted in gross losses of £353 million. The Payment Systems Regulator (PSR) has required Pay.UK to coordinate work with its member banks to establish a Confirmation of Payee (COP) service that provides an account name checking service before a payment is made. Once the scheme is in place, anyone setting up a bank payment will be alerted if the name on the recipient account does not match, is incorrect or misspelt, meaning it can be corrected before a payment is made. COP will help fight APP scams, where people are tricked by a fraudster into sending money to the wrong account, as well as picking up user account detail entry errors.

"The new Confirmation of Payee service will help stop payments being made inadvertently to criminals."

The regulator requires this new fraud prevention service to be operational by the end of March 2020. It should help bring authorised push payment scams under control. Several other countries are watching this UK project closely and are expected to introduce similar services.

Privacy Enhancing Technologies

Another area of innovation being promoted by regulators is the use of Privacy Enhancing Technologies (PETs) that can facilitate the sharing of intelligence between firms, regulators and international law enforcement agencies without compromising data protection requirements. PETs seek to balance the need to share more data with GDPR compliance.

APIs

A major innovation is the greater exposure of functionality as services and use of Application Programme Interfaces (APIs) to allow systems to access these. Innovative FIs are publishing more services and allowing secure access via APIs. Open banking is a good example of this trend. ■

Recommendations

- FIs are encouraged to take a more holistic approach to fraud, compliance and cyber security and take an end-to-end view. The scale of the problem is growing and this requires organisational and system changes to be made.

- Greater investment in technology is required in order to improve protection from fraud attacks and strengthen crime prevention defences. Current strategies, structures and systems simply can't provide the protection needed.

- Financial service providers should be adopting enterprise level platforms that address both fraud and compliance needs and utilise ML and AI. A combination of the best people, processes and technologies are needed to win the fight against crime.

- With payments increasingly being processed in real-time, decisions have to be taken faster and this requires new approaches to fraud and crime prevention being introduced. The latest fraud platforms have been designed to operate with real-time payments.

- Organisational structures should be revised to enable greater collaboration across fraud, risk and compliance teams. Departmental silos need to be removed and scarce data scientist resources must be used more effectively.

- An enlarged pool of structured data is necessary in order to improve decision-making and prevent fraud and financial crime. Data must be digitised and shared across an organisation. Accurate customer verification and strong authentication are now regulatory requirements.

- IT departments should liaise more closely with fraud and compliance departments due to the growing importance of cyber security and number of attacks. Behavioural intelligence techniques can help protect against insider attack threats.

- The lack of a national ID verification programme is making it harder to prevent fraud and financial crime. This is making it easier for criminals to operate and making defence the responsibility of each and every FI.

- Greater collaboration between regulators, FIs and technology providers needs to be encouraged. Crime and fraud should not be seen as competitive issues. The collaborative initiatives underway are encouraging and should be supported and expanded.

- FIs need to ensure that they maintain the right balance between providing a strong customer experience, fraud prevention and regulatory compliance.

About FICO, Benefactor of Project Futures

FICO (NYSE:FICO) is a leading analytics software company, helping businesses in 90+ countries make better decisions that drive higher levels of growth, profitability and customer satisfaction. The company's ground-breaking use of Big Data and mathematical algorithms to predict consumer behaviour has transformed entire industries. FICO provides analytics software and tools used across multiple industries to manage risk, fight fraud, build more profitable customer relationships, optimize operations and meet strict government regulations.

With thanks

To all members of the Project Futures team and to Mark McMurtrie, Director of Payments Consultancy Ltd, who moderated the workshop and authored this report. The EPA would also like to thank the Benefactor of Project Futures, FICO, for their backing of the project and its workshops, and in helping identify technology and future innovations that will spark a dynamic change for both businesses and consumers.

To work with us to create a better payments industry in future...

To join our Project Futures (EPA members only) contact:
calum.stephens@emergingpayments.org

To find out more about joining the Emerging Payments Association, contact:
keri.farrell@emergingpayments.org

Workshop participants

BANKING CIRCLE	FICO Decisions
BARCLAYS	ingenico GROUP
LLOYDS BANKING GROUP	buguroo
ZIP	PROTEAN RISK
Payments Consultancy Limited	EPA EMERGING PAYMENTS ASSOCIATION

EMERGING PAYMENTS
ASSOCIATION

Emerging Payments Association

The News Building,
3 London Bridge Street,
London, SE1 9SG, UK

Tel: +44 (0) 20 7378 9890

Web: emergingpayments.org

Email: info@emergingpayments.org

@EPAssoc

in 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 payment companies. Its goals are to strengthen and expand the payments industry to benefit 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 150 members and is growing at 30% annually. Its members come from across the payments value chain; including payment schemes, banks and issuers, merchant acquirers, PSPs, merchants and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.