EMERGING PAYMENTS ASSOCIATION

SUPPORTED BY REFINITIV

Financial Crime, Payment Fraud and the Role of Digital Identity

2021

JANE JEE
Leader, EPA's Project Financial Crime
Chair, **Kompli-Global Limited**

WELCOME

Thank you for your interest in this Emerging Payments Association (EPA) white paper created as part of our *Project Financial Crime.* The primary research for this paper draws on the support of key industry stakeholders and subject matter experts including our Project Financial Crime team and the broader EPA membership. In this paper we provide an overview of the current landscape, emerging threats and insights into how fraud controls can be improved.

Criminals understand how they can profit from financial crime and commit payment fraud as evidenced by the escalating number of attacks and levels of losses incurred. I find it worrying how they are now working more closely together, in effect creating a crime marketplace and been quick at adopting the latest technologies. Promisingly, our research highlights some initiatives that are making a real difference and also suggests ways for the industry to collaborate to a greater extent.

As part of the research, these topics were discussed in an EPA Projects webinar with a distinguished panel of expert speakers: Professor Michael Levi from Cardiff University, Alison McDowell representing the Department for Digital, Culture, Media and Sport, Caitlin Sinclair from Refinitiv and Western Union's Alex Beavan. If you missed this discussion I would strongly encourage you to check it out now as it offered many helpful suggestions.

I'd like to give a big "thank you" to Refinitiv for sponsoring the research and to EPA Ambassador Mark McMurtrie who conducted the interviews and authored the report. I hope that, like me, you find it to be an interesting read. We welcome your feedback. ■

INTRODUCTION

The issue of Financial Crime and Fraud Prevention has never been as important as it is today. The National Crime Agency (NCA) estimates that the total cost of organised crime to the UK economy amounts to £37 billion annually.

Anti Financial Crime - the four key areas

MONEY LAUNDERING

SANCTIONS & EMBARGOES

FRAUD

CYBER CRIME

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. Sanctions and Embargoes prevent money flowing to blacklisted nations and individuals. Payment fraud refers to any false or illegal transaction often including credit and debit cards, remote banking and authorised push payments. There is a big detrimental humanitarian and environment impact in addition to the amount of financial losses.

Research from the Nilson Report shows that card fraud continues to grow annually and is estimated to total $30 billion globally in 2020 equating to 7 cents per $100 card volume and to increase to $38 billion by 2027. ■

Table of Contents

RESEARCH HIGHLIGHTS

	DESCRIPTIONS
Current landscape	• We are not winning the war and criminals are getting cleverer • COVID has changed the market and increased levels of attacks • Fraud keeps growing especially APP and remote purchases • AML must remain a top priority • Consumer education is lacking and criminals are exploiting this
Emerging threats	• We are seeing an increase in attack types and volumes • Botnets and Synthetic IDs are being used at scale • Company registration weaknesses are being targeted • Realtime payments make it harder to stop fraud • Brexit may result in less data sharing and collaboration
Current protection gaps	• Siloed operations and systems exist at most FIs • Static rules and transaction monitoring are now insufficient • It is taking too long to rollout new technologies and programmes. Adoption must be accelerated • Outdated approaches are creating vulnerabilities • Poor communications and practices exist and require attention
New technologies	• 3DS and COP should reduce CNP and APP fraud losses • Biometrics, including behavioural, will be key to changing the current position • ML and AI are a must have for all FS providers going forward • W3C are developing helpful new standards including SPC, DID and payment request API • P2PE and Tokenisation will protect card payments if adopted
Current limitations	• Legacy system constraints exist making defence harder • Limited data sets are being used due to lack of system integration and data sharing • Analogue thinking, out-dated mind-sets and employee skill sets • Need for next generation platforms and digital FinCrime sandboxes
Role of digital identity	• Seen as having a critical role going forward • Will provide a secure foundation layer to prevent crime upfront and on an ongoing basis • Will deliver assurance and trust between multiple stakeholders through Digital Identity and Trust Frameworks • Will offer stronger protection for private and public sector services • Will enable access control to age-restricted products and services
Collaboration and data sharing	• Regulatory clarity on the acceptability of data sharing, addressing GDPR concerns • Improvements in risk decision making require more data • Greater internal data consolidation and departmental collaboration • Adding data into collaborative networks and data lakes
Challenges and barriers	• Status quo. Current platforms and approaches are insufficient • Inability to share data today • Organisational attitudes, tone of board, lack of departmental collaboration • Regulators are struggling to adjust to new technologies, payment options and types of FS provider • Law enforcement lacks resources to prosecute many cases • Low levels of consumer and employee education and awareness

CURRENT LANDSCAPE

We are not winning the war

Our interviewees were clear that we are constantly playing catch up with the criminals and that the current defence approaches are broken and fundamental change is required. Society, organisations and individuals are all suffering as a result of these crimes and collectively we are facing an acceleration in risk. In the majority of cases the criminal is at least one step ahead of Financial Services (FS) providers.

Today, it is far easier for criminals to create fake accounts and to buy complete identities at a relatively low cost. Due to a rapidly increasing range of payment methods and the faster movement of funds, much faster risk decision-making is required as there is less time available to stop abuse.

"Despite investing considerable resources to comply with a plethora of financial crime regulations and operating multiple fraud prevention solutions, we don't seem to be winning the war against the criminals."

Global bank

Interviewees felt that most organisations are standing still from a fraud perspective whilst the overall market they are operating in is growing.

Fraudsters are innovating at scale

We learnt how fraudsters are investing more time and money to generate higher rewards. Criminals are working together as part of an ecosystem each with their own area of specialism. They buy from and sell to each other, and utilise the latest technologies allowing them to target lower sized frauds at volume and pace.

There is a greater breadth of attack vectors to be defended against and the criminals are showing higher levels of professionalism. The number of scams being initiated far exceeds levels previously seen and these are much harder to spot. FS providers constantly have to react to new threats.

"It is 4000 times easier to commit crime today thanks to the amount of technology available and the fact that victims tell you everything you want to know."

Frank Abagnale
Convicted fraudster, author and inspiration for Steven Spielberg's 'Catch me if you can' film

Cybercrime continues to grow

Our interviews confirmed that cybercrime continues to grow globally with the McAfee 'Hidden Costs of Cybercrime' survey estimating losses totalling more than $1 trillion last year. The UK National Cyber Security Centres highlights a 40% increase in ransomware attacks and 600% more malware attacks.

COVID changed the market

The COVID crisis has dramatically accelerated digital payments adoption with contactless payments now accounting for 27% of all UK payments according to latest UK.Finance statistics. Online purchases and the usage of mobile wallets have also grown significantly as everyone was forced to adapt. It is clear that the crisis has accelerated digital transformation across all sectors of the economy and brought forward changes that would have previously taken years.

The criminals quickly spotted the opportunities available from all the disruptions and changes in consumer behaviour. With physical shops closed a new breed of digital consumers (described by interviewees as 'digital virgins') started buying online but lacking the knowledge to spot a scam or fake website or know how to protect their sensitive personal information. Additionally, many businesses entered the eCommerce world for the first time through the launch of apps and eCommerce websites without fully understanding how to ensure they and their customers were to be protected. Also, employees forced to work from home have often been operating in insecure working environments. The criminals have had a field day and exploited every available loophole. The COVID crisis resulted in a massive increase in scams especially relating to PPE supplies, fake employment roles, puppy purchases, and romance scams.

"I think we should expect a crime wave for years to come after the trauma of 2020 and the COVID-19 pandemic."

Tony Sales, The Big Con

Government backed business loans (UK BBLS) were introduced quickly but perhaps without sufficient due diligence checks being undertaken. Initial forecasts were that these could have amounted to £15-£26 billion of losses for the UK economy but it is good to hear that this has now been revised down significantly. Collectively UK banks declined 44,000 fraudulent applications, which could have amounted to £1.6 billion of bad loans.

AML remains a top priority

Money Laundering continues to be a major area of concern for all payment industry stakeholders. The United Nations estimates that the amount of money laundered globally equates to 2-5% of global GDP, amounting to $800 billion to $2 trillion US dollars.

Encouragingly, tighter financial regulations including the European 6th AML directive, the US Anti-Money Laundering Act of 2020 and high investment made in compliance programmes by banks are starting to make an impact but we still have a long way to go if Money Laundering is to be controlled.

Banks faced record fines totalling $12 billion in 2020 for Money Laundering, violation of KYC and operating guidelines and personal data breaches. The US market leads this league table with 12 fines being issued totalling $11.1 billion.

The low absolute number of fines being issued is a reflection of the difficulty in assigning money laundering responsibility and the scarcity of regulatory and law enforcement resources.

Yes, banks are investing very heavily in AML compliance programmes, with one estimate suggesting £28 billion being spent by UK FS firms per year. However, interviewees noted that much of this was focussed on demonstrating compliance to the regulators rather than actually stopping criminal activity and fraud.

2020 Bank Fines Report

RANK	COUNTRY	FINE TOTAL	FINE COUNT
1	US	**$11.1 Biilion**	12
2	Australia	**$981 Million**	3
3	Israel	**$902 Million**	1
4	Sweden	**$539 Million**	2
5	Germany	**$215 Million**	4
6	UK	**$156 Million**	4
7	Canada	**$127 Million**	1
8	China	**$83 Million**	7
9	Iran	**$37 Million**	1
10	Turkey	**$21 Million**	1

"UK Financial Institutions are spending £28 billion per year on AML Compliance, which is equivalent to half of the national defence budget, but much of this is to meet increasing regulatory expectation, rather than rising criminal threats."

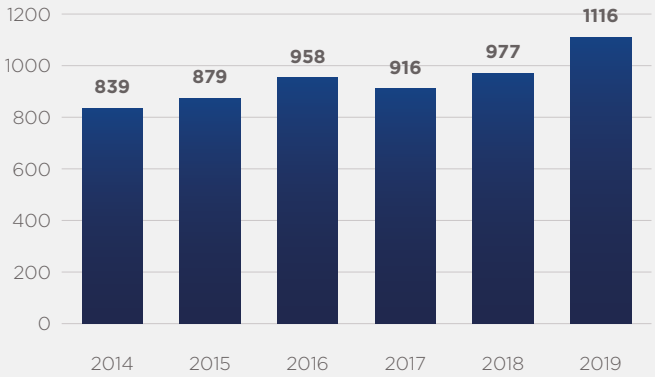
Financial crime specialist

EU AML Changes

This month we learnt that the EU intends to significantly strengthen its fight against Money Laundering. The proposals include:

- The transfer of the most important provisions of the existing Anti-Money Laundering Directive into a new Regulation. This means that uniform standards against money laundering will apply in the EU. Unlike a directive, a regulation does not have to be transposed into national legislation.
- The existing fourth EU Anti-Money Laundering Directive and its 2018 extension (AMLD5) will be repealed and replaced by a new directive. This directive will address any issues not covered by the new AML Regulation.
- The creation of a EU Anti-Money Laundering Authority. This will strengthen the independence of the new EU supervisory authority vis-à-vis the interests of the member states.
- Strengthening the regulation of crypto-asset providers and extending due diligence requirements.

Suspicious Activity Reports for US Depository Institutions in Thousands



SARS rising

The number of Suspicious Activity Reports (SARs) being filed in each country continues to increase annually. In the US the Financial Crime Enforcement Network (FinCEN) reports that over 1.1 billion were reported in 2019. These high levels, which are seen in every country, show how big a task it is to manage AML. This is partially a reflection of the annual growth of the number of financial transactions that are being performed.

"Customer present card fraud has been brought under control thanks to the introduction of Chip & PIN technology. This shows what can be achieved through the development of international standards, industry wide co-operation and the upgrading of products and processing systems."

ingenico
a Worldline brand

Fraud market statistics

The Crime Survey for England and Wales confirms that fraud makes up the majority of crime with 3.7 million incidents being reported, compared to 356,000 incidents of burglary and 124,706 cases of theft. Additionally, identity fraud cases are also growing dramatically and now make up 61% of the total cases held in the British National Fraud Database.

The UK market publishes comprehensive payment fraud statistics annually and these may be seen as a barometer for other markets. The latest 'Fraud the Facts' report from UK.Finance shows that overall £1.26 billion was lost to fraud in 2020.

It is good news that collectively UK banks stopped £1.6 billion of unauthorised fraud losses through fraud prevention initiatives and the Dedicated Card and Payment Crime Unit (DCPCU) arrested over 122 fraudsters preventing an estimated £20 million of fraud.

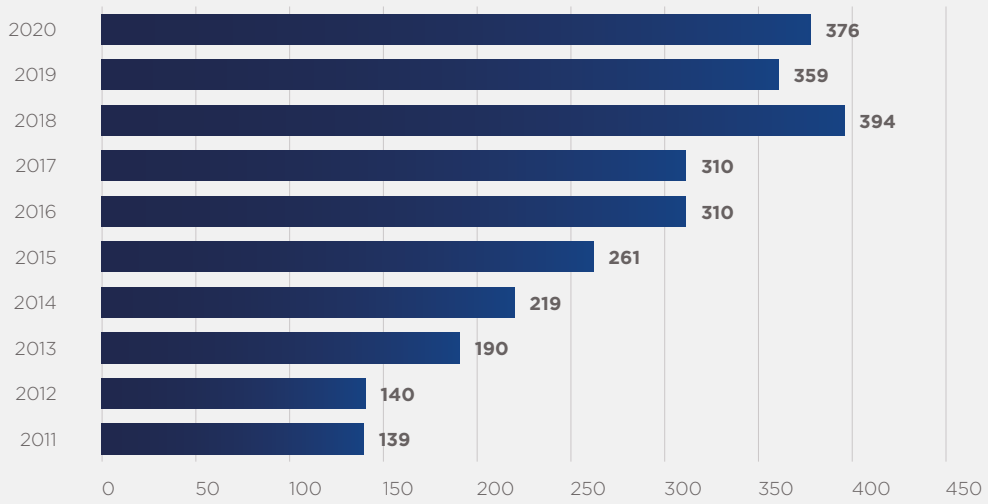
It is hoped that the rollout of Confirmation of Payee (COP), which checks for a match of payee name against the entered sort code and account number, will reduce APP losses and that Strong Customer Authentication (SCA), which uses multi factor authentication, will help reduce eCommerce CNP losses.

CATEGORY	AMOUNT	% CHANGE
Card payment fraud	**£574 million**	+3% by volume -7% by value
Authorised push payment fraud	**£479 million**	+22% by volume +5% by value
CNP remote purchase fraud	**£452 million**	+12% by volume -4% by value
Remote banking fraud	**£197 million**	+64% by volume +31% by value
Mobile banking fraud	**£22 million**	+48% by volume +41% by value
Lost and stolen	**£79 million**	-30% by volume -17% by value
Card ID theft	**£30 million**	-36% by volume -21% by value
Card not received	**£4.5 million**	+7% by volume -15% by value
Face to face retail fraud	**£49 million**	-24% by value
CEO fraud	**£10 million**	+24% by volume -41% by value

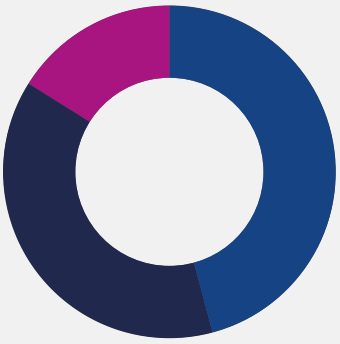
"The UK lost £1.26 billion to payment fraud in 2020"

UK Finance

UK Internet/eCommerce fraud losses £ million

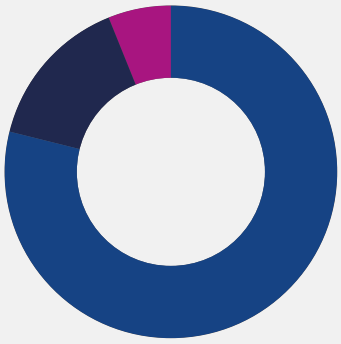


UK Payment Fraud Losses £1.26 Billion



Payment card **46%**
App **38%**
Remote banking **16%**

European Card Payment Fraud Losses €1.43 Billion



CNP **79%**
POS **15%**
ATM **6%**

The European Central Bank 2020 fraud report shows similar trends to the UK market with overall card fraud totalling €1.8 billion which represents 3.7 cents per €100 worth of transactions. Similar to the UK, the largest proportion of card payment losses come from CNP remote purchases accounting for €1.43 billion and 79.5% of the overall amount, 11.2% from Lost and Stolen, 5.4% from Counterfeit cards, 0.6% from card not received. Across the channels where fraud occurred, 79% came from the internet, mail or phone, 15% from POS terminals and 6% from ATMs. The latest figures from Euromonitor show that in 2020 the greatest decrease in overall fraud was achieved by Denmark (-48%), Hungary (-39%) and the UK (-7%) whilst fraud grew in Norway by (+172%), Poland (+47%) and in Greece (+20%).

Consumer education is lacking

We consistently heard of the low levels of customer understanding of crime prevention techniques and how this creates opportunities for fraud. The COVID pandemic has resulted in many new or inexperienced digital consumers and businesses that are vulnerable to cyber attacks and scams including phishing, vishing and smishing.

However, consumer inertia to new processes and the use of fraud prevention tools must be overcome. FS providers, therefore, have an important role to play in better educating consumers on how to avoid becoming a victim and on the use of security tools and follow best practices.

We heard that during the last 18 months, an increasing number of financial services and payment providers have introduced new tools within their digital account management sites to allow customers to take direct control of their account spending and setting their own transaction limits and daily spend amounts.

Crypto needs new thinking

Cryptocurrencies are now being adopted as part of the mainstream with usage growing, despite regulatory concerns and pricing volatility.

"Crypto customers may not wish to be tracked for privacy concerns but they should not think their payments are anonymous. Crypto exchanges can and do share data following a court order or regulatory request and have a good record of collaborating with each other."

CoinPayments

But regulators are struggling to determine how best to regulate crypto usage, given the dynamic nature of this new payment technology. Our interviewees highlighted that current FinCrime and fraud prevention controls were not designed with crypto in mind and as a result require adjustments to be made.

Cryptocurrencies are increasingly being used by criminals to commit money laundering. Authorities recognise this and have increased their number of investigations. The British Police Economic Crime Command have this year had some big successes seizing first £114 in June and then in July £180 million of cyrptocurrencies which were suspected of being used to launder money. ■

"Advances in technology has led some criminals to move to more sophisticated methods to launder money, such as using cryptocurrencies."

British Transport Police

EMERGING THREATS

“Fraud is like a balloon, you squeeze it in one place and it always pops out in another spot.”

Payments Consultancy

What has not changed?

The main financial crime threats continue to be from organised crime groups, terrorists, drug gangs, child exploitation and cyber attacks. Criminals are not impinged by national borders and are always looking for the weak point in defences, whether physical, legislative or technological. The risks to organisations and individuals remain much the same as they always have been, but criminals are now far better at exploiting vulnerabilities at scale. We recognise that attacks constantly shift and will always move to the weakest points.

We heard how some regulators appear to be struggling to keep pace with the changing market and technology landscape. This is not a new phenomenon; they remain more comfortable overseeing traditional banks. But we also heard of other regulators from South East Asia and the Middle-East who are doing a good job in transitioning to the new market realities. Regulations often appear to be failing to keep up with the latest technological developments.

What has changed?

Fraudsters are highly professional, well resourced and organised. They make use of all the latest technologies and resources available to them.

One of the most significant changes is the increase in botnet attacks. These have progressed from Distributed Denial of Service (DDOS) to more Credential Stuffing attacks with the objective of validating stolen credentials. We heard how there are millions of malicious robot calls being made daily and also how criminals are co-ordinating operations into what are called ‘fraud farms’ in order to circumvent anti-bot defences.

“Botnets are being deployed at scale by criminals to attack organisations and customer accounts. New approaches, technologies and platforms are needed in order to tackle this problem.”

cybertonica

“The consequences of an attack are far greater than they ever used to be. This includes the high financial sums involved, the reputational damage and loss of customers.”

Kompli-Global® SAFE IN THE KNOWLEDGE

“The regulators are currently reviewing how they can become more familiar with Cryptocurrencies and the best ways to monitor and control them.”

CoinPayments

More data is available to the criminals

Fraudsters have access to many more consumer data points than previously. Social engineering has become professionalised and customers are too open about sharing details. Social media data harvesting is one popular technique being used by criminals.

"It used to take many weeks of hard work to get the identity information needed to commit fraud but now this can be gathered in 15 minutes and it's a very safe environment to work in" Frank Abagnale, Fraudster and Author

"Social engineering has become a big issue and one that can't be solved entirely by technology."

REVELOCK

A major area on concern relates to synthetic identities where criminals combine real and fake information to create a new identity. The real information used in this fraud, such as a credit card, is usually stolen. This information is used to open fraudulent bank accounts and then to make money transfers and online purchases.

"The growing use of Synthetic ID is a cause for great concern."

cybertonica

We heard how all of this data is being monetised by criminals through marketplaces especially on the dark web. It is worrying to learn how complete identities can now be purchased at a relatively cheap price, given the long-term impact of identity fraud. On a macro level the primary impact considered is one of economic losses ignoring the equally damaging human and psychological consequences for individual fraud victims.

Increase in attack types and volumes

The number of attack types continues to grow each year. Each type has its own characteristics, occurrence frequency and size of financial losses. Those regularly highlighted in our research include: account takeovers, COVID related scams, Money mule recruitment, deep fake videos and SIM swaps.

Company registrations

Our research identified company registration and ownership structures as being particular areas of concern. It is felt that it is currently too easy for criminals to set up fake companies using false documentation and hide ultimate beneficiary owners behind umbrella companies. Data inaccuracies, shell companies and issues with public registers are further AML challenges that have to be overcome. We learnt how criminal networks are exploiting these vulnerabilities to launder money.

Contactless

Contactless card payments are becoming increasingly popular all around the world with the COVID pandemic accelerating adoption as it was felt to be a safer way to pay in-store. Regulators are now allowing higher value transactions to be made by a contactless card but interviewees expressed concerns that this may lead to higher levels of card fraud.

CLUSTERS OF PAYMENT RELATED FINANCIAL CRIME		
Money laundering	Abuse of payment card	Push payment fraud
Transaction laundering	Account takeover	First party payment fraud
Direct debit fraud	Merchant fraud	Cash
eWallet fraud	CEO / Invoice fraud	Cheque fraud

"We may be inviting fraud if we don't implement higher contactless transaction limits thoughtfully. Greater customer and merchant data will be needed in order to manage the risk effectively."

CURVE

Brexit

It is too early to know the full implications of Brexit on FinCrime but this may reduce the opportunities for data sharing and collaboration. Interviewees expected to see increased regulatory divergence over time. It was mentioned that this would bring both flexibility and complexity. The first signs of regulatory diversity have been seen with the UK delaying active enforcement of PSD2 SCA for eCommerce payments until March 2022. ■

CURRENT PROTECTION GAPS

Siloed operations

Consistently the first gap raised in our research interviews relates to siloed operations and systems. Banks have multiple departments working in FinCrime, Fraud prevention and Cyber security, each with their own remits, priorities and ways of working. Also, the IT systems used by each department tend to have a narrow focus and do not work efficiently together. Each department uses slightly different types of data but overlooks the overall benefits from aggregating all of the data. Additionally, siloed thinking can be as much of a challenge as siloed systems. We continually heard how more inter-departmental collaboration and data sharing is needed.

Even within a single department you will often find legacy and new platforms working alongside each other, perhaps as a result of M&A, but not sharing data effectively with each other. Too frequently the full data points that are available within an organisation are not shared. This prevents an organisation having a 360-degree view of their customer.

Even where data is available the quality of the data may be questionable, often it is not clearly structured and lacks realtime data sources.

Slow rollout of fraud prevention programmes

The banking sector is introducing several new solutions to tackle fraud, but these are taking too long to be implemented. Card issuers, networks, acquirers and merchants are introducing Three Domain Security (3DS) to deliver strong customer authentication in order to secure remote commerce purchases. However compliance deadlines have repeatedly been delayed.

The Confirmation of Payee (COP) account name checking service is another helpful tool to avoid a customer making misdirected payments perhaps as a result of a scam. But the U.K.'s Payment Systems Regulator (PSR) only required the COP service to be adopted by the largest UK banks and implementation deadlines were delayed, which meant that criminals could continue to exploit vulnerabilities and commit Authorised Push Payment (APP) fraud.

"Confirmation of Payee needs to be more widely implemented if APP fraud is to be reduced as fraudsters always switch their attention to the weak points."

Fraud Subject Matter Expert

Outdated approaches

Many organisation continue to place an over reliance on the use of transaction monitoring tools and fail to take into account wider customer behaviour and environment. Interviewees highlighted the need to combine inbound and outbound payments monitoring and that outdated fraud frameworks and strategies continue to be run. A further area of concern relates to the continued use of static fraud rules. Experience shows that these quickly become ineffective against changing criminal behaviour.

"We continue to see an overreliance on the use of static fraud rules and transaction monitoring. Thanks to the higher velocity and speed of transactions these no longer offer sufficient protection."

REVELOCK

"To make effective risk based decisions you need access to the right data. This should be consolidated, richer, layered and of higher quality. Also a greater focus should be placed on reviewing the behaviour of the customer and comparing this against their history rather than looking solely at an individual transaction."

KPMG

FS providers conduct KYC checking at the time of account opening but some believe pay insufficient attention to perpetual or ongoing KYC reviews during the course of the customer relationship. We heard that some FS employees have out-dated skill sets and are held back by 'brick and mortar' organisational thinking as well as some compliance teams becoming stuck in their ways.

Poor communications and practices

Our research highlighted many instances of poor communications and industry practices that if addressed would lead to a reduction in crime. Interviewees frequently mentioned the weak communications FS firms have with their customers and how there is insufficient industry level collaboration on creating and promoting fraud awareness communication campaigns.

Even when campaigns are developed like the UK's 'Take Five to Stop Fraud' campaign, which contains clear and practical advice, not enough consumers are aware of it as a result of poor promotion by banks and the lack of an effective marketing campaign. Encouragingly, HSBC recently announced a fraud awareness app for use by their business customers.

CIFAS and UK Finance partnered to develop the 'Don't be fooled' campaign to deter young people and students from becoming money mules. This campaign highlighted the risk of being enticed to move money on behalf of a criminal and the negative long-term impact it can have on a young person's life. Interviewees questioned how many young people had seen this campaign and would have liked to see greater intelligence sharing of the campaign results.

Additionally, it is felt by interviewees that many banks could do a better job of promoting the range of security and control services that they do offer. Customers have insufficient clarity on what they can expect from their bank and what is their own responsibility. FS providers need to be more proactive in delivering fraud and crime education and awareness services. Interviewees felt that 'friendly card fraud' losses could be reduced if greater attention and sensitivity were applied to this area. This includes the unauthorised use of a card within a household as well as the denial of a legitimate transaction perhaps through embarrassment.

Interviewees commented that it is good to see more banks like NatWest enabling customers to self manage daily transfer and spend limits and thereby reducing their exposure to fraud. ■

"There is no silver bullet to managing risk as criminals quickly switch their attention to the weakest link, therefore a holistic approach is needed."

CURVE

"The top ways to identify eCommerce fraud are by analysing the customer profile, location, order details and the device ID."

Risk management solution provider

WHICH TECHNOLOGIES OFFER THE GREATEST POTENTIAL

3DS and COP

EMV Three Domain Security (3DS) multi factor authentication is being introduced to tackle remote purchase fraud and COP to help reduce APP fraud. Both technologies are expected to have a major impact on reducing fraud levels once implementation and rollout have been completed. An international specification for COP would be helpful to accelerate worldwide adoption.

"3DS technology allows customers to be authenticated securely. Adoption by issuers, acquirers and merchants will deliver regulatory compliance and help bring levels of remote purchase fraud back under control."

consult hyperion
securing tomorrow's transactions

Biometrics

Biometrics is expected to play a far greater role in FinCrime and fraud prevention strategies as a result of the increased user adoption of smartphones. No single biometric is the clear leader, each has its own place and often multiple biometrics will work alongside each other. As with all fraud prevention strategies, results have to be balanced against friction and cost.

Finger vein technology has its advocates but currently usage is largely restricted to corporate banking access due to the high costs and logistical issues associated with the supply of finger vein hardware readers.

"India's Aadhaar programme has demonstrated the power of biometrics, using a combination of Iris patterns and Fingerprints to create a system that is accessible to the entire population."

consult hyperion
securing tomorrow's transactions

Face ID and Fingerprint recognition has become the primary secure access points to smartphones. However we heard during our research that facial recognition accuracy varies by skin tones and gender. The FS industry needed to introduce 'Liveness' checks as part of electronic KYC enrolment processes in order to prevent fraudsters presenting static images. Usage of Voice biometrics is growing in environments associated with Voice Commerce and IOT devices.

Use of Behavioural Biometrics (BB) is on a fast growth path particularly for SCA compliance. This technology creates a user profile based on how a user behaves and interacts, from which risk based decisions can be taken.

"An appropriate amount of friction should always be applied and consistency is key in establishing consumer confidence."

Entersekt

"One Time Passwords delivered by a SMS text can no longer be relied upon thanks to criminals using SIM swaps and social engineering to conduct fraud."

Entersekt

Machine Learning and Artificial Intelligence

All organisations are developing strategies to make greater use of ML and AI. These technologies are needed in order to cope with the growth in transaction volumes, the need for faster decision-making and the increased sophistication of attacks. While the two terms are often used interchangeably, ML is only one of the many fields of AI. To maximise ML effectiveness we heard the importance of neural nets, deep learning, contextual data, expert workflows and black boxes for fraud modelling.

"Criminal are adopting new technologies faster than financial institutions as they don't have to submit business cases to an investment committee and worry about disrupting the UX or generating False Positives."

Risk management solution provider

ML platforms ingest tens of thousands of complex signals and analyse behavioural patterns to monitor activity and allow decisions to be made in fractions of a second. Critically, ML models enable a significant reduction in the number of false positives whilst increasing the detection of fraudulent or suspicious activity. This makes ML the most effective resolution to the issues presented by traditional platforms.

"Machine Learning models allow continuous learning from behaviour, but are only as good as the quality of the data they are learning from."

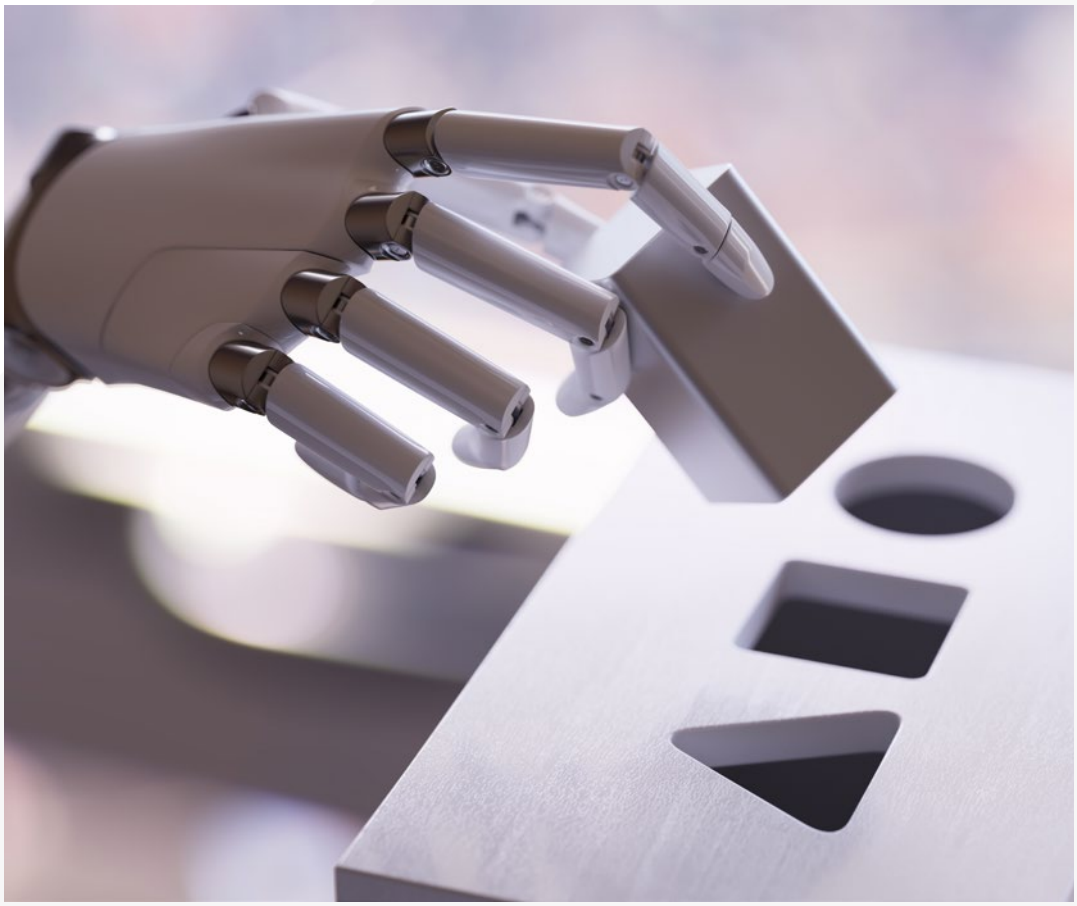
cybertonica

We heard from interviewees that AI and ML must be part of every AML strategy as these two technologies allow FS providers to move from reactive to proactive detection. However, FS firms will need to help up skill their staff in the best use of these technologies.

Collaborative transaction monitoring and analysis

We heard how the Pay. UK's Mule Insights Tactical Solution (MITS) , which utilises data from all banks, is making a real difference in tracking suspicious payments as well as in identifying money mules. This technological solution enables the tracking of suspicious payments between FS providers, even if the money is split between multiple accounts or travels between different institutions.

Similarly in the Netherlands the five largest banks have established Transaction Monitoring Netherlands (TMNL) in their collective fight against money laundering and the financing of terrorism by the identification of unusual patterns.



Both these examples show how consolidating transactions and using latest data analytics allow for more effective detection of criminal money flows and networks. They also highlight that combining transaction data will provide new inter-bank information that can be used in the fight against financial crime. We also heard of the differences between the rights of sharing data for AML and fraud purposes.

World Wide Web Consortium (W3C) initiatives

The W3C, the main international standards organisation for the worldwide web, are running a number of programmes to strengthen internet security usage and user authentication. Some of these have specific relevance to the payments industry. Key initiatives include a series of browser security enhancements and a slimmed down Payment Request API specification. This API allows users to register their payment credentials and select the right payment type through the browser.

Additionally the W3C have helpfully developed specifications for Secure Payments Confirmation (SPC). We learnt that the vision for SPC is to streamline strong customer authentication (SCA) during a Web payment and how this will enhance security and improve Web commerce experiences.

"Secure Payment Confirmation is a Web API to support streamlined authentication during a payment transaction. It is designed to scale authentication across merchants, to be used within a wide range of authentication protocols, and to produce cryptographic evidence that the user has confirmed transaction details."

World Wide Web Consortium (W3C)

Card payment security technologies

The implementation of Point-to-Point Encryption (P2PE) technology for face-to-face card payment transactions removes the risk from a data breach and protects the retail store environment. It also simplifies and reduces the cost of PCI DSS compliance. Another important card security technology is Tokenisation which replaces the sensitive card account number with a digital identifier that if stolen cannot be monetised. Network Tokens are the next incarnation of tokenisation with greater adoption anticipated soon. These will add new layers of security at the same time as delivering improved authorisation rates

CRYPTOGRAPHIC TRANSACTION MONITORING

HOMOMORPHIC ENCRYPTION

PRIVACY ENHANCING TECHNOLOGIES

NATURAL LANGUAGE PROCESSING

TOKENISATION

POINT-TO-POINT ENCRYPTION

ELLIPTIC ADDRESSES

Other interesting technologies

Our research identified many other technologies that can help prevent FinCrime and reduce payment fraud. These include natural language processing, cryptographic transaction monitoring using elliptic addresses, Privacy Enhancing Technologies that allow data sharing between parties, homomorphic encryption in order to perform data analytics without compromising privacy and, perhaps in a longer time horizon the use of ultra wideband technology which can deliver precise use location data within a building or shop.

No report would be complete without mentioning the potential for the use of blockchain technology. Interviewees agreed that this technology is attractive and could deliver benefits. In our research we heard how a large global bank is adopting blockchain for a corporate payment distributed ledger. ■

CURRENT LIMITATIONS

Too slow

Payments now move much faster than they used to and often in near realtime. But many organisations are yet to change their tools to reflect this reality and keep up with the fast pace of change. Retroactive controls, like post event transaction monitoring, are too late as the criminals are likely to have already moved the funds on to another institution. Traditional banks have generally been too slow to innovate and to strengthen their fraud prevention tools and controls.

Insufficient data

Legacy systems typically only have access to a limited dataset held by an organisation. Additionally, current systems often fail to capture all of the data elements that are available within an electronic payment transaction with device location being one example. These data restrictions are due to both technical and business decisions. We learnt of a lack of willingness to collaborate and share data between departments. Pattern analysis is a key component in preventing crime and fraud but to be effective this requires access to the maximum amount of data.

"A new holistic approach to fraud management is needed which utilises all of the data that is available within an organisation."

WesternUnion WU Business Solutions

Resource constraints

Data scientists and FinCrime/Fraud prevention specialists are in short supply and this is impacting both FS providers and vendors. These key individuals often prefer to work on next generation technologies and tools, rather than legacy systems, resulting in the current tools falling further behind market needs.

"New regulations should be framed around data rather than documents in order to encourage the greater use of technology and thereby strengthen protection levels."

Kompli-Global® SAFE IN THE KNOWLEDGE

Analogue thinking

Many organisations have failed to fully embrace the digitisation of banking and payments. Too often regulators still think in a legacy world of bank branches and paper-based KYC checking.

Lack of a FinCrime sandbox

We have seen the benefits of making digital sandboxes available to FinTechs. Our research highlighted how a FinCrime digital sandbox would allow new fraud models to be developed and optimised quicker.

Next generation solutions are needed

We heard a compelling case for FS providers to accelerate their investment in next generation RegTech, FinCrime and Fraud Prevention systems. These are needed in order to strengthen controls, reduce losses and deliver full compliance. We learnt that it has been hard to get business cases approved due to conflicting business priorities but encouragingly this situation seems to be improving. These platforms will utilise new technologies, operate in realtime and be accessible via a single API. A standardised implementation of fraud solutions will also eliminate any weak points in the chain. ■

"A new approach is needed if you want to get on the front foot and make life harder for the criminals. Departmental silos must be eliminated and single API access to technology platforms is required. Greater collaboration and data sharing will also allow improved decision making."

REFINITIV

THE ROLE OF DIGITAL IDENTITY

Foundation layer

Digital Identity (DI) services can solve several of today's problems, if implemented well, but it is recognised that they are not the complete answer. The FCA lists DI as one its key pillars for user protection. DI provides provable and sharable identity, which is particularly important when onboarding customers but also has a key protection role to play when users are transacting. Many payment professionals we spoke to felt that the lack of a national DI service is a key obstacle in fighting crime and fraud.

We heard in our research that countries who have implemented national identity services have seen fraud levels driven down as the genuine status of a user is known both at time of account opening and when subsequently transacting. DI services should not be confused with national ID cards and need not, if implemented well, be tainted by the same privacy concerns. Interviewees highlighted how DI services can provide greater accuracy on verifying an identity than an ID card as they have access to far more data points.

There are three popular DI service approaches:

- State run federated models which are designed and run by national Governments
- Government and private sector partnership, with Government setting the regulatory framework and then the private sector developing and operating services
- Private sector initiatives without Governmental involvement, but competitive pressures often restrict participation

Assurance and trust

DI can provide assurance and trust between unknown parties, helping prevent impersonation scams. Key benefits of DI tokens include the elimination of doubt and providing certainty. We heard of the importance of having strong public and private sector partnerships and for a very broad range of stakeholders to be involved. Governments have a key role to play particularly in establishing the framework on how all parties should work together and addressing concerns relating to privacy and data sharing.

"The accuracy of customer identification and authentication checks will be improved by the introduction of digital identity services as well as delivering enhanced authorisation capabilities."

consult hyperion
securing tomorrow's transactions

"Digital identity is a key tool in preventing FinCrime as it makes life tougher for the fraudster. It will be a crucial method for customers to use to prove who they are."

GBG

DI addresses several security weaknesses and enables access control to be introduced for the sale of age restricted products and services. It also reduces reliance on Knowledge factors, which are known to be inherently weak. We heard how "Having a digital identity that can be used easily and universally will become a cornerstone of future economies".

"Digital identity solves many of today's challenges including improved KYC checking at time of customer enrolment, controlling access to restricted products, and allowing the introduction of improved monitoring."

REFINITIV

UK initiatives

The UK is actively making plans to introduce a digital identity and attributes trust framework. The Department for Digital Culture Media and Sport (DCMS) is leading the programme. This framework will help establish a clear understanding between people using identity products, organisations relying on the service and the service providers, letting each party know that the data is being used appropriately and kept safe. The expectation is that users will maintain a secure wallet on their devices in which will be stored a range of trusted pieces of information, often referred to as attributes. The UK trusted framework is attracting interest around the world and is expected to influence international best practices.

European initiatives

As part of our research we spoke with Bank ID from Sweden who are one of the most respected digital identity scheme providers in the world. They have been operating for 18 years and have achieved an impressive 8 million users of the national population of 10 million, with an incredible 98% penetration between the 18-67 years age group. They explained how banks, insurance companies, private companies, local and central authorities collectively utilise digital identity in over 5000 services accounting for more than 6 billion transactions annually, with each user's digital identities being checked around 65 times monthly.

"Digital identity needs to offer a great user experience, be highly secure, available everywhere and used on a regular basis, if it is to be successful."

BankID

Once again, it has been the strong partnerships that exist between stakeholders that have been one of the reasons for its success.

"A digital identifier allows confirmation of the real user. It is the equivalent of moving from a Customer Not Present to a Face to Face transaction."

BankID

We heard how the Baltic States are another European success story for the introduction of digital identity authentication services. They are some of the most digitally advanced countries in the world. Their Smart ID app is heavily used in Estonia across the finance, education, healthcare, domestic and commercial sectors and also in Latvia and Lithuania. Additionally we received positive feedback about the Danish NEMID and Belgium ITSME programmes.

eIDAS

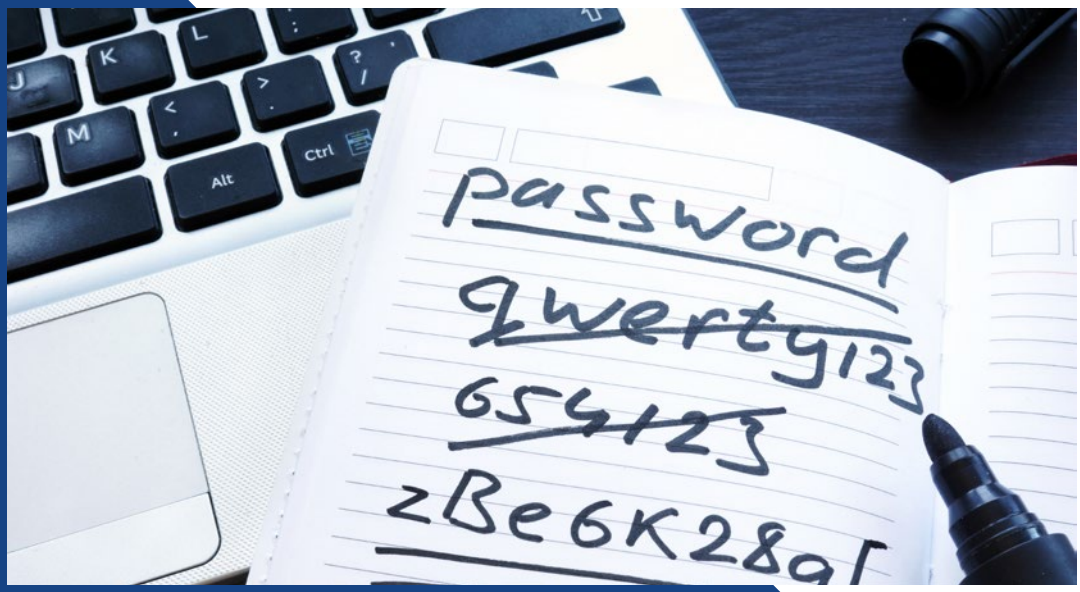
The EU established the Electronic Identification Authentication and trust Services (eIDAS) regulation in 2014 as part of its digital agenda. This was seen as an important element in driving digital growth and an enabler for cross border electronic transactions. It laid down a clear foundation and legal framework that required incorporation into national legislation by all member countries.

However, adoption levels have not been as high as the EU had hoped for. Many countries were slow to implement and some only transposed part of the regulation. The major usage has come from public services with private sector involvement (including banks) much lower than anticipated. We also learnt how inconsistencies between national implementations created issues and delays. It was also highlighted to us that eIDAS was not originally designed for AML purposes.

However in 2020, the national COVID lockdowns and switch to working from home acted as a stimulus for greater adoption of electronic ID services. Therefore the EU conducted an open market consultation in August and September 2020 to collect feedback on the drivers and barriers to the development and uptake of trust and eID services in Europe. This has led to plans now being developed to deliver a new pan-European digital wallet, that can be accessed by fingerprint or retina scan, that can store official documents such as a driver's licence and other attributes in a secure vault. The intention is for this digital wallet to be used for a variety of services offered by both the private and public sector.

"Usage of the wallet will not be compulsory, but citizens who choose to sign up will benefit from an extra-secure digital ecosystem and greater flexibility, ideal for post-pandemic life."

European Commission



Australian initiatives

Australia is another country progressing digital identity services at pace. Similar to the UK, the Australian Federal Government has established a Trusted Digital Identity Framework (TDIF). Recently this has been supplemented by the launch of ConnectID a government-accredited operator of a digital exchange, which makes it easier for users to share, store and receive personal identity information online.

W3C

Our research suggests that potentially one of the most significant global initiatives is the W3C Digital Identifiers (DIDs) programme, which will offer a new type of identifier that enables verifiable, decentralised digital identity standard. DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities so that they can deliver proof of control without requiring permission from another party. ■

GREATER COLLABORATION AND DATA SHARING

Regulatory clarity

Regulators have a critical role to play in encouraging stakeholders to share more data and collaborate to a greater extend. Currently, concerns exist that privacy and competition regulations prevent the sharing of data. This ought not to be the case. Money Laundering Regulatory Officers (MLROs) should have the ability to share fears of fraud and criminal activity with their peers. GDPR does not necessarily trump other regulations but we heard the request for regulators to offer clear advice on how and when data can be shared and how to resolve conflicts between regulations.

Data Sharing

Collaborative networks and forums are considered a helpful way to share data in a controlled manner and provide a platform for learning. In our research we heard how "data needs to be shared more effectively if we are to stop the criminals". The FS industry should not be competing with each other on fraud prevention. We heard suggestions that data from all channels, departments and organisations should be depersonalised and then fed into a massive data lake, to allow sophisticated data analysis to be conducted. Data is seen to be a critical asset in the fight against crime.

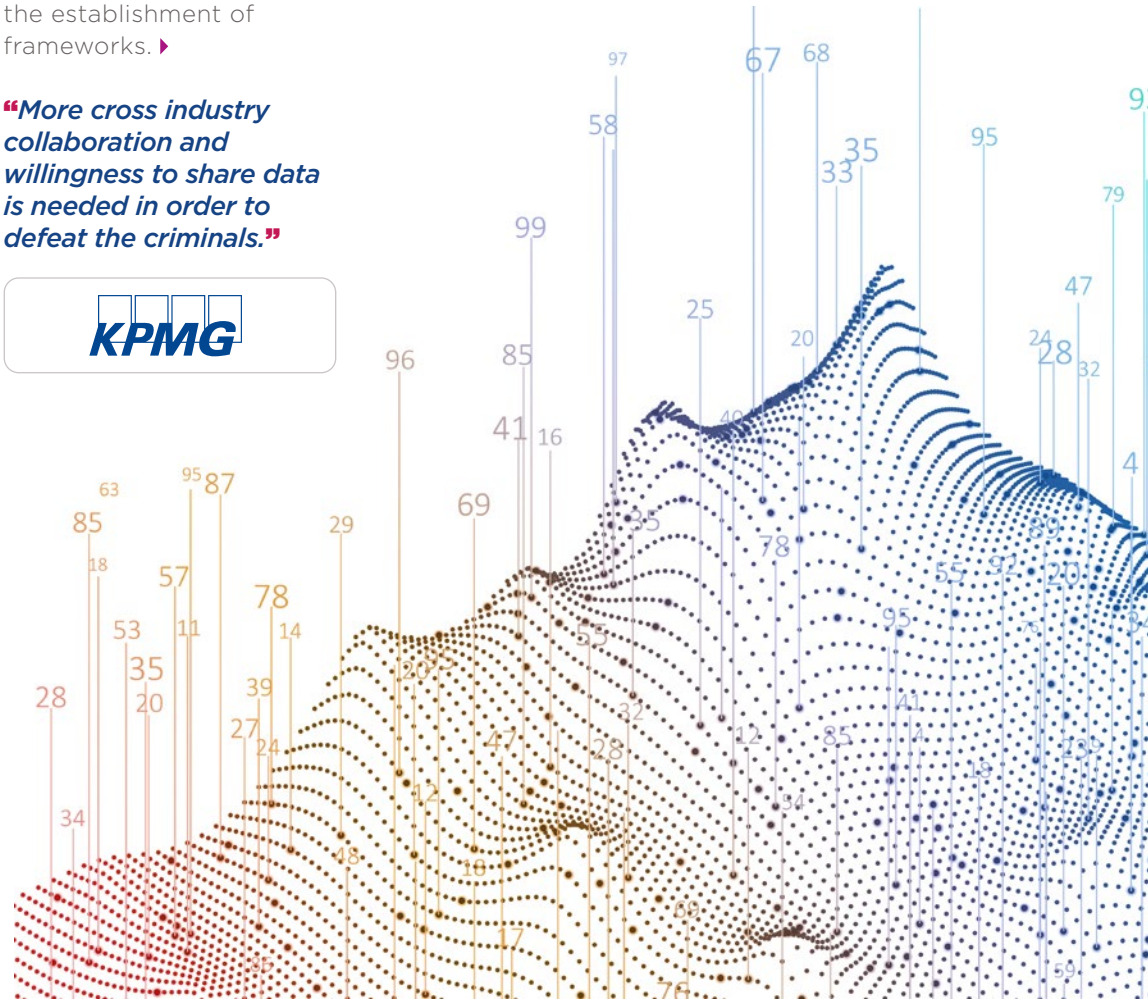
Some attitudes to data sharing do need to change, as we heard examples of FS providers wanting the outputs from data sharing despite being reluctant to input their own data into the pool. Perhaps more education is needed to persuade stakeholders of the benefits of sharing data. It is felt that clearer signalling from regulators would be helpful. The use of Privacy Enhancing Technologies (PET) will address some concerns, but we also need additional help from the regulators. Greater engagement across industries and sectors has been identified as being helpful alongside the establishment of frameworks.

"More cross industry collaboration and willingness to share data is needed in order to defeat the criminals."

KPMG

"The Global Coalition to Fight Financial Crime promotes: more effective sharing of data between public and private entities; proposes mechanisms to identify emerging threats and best practices; and identifies pressure points in the current AML framework and proposes solutions to these, that is why we are a member."

REFINITIV



Global Initiatives

FATF

The Financial Action Task Force (FATF) is a global money laundering and terrorist financing watchdog. This inter-governmental body, with members from more than 200 countries, sets international standards that aim to prevent these illegal activities and the harm they cause to society. FATF Recommendations ensure a coordinated global response to prevent organised crime, corruption and terrorism. They help authorities pursue the money of criminals dealing in illegal drugs, human trafficking and other crimes.

FATF reviews money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. The FATF monitors countries to ensure they fully implement recommendations and hold non-compliant countries to account. In July FATF announced that Malta is to be added to the Grey list, making it the first European country to be so classified.

MONEYVAL

Europe's equivalent to FATF is MONEYVAL.

This has been operating since 1997 with the aim of ensuring that European member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in this matter.

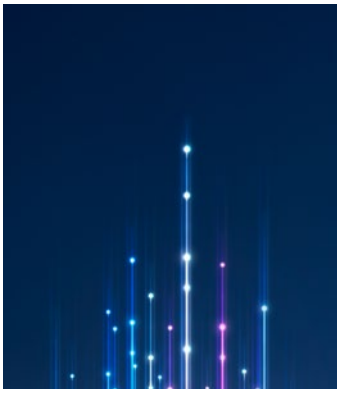
Individual countries have developed national groups to co-ordinate their fight against money laundering. Here are a few examples from the UK, Sweden and the Netherlands.

JMLIT

The Joint Money Laundering Intelligence Taskforce (JMLIT) has been established by the UK National Economic Crime Centre (NECC) as a partnership between law enforcement and FS providers to exchange and analyse data relating to money laundering and wider FinCrime threats. Its purpose is to tackle high-end money laundering schemes, which are complex, multi-institutional, and multi-jurisdictional, by providing a forum to share information on new typologies, existing vulnerabilities, and to share intelligence. This collaboration has led to thousands of suspicious accounts being closed, numerous arrests being made and the prevention of transfers valued at many millions of pounds. This is a positive example of the results from collaboration and data sharing.

SAMLIT

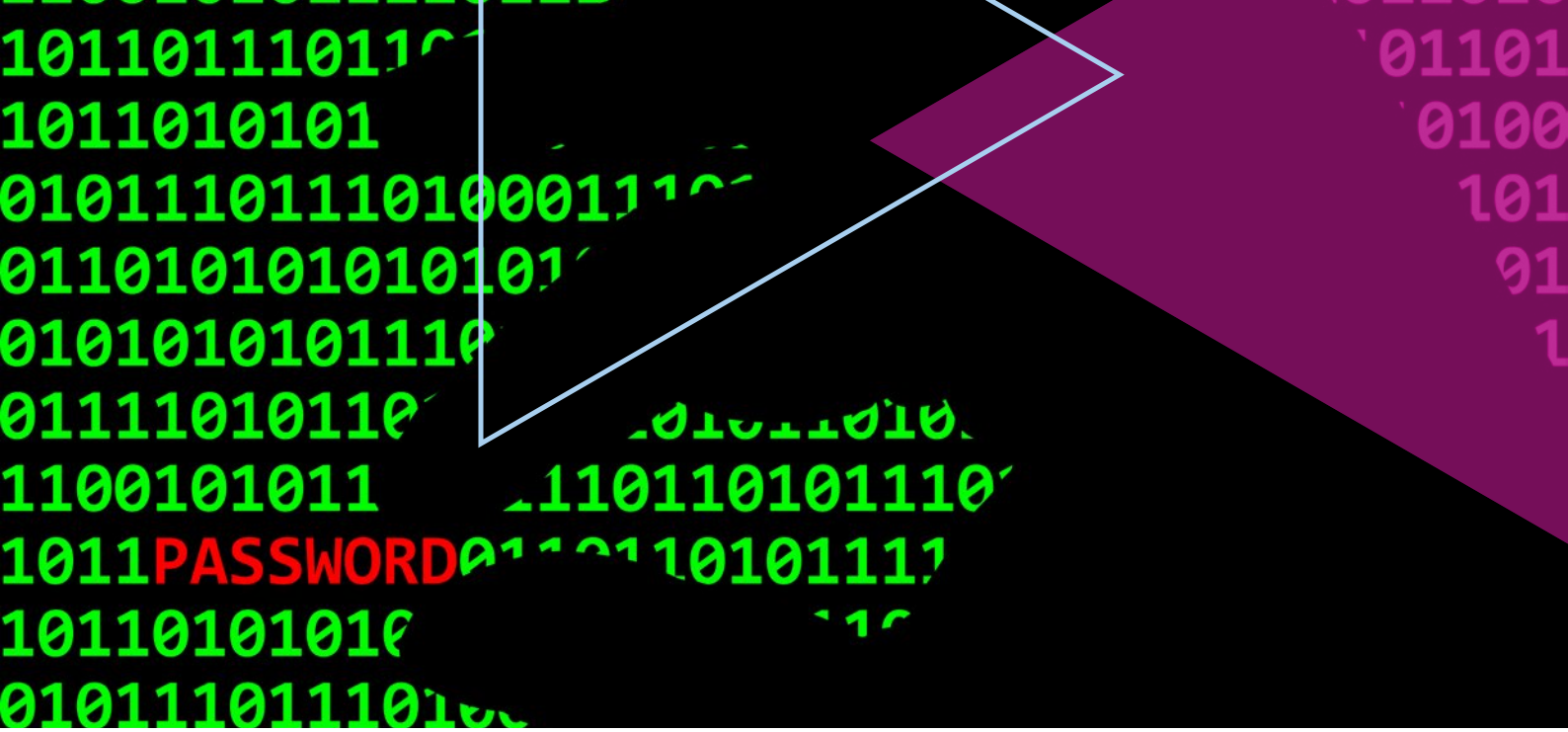
In Sweden, following a successful trial of SAMLIT, the Swedish banks, banking association and the intelligence unit



of the Police National Operations Department have decided to increase their cooperation to take their fight against money laundering to the next level by expanding their investment in SAMLIT.

AMLC

In the Netherlands, AMLC was formed with the intention of developing into a platform where the parties involved in combating money laundering could share their knowledge and experience and work together operationally. The basic principle is that all the public and private parties who play a part in combating money laundering should work in the centre together and be supported from that centre. ■



CHALLENGES AND BARRIERS

Organisational

There are many organisational challenges that need to be addressed in order to make a significant difference to the fight against crime. These start with the board of directors who need to set the right tone for an organisation and make it clear that fraud needs to be taken more seriously and that departments must work closer together. Employees should understand that prevention is as important as compliance and fraud ought not to be treated as an acceptable operational cost. Additionally, it must not be seen as a competitive issue and it is wrong to fear talking about fraud. This may require a shift in cultural attitudes and new incentives. Our research highlighted the clear differences that exist between new FinTech providers and legacy banks.

"Many compliance teams have become stuck in their ways and continue to rely on outdated processes that came from a branch-based environment. An upskilling of employees and a new mindset is needed."

Independent AML Subject Matter Expert

Regulatory

We heard the call for improved regulatory understanding and less scepticism of Neobanks and FinTechs. It was highlighted that the amount of regulation has increased considerably in recent years, but much of this is felt to be too broad brush in nature and the inconsistencies internationally cause unwelcomed complications.

It is acknowledged that the regulators face many challenges in managing the rapidly changing payments landscape and may need additional resources, new skillsets and improved understanding of the latest technologies. As an example there is wide variation in approach globally to regulating cryptocurrencies. Interviewees called for greater engagement by the regulators with tech providers but equally FinTechs must respect the concerns of regulators and find ways to work with them better. Interviewees raised the need for more international standards and greater alignment between those that exist.

Law Enforcement

Interviewees highlighted the need for greater cooperation between law enforcement and FS providers and how this needed to be at an international level due to the global nature of money laundering, the ease of sending money across the world and because criminals aren't constrained by national borders.

"The police need more powers, greater assistance from tech and FS companies and an easing of GDPR restrictions, if they are to increase conviction rates."

Former senior law enforcement officer

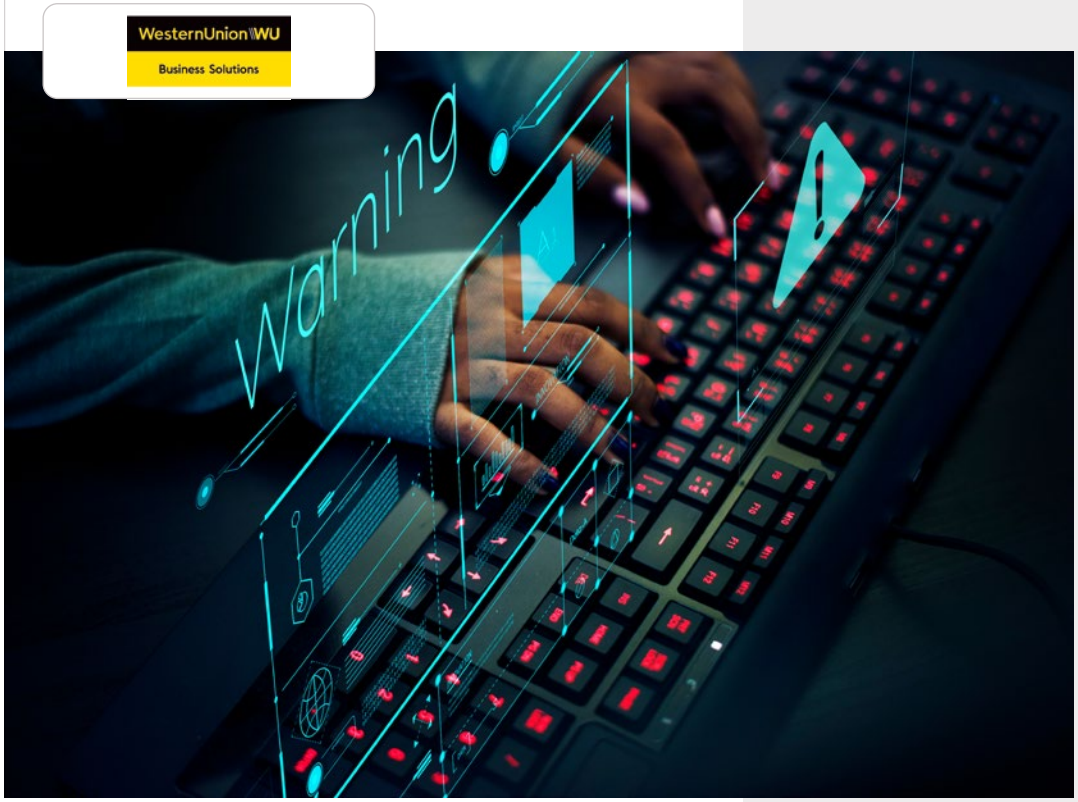
A key challenge identified is the low priority assigned by law enforcement to FinCrime and reluctance to take these through the full legal process. This may partly be due to the responsibilities placed on FIs by regulators to pick up the cost of fraud and to compensate customers. We did hear how Interpol and national organisations like the DCPCU can make a real difference but these organisations could only take on a very limited number of cases each year due to resource constraints.

Latest technologies

We learnt that many organisations are comfortable with their status quo and have resistance to the use of newer technologies as well as to blending new with old tech. This may be as a result of familiarity with existing systems and current technology skillsets but could equally be due to a desire to protect department structures and responsibilities. Compliance, fraud and cyber security teams are often reluctant to change their behaviours and fear having shared technology platforms or becoming part of a centralised shared services function. Incompatibility between systems is frequently a barrier to greater data sharing and mindset shifts may well be needed if we are to see new technologies and solutions introduced.

Our research also highlighted that procurement policies in place at some banks make it difficult to procure new systems from smaller sized vendors. This may delay the introduction of next generation systems, allowing criminals to exploit vulnerabilities for longer.

"Everyone has a key role to play in preventing fraud. That is why it is so important to be educating customers and employees on the latest attack profiles and scams."



Awareness and Education

Low levels of customer awareness and education are further challenges that must be overcome. This highlights that education is needed but poses the challenge on who should be providing this. Big banks often recognise the case for providing resources to improve a customer's knowledge and awareness, in order to protect their own businesses from poor customer behaviour, although some FIs feel that the Government has a big role to play as issues are greater than economic.

FS providers do educate their employees on a wide range of FinCrime topics including AML, bribery, terrorist financing and sanctions checking as part of regulatory compliance. But this becomes a bigger challenge each year as the criminals get more sophisticated and therefore the scope of training needs to increase. ■

CONCLUSIONS

Financial crime and payments fraud are escalating problems and ones that need to be taken more seriously by all stakeholders...

...They result in negative impacts for society, organisations and individuals. Strong defence is not an easy task as the criminals are continually getting more sophisticated and as soon as defences are tightened in one area the attacks shift to a weaker point. Encouragingly new technologies and strategies are starting to make a real difference. It is unrealistic however to expect to stop all types of fraud and crime, but the aim should be to make life harder and uneconomic for criminals.

Manual and static prevention approaches are ineffective, automation is needed and technology offers the greatest chance of success. No silver bullet exists and so a multi-layered strategic approach is recommended. There are many key technologies that justify investment including ML, AI, Biometrics, 3DS, COP, Tokenisation and P2PE. Current systems are not performing optimally through age, design and functionality. System duplication and departmental silos should be eliminated with investment in next generation platforms required.

Risk decision-making can be improved through access to larger data sets. This includes the consolidation of all data available within an organisation and supplementing this with external data sources. Greater collaboration with external stakeholders should also be encouraged.

Crime and fraud prevention will benefit from having a digital identity foundation layer. This will deliver assurance when a new customer account is set up and then when the account is being used. The introduction of identity and trust frameworks will allow thousands of private and public sector services to benefit from certainty of customer identity.

Many challenges need to be overcome and this will require the active support of FS board of directors, regulators, law enforcement agencies and payment providers. Customers also need to play a greater role to protecting themselves but to do so more awareness campaigns and education need to be supplied.

Hopefully, this white paper will help inform stakeholders of the issues and highlight areas that require attention and investment. The EPA and its members look forward to assisting the industry make the changes needed in order to make life harder for criminals and strengthen protections for organisations and individuals. We look forward to discussing the findings with you

About Refinitiv

Refinitiv, an LSEG (London Stock Exchange Group) business, is one of the world's largest providers of financial markets data and infrastructure. With over 40,000 customers and 400,000 end users across 190 countries, Refinitiv is powering participants across the global financial marketplace. We provide information, insights, and technology that enable customers to execute critical investing, trading and risk decisions with confidence. By combining a unique open platform with best-in-class data and expertise, we connect people to choice and opportunity – driving performance, innovation and growth for our customers and partners.

Research Participants

Between April and June 2021, the EPA conducted extensive primary research through a series of detailed stakeholder interviews. We assessed the FinCrime and Payment Fraud market landscape, identified current gaps, looked at which technologies offered the greatest potential, where investment should be made and the key barriers that must be overcome. A key area of focus was investigating the potential for digital identity as a secure foundation layer in order to reduce financial crime and payment fraud.

Interviewees included subject matter experts from financial services providers, card issuers, payment processors, digital identity specialists, consultancies and solution providers. This white paper has been structured according to the questions asked in our research interviews.

We heard from over 25 organisations as part of our research including those listed below. These organisations operate in multiple countries and are representative of the entire payments industry. We would like to express our thanks for the support we received.

About Payments Consultancy Ltd

Payments Consultancy Ltd, the commissioned researcher and author of this white paper, is an award-winning payments consultancy that advises banks, card issuers, acquirers, merchants, payment providers and investors. The company provides specialist advisory services related to:

- Strategy development
- Market assessments
- Competitive analysis
- Supplier selection
- Commercial due diligence

Payments Consultancy's primary consultant is Mark McMurtrie who has over 25 years payments experience. Mark is an ambassador for the EPA, industry commentator, conference chairman, popular speaker and awards judge.

Emerging Payments Association

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

Tel: +44 (0) 20 7378 9890

Web: emergingpayments.org

Email: info@emergingpayments.org

@EPAssoc

Emerging Payments Association

About the EPA

The Emerging Payments Association (EPA), established in 2008, sets out to make payments work for everyone. To achieve this, it runs a comprehensive programme of activities for members with guidance from an independent Advisory Board of 15 payments CEOs.

These activities include a programme of digital and (when possible) face-to-face events including an online annual conference and broadcast awards dinner, numerous briefings and webinars, CEO Round Tables, and networking and training activities. The EPA also runs six stakeholder working groups. More than 100 volunteers collaborate on the important challenges facing our industry today, such as financial inclusion, recovering from COVID-19, financial crime, regulation, access to banking and promoting the UK globally. The EPA also produces research papers and reports to shed light on the big issues of the day and works closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, UK Finance and Innovate Finance.

The EPA has over 130 members that employ over 300,000 staff and process more than £7tn annually. Its members come from across the payments value chain including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, TPPs and more. These companies have come together to join our community, collaborate, and speak with a unified voice.

The EPA collaborates with its licensees at EPA EU and EPA Asia to create an interconnected global network of people passionate about making payments work for all.

EPA's Project Financial Crime

Mission Statement: To deliver community-driven solutions that address the problems posed by digital and financial criminal activity and position the EPA and its members as leaders in tackling financial crime.

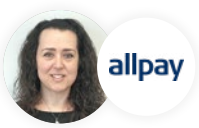
Jane Jee
CEO
Kompli-Global

Philp Creed
Co-Founder and Director
fscom

Jonathan Jensen
Regulatory Policy Advisor
GB Group plc

Steve Pannifer
COO
Consult Hyperion

Fabien Ignaccolo
CEO
Okay



Victoria Preece
Compliance Manager
allpay

Anthony Gudgeon
Fraud Manager
Contis

Jonny Bell
Director – Customer & Third Party Risk Solutions, Data & Analytics
Refinitiv

Neil Turner
Manager, Compliance and Regulations
Mastercard

Simon Booth
Marketing Manager
Lexis Nexis Risk Solutions