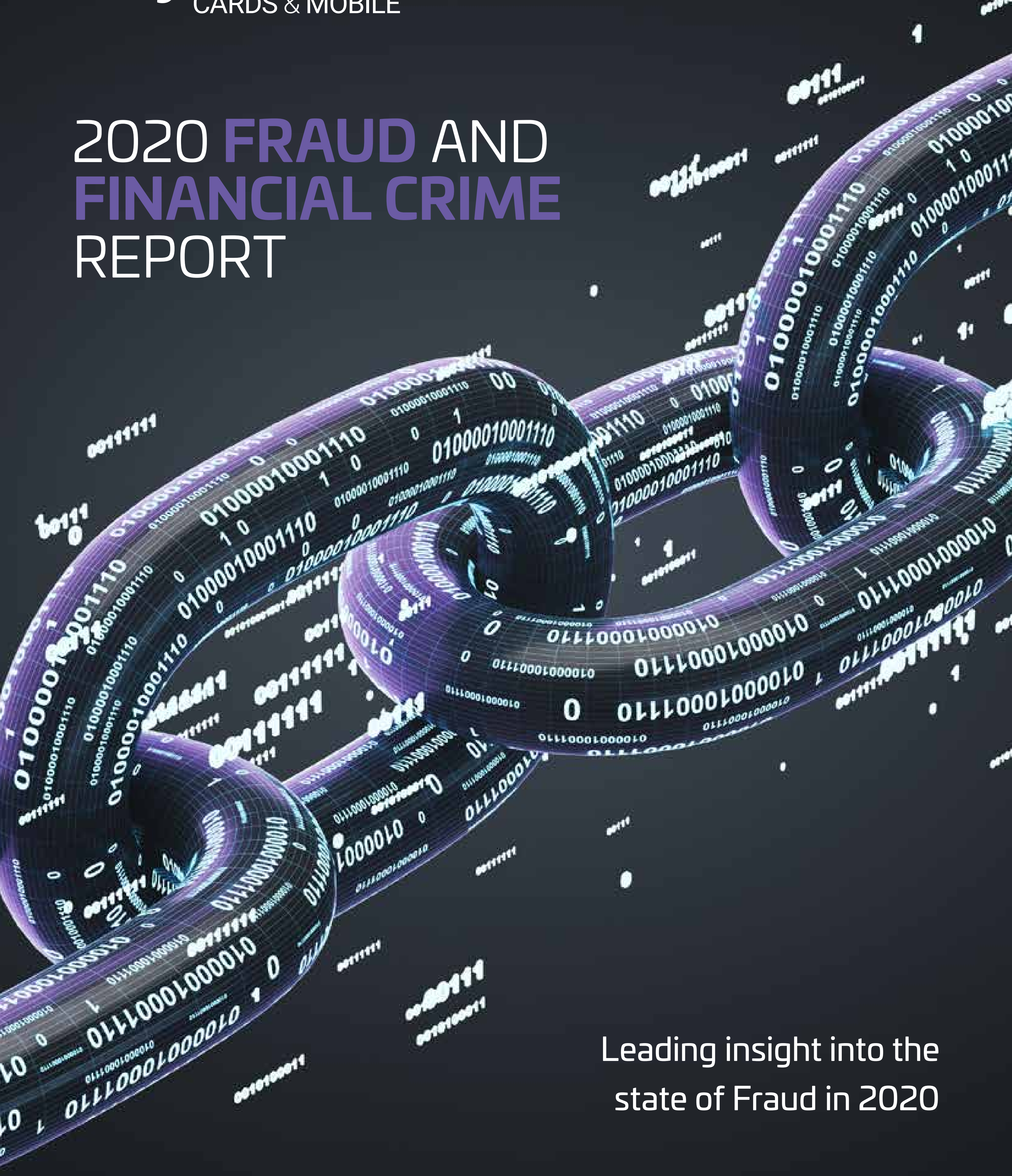
PAYMENTS INDUSTRY INTELLIGENCE
Payments
CARDS & MOBILE

Sponsored by

INFORM

2020 FRAUD AND FINANCIAL CRIME REPORT



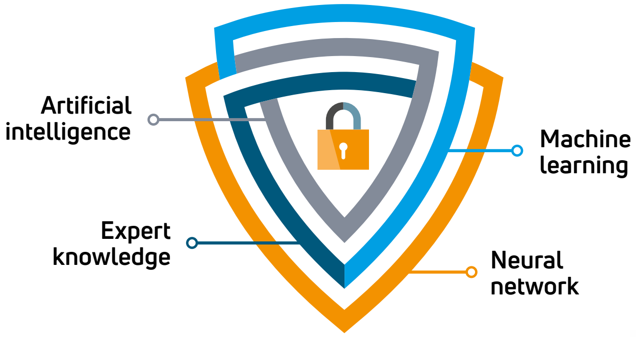
Leading insight into the state of Fraud in 2020

Fighting Fraud with Intelligence

Transform your customers from fraud victims to brand ambassadors

As the preferred provider of card fraud prevention solutions in one of the fastest industries, Nets delivers a focus on the customers' needs for feeling safe and secure. We do that by delivering easily adaptable counter fraud solutions using next generation technologies to create seamless customer experiences.

3D Secure
Risk-based authentication
Smart Block
24/7 cardholder call centre
Token Service for HCE, QR and BLE

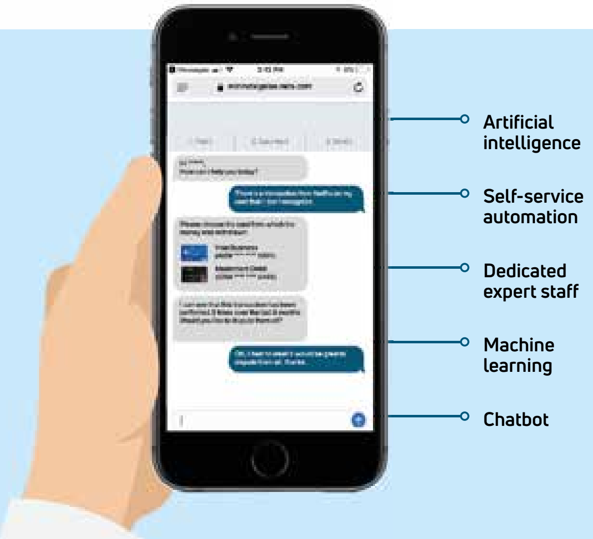


Automated & Digitalised Fraud Management Solution

- Reduce fraud losses by up to 40%
- Automated customer communication to reduce friction and improve experience
- Risk and reward based pricing structure
- Dedicated onshore team

Next Generation Disputes Management

- Market-leading resolution rates
- Up to 50% reduction in the cost of managing disputes
- Significantly improved customer experience
- Plug and Play – rapid – no set up cost



For more information visit: ***www.nets.eu/fraud***

Contact: Michalis Michaelides, VP Business Development: mmich@nets.eu

nets

iovation research finds rise in gaming industry bonus abuse and credit card fraud

iovation, a TransUnion company, has released its 2020 iGaming Report which analyzes more than four billion global online gambling transactions screened for fraud indicators.

Bonus abuse was the number one reported fraud by iovation's iGaming customers for the third year in a row, rising 72 percent from 2018 to 2019. Gambling bonuses often include giving a new player house money to gamble or existing customers incentives to play more. Bonus abusers then use multiple accounts with different email addresses in order to claim the same bonus sometimes hundreds of times, which is often against gambling operators' terms.

The report also highlighted a 37 percent growth in credit card fraud from 2018 to 2019, as well as a significant shift towards mobile transactions. In 2019, 79 percent of all iGaming transactions came from mobile phones and tablets, an increase of 13 percent over 2018.

Tokenisation to generate over $40bn in global revenues by 2024

A new report from Juniper Research has found that annual revenues from tokenised mobile payments, (where account details are replaced with data useless to fraudsters) will exceed $40 billion by 2024, growing from an estimated $17 billion in 2019. Of this, over $30 billion will be through remote eCommerce, rather than contactless payments at the point of sale.

The new research, Mobile Payment Data Security: Tokenisation, Encryption & Regulation 2020-2024, found that the ability to use standard tokens and multifactor authentication protocols through Secure Remote Commerce will increase the use of such security measures in browser-based commerce, where previously it was mostly limited to native apps. The report notes that this will be aided by 3D Secure 2.0 standards. As a result Juniper Research believes virtually all remote payments will be tokenised by 2024, along with all Near Field Communication-based payments.

FICO release latest fraud statistics from FICO Asia Pacific Fraud Forum

The proliferation of real-time payments platforms, including person-to-person (P2P) transfers and mobile payment platforms across Asia Pacific, has increased fraud losses for the majority of banks according to research from Silicon Valley analytics firm FICO. Their survey with banks in the region, conducted at their APAC Fraud Forum, found that 78 percent have seen their fraud losses increase in the last year.

The results showed that social engineering was named as the number one fraud concern for 40 percent of banks when it comes to real-time payments. Account takeovers were ranked second, with false accounts and money mules also rated as problems.

More than 90 percent of APAC banks surveyed thought that convergence between their fraud and compliance functions would be helpful in defending transactions on real-time payments platforms.

FICO European Fraud Map Shows UK Card Fraud Losses Hit Record £671 Million

FICO has also released its annual interactive European Fraud Map, which shows that the UK's card fraud losses hit a record £671 million in 2018, up 19 percent on the previous year.

The UK's card fraud losses were the biggest in Europe, and account for nearly half of the €1,616 million (approximately £1,400 million) lost to fraud across the 19 countries in the map. This development comes just a year after the UK managed to cut fraud losses by 8 percent.

The report states that primary cause of these record-breaking losses is an epidemic of high-profile data breaches.

PayPal and Polaris Join Forces to Fight Human Trafficking

Polaris, a leader in combating human trafficking, has announced the creation of a newly formed Financial Intelligence Unit. The Financial Intelligence Unit, which is made possible by financial and subject matter support from PayPal, is designed to leverage intelligence from the U.S. National Human Trafficking Hotline and other sources to interrupt trafficker cash flows and enable prosecutions for financial crimes including money laundering.

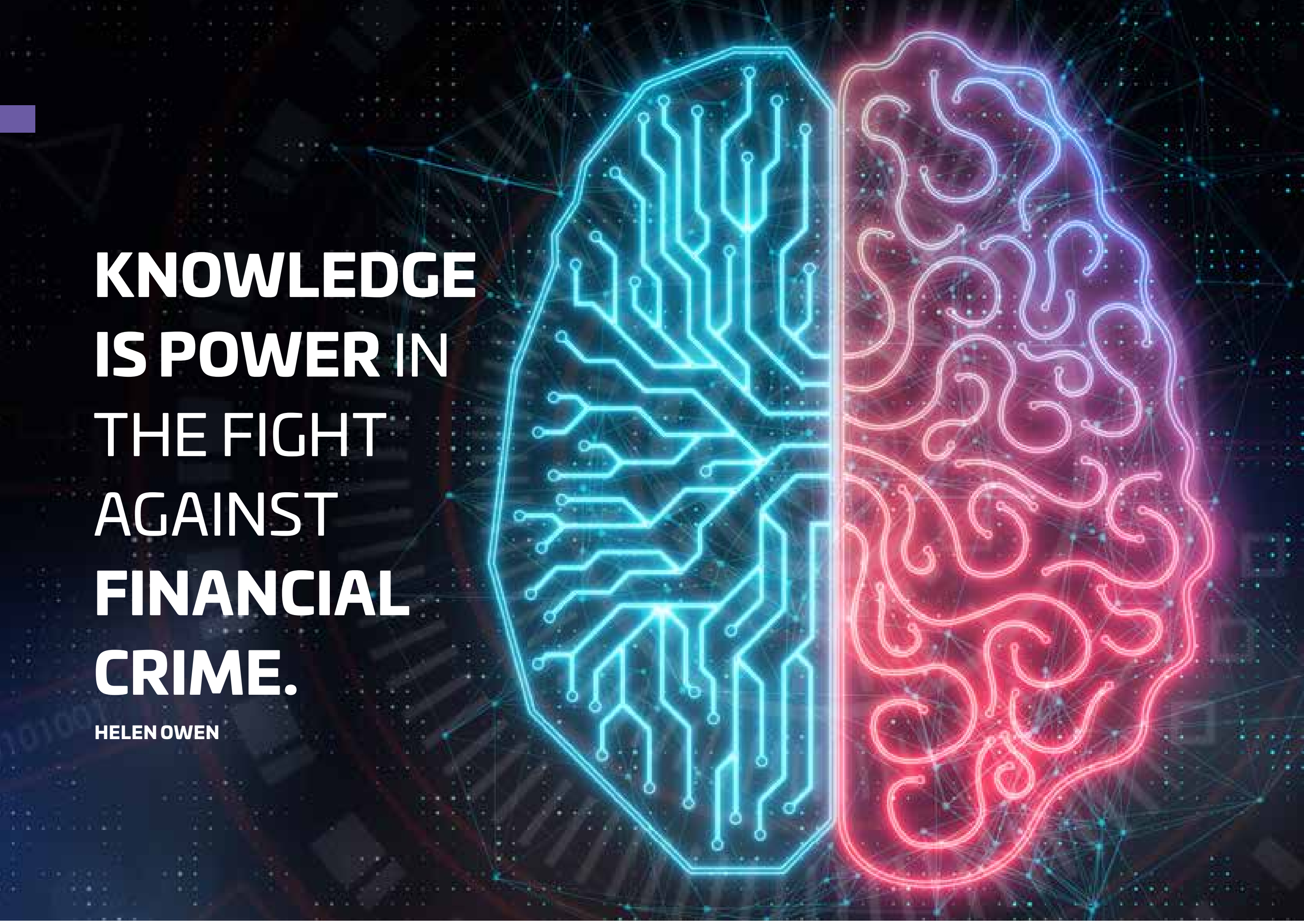
"Financial institutions have long been powerful partners in the fight against human trafficking," said Sara Crowe, director of Polaris's Strategic Initiative on Financial Systems. "Thanks to our partnership with PayPal, anti-money laundering professionals will have more opportunity than ever to share information, identify new techniques to effectively zero-in on those who profit off of the exploitation of others, and provide actionable information to law enforcement. In doing so, we help bring accountability to those who financially benefit from trafficking and restore freedom to countless thousands of people around the world."

RedCompass joins the Traffik Analysis Hub and announces launch of RedFlag Accelerator

Leveraging their expertise in payments, financial crime and data analytics, specialist consultancy RedCompass has developed 'RedCompass RedFlag Accelerator'; a standardised toolkit of human trafficking and modern slavery indicators and alert scenarios.

RedCompass RedFlag Accelerator draws on the work done by the UN, Banks Alliance, governmental agencies and the police, to enable banks to isolate key flags and patterns. By enriching the data collected by these agencies and institutions, the toolkit will allow compliance, financial crime and data teams to accelerate their search for human trafficking traces in their organisations.

The RedFlag Accelerator, will be a living tool, made available via the TA Hub - a platform developed by STOP THE TRAFFIK and IBM which uses cognitive technologies to allow cross-sector partners to gather and share human trafficking information easily and quickly, as part of their day-to-day business.



KNOWLEDGE IS POWER IN THE FIGHT AGAINST **FINANCIAL CRIME.**

HELEN OWEN

Financial crime comes in many guises and it proliferates across segments, sectors and geographies. Theft, fraud, deception, corruption, money-laundering… the possibilities for making and moving money illicitly are seemingly vast, often with low risk and high returns for the perpetrators.

While financial crime can be committed on a small scale purely by ill-intentioned individuals, it more often extends to large-scale, highly organised operations. These larger networks can span international borders, often with close connections to violent crime and even terrorism.

Financial crime is everyone's problem

A recent survey by Refinitiv revealed that 47 percent of organisations across a variety of sectors had pinpointed financial crime in their global operations over the last 12 months. The most worrying thing about this statistic - this already high percentage are just the companies who did actually spot illegal activities - undoubtedly there are far more criminals who succeed in staying under the radar.

Last year, the Financial Action Task Force (FATF) found that the UK had one of the toughest systems for combatting money laundering and terrorist financing of over 60 countries it has assessed to date. Despite this, serious and organised crime is estimated to cost the UK at least £37 billion each year, with the proceeds from large scale drug dealing, human trafficking and other serious crimes being laundered through the country's financial systems. Fraud is a particularly big problem, with The Home Office estimating the social and economic cost of fraud to individuals in England and Wales to reach £4.7 billion per year, in addition to the £5.9 billion of costs hitting businesses and the public sector. And all this is just in the UK, where supposedly the financial crime-fighting systems are among the most effective in the world…

Across the continent, things are certainly no better. Research by Europol reveals that, despite increased regulation and compliance efforts, on average only 1 percent of criminal proceeds flowing through the international financial system every year are detected and dealt with by the appropriate law enforcement agencies. Globally, 2–5 percent of the world's GDP ($800 Billion–$2 Trillion) is laundered each year according to figures from the UN.

Whether it's theft, fraud, money-laundering, terrorist financing or other forms of corruption, there are three key things that all these forms of financial crime have in common:

1. The plethora of regulation attempting to address the issue
2. The bottom-line cost to impacted businesses
3. The devastating societal and economic impact

These factors are driving the need for innovative, effective ways for financial institutions, acquirers, PSPs, merchants and solution providers to reduce the volume and impact of financial crime, as well as meet their compliance obligations.

Scaling the data challenge

Undoubtedly, the single most effective asset for fighting financial crime is knowledge – including customer profiles, information on changing trends and insight on financial crime warning signs. Building this knowledge needs to start with data – trusted, accurate, current, comprehensive data from as many internal and external sources as possible. Organisations also need the ability to combine all of this data from across channels and sources in order to build a clear picture of financial crime and power more effective detection and prevention measures. Even these first two requirements present several problems for a variety of organisations.

Speaking from a financial services perspective Tom Hewson, Senior Partner at specialist consultancy RedCompass cautions: "Most banks suffer from data quality problems to some extent. Achieving consistent, complete and correct data across a large organisation is tough. Different parts of the organisation may use different systems to store the same types of data and these may have different standards for data entry. Fragmented systems are a fact of life".

The same is true of many other businesses, including larger merchant organisations, who often have to contend the challenges of multiple operational divisions, siloed teams and legacy technology – making it difficult to standardise and pool data in a meaningful way. The need to remove silos is an extremely difficult challenge for many organisations to overcome. Digital transformation is a long road and not all organisations can afford the effort, complexity, time and costs of replacing legacy systems. Where this is the case, specialist technology layers that help bring data together from across silos can help.

Those organisations who are further along their digital transformation journey, (as well as those newer, digital-first businesses) have begun efforts to create central data-as-a-service platforms, using a data lake approach to combat this issue and build a stronger, data-powered foundation from which to combat financial crime.

Turning information into intelligence

While data is certainly the start-point for knowledge, it is, of course, not knowledge in itself – this base information needs to be analysed and interpreted to create real, actionable intelligence.

As we explored in *Payments Cards & Mobile's* first magazine edition of 2020, (pg. 18) Artificial Intelligence and machine learning are two of the key technologies which are beginning to have a real impact in the fight against payments fraud. However, their applications are much further-reaching, with the potential to produce real results in detecting and preventing a broader range of financial crime.

Data science processes and technologies enable information to be gathered from vast and often disparate data sources to transform businesses' approach to compliance, build financial crime intelligence and support faster, more effective action.

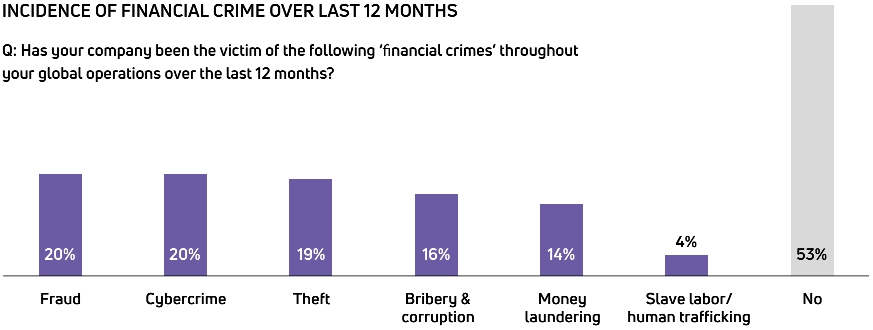
In the fast-moving world of financial crime, data is only as good as the last time it was updated. Real-time, or near real-time data is extremely valuable, as is the ability to analyse it and take action at the same speed. Machine learning not only allows for the analysis of mass volumes of data, but it also offers the power of speed, harnessing the opportunity to quickly and continually detect and react to patterns in a way that humans alone cannot.

While data and sophisticated analytics are the key ingredients for building financial crime intelligence, it is not all down to the machines to wage the war. "Data isn't everything – don't forget the human element," advises Roy Prayikulam, Head of Professional Services at Artificial Intelligence company INFORM, "the knowledge that experts collect over the years is extremely valuable. Yes, machine learning is valuable, however, one size doesn't fit all you must pick your algorithms wisely." Ultimately, developing, training, feeding and monitoring the performance of machine learning is still a human task and proves most effective when combined with expert understanding of how criminals operate and adapt.

> **"Serious and organised crime is estimated to cost the UK at least £37 billion each year"**

INCIDENCE OF FINANCIAL CRIME OVER LAST 12 MONTHS

Q: Has your company been the victim of the following 'financial crimes' throughout your global operations over the last 12 months?



The trick is in finding the balance between technology and the human touch, creating a perfect hybrid that reduces the leg-work for businesses, while increasing the efficiency and effectiveness of identifying and shutting down financial crime.

Know your customer: beyond compliance

Know Your Customer, or KYC is a term frequently used in the world of financial crime - usually in reference to regulation. Naturally, all organisations want to protect themselves against the possible fines, sanctions and reputational damage that result from financial crime - and KYC is a fundamental part of that process. However, there is much more to gain that just meeting the minimum regulatory obligations to avoid taking a financial hit.

The success of criminal activities – whether that is fraud, identity theft, or money laundering - is centred on the perpetrators' ability to hide their activities and their identities. If you increase the transparency around those activities and expose the source, you can confidently act to combat them.

Digital identity specialists, Trulioo, give a concise description of the basic steps involved in KYC:

- Establish customer identity
- Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate)
- Assess the risks associated with that customer through monitoring the customer's activities

The main focus here is to accurately identify genuine customers and legitimate activity; in the process, highlighting those who are not genuine or legitimate. Knowing the customer by using data, intelligent technology and human expertise can help businesses to build customer profiles, track typical behaviours and raise flags when concerning changes happen to those patterns.

But there is also an opportunity to build on the capabilities that 'have' to be put in place for compliance purposes – and use them to great advantage. Going beyond the minimum KYC requirements can help businesses be more proactive in the fight against financial crime and protect against losses. It can also help to power better experiences and more personalised services for genuine customers; the better you know your customer, the better you can serve them.

When it comes to knowledge-sharing is caring

Gaining ground on tackling criminal activities will require more than just the breaking down of internal department and data silos in each bank, merchant and service provider – it will also need the barriers between those organisations to be lowered.

Sharing data is a tricky subject for many reasons. For a start, financial services companies and merchants are often understandably reluctant to share data because of the fear of losing competitive edge or breaching confidentiality.

"Globally, 2–5 percent of the world's GDP ($800 BN–$2 TN) is laundered"

Data protection rules in the form of GDPR and the ePrivacy Directive, which are all carefully designed to protect consumers, also drive a barrier between businesses when it comes to sharing information on financial crime. A recent survey from Refinitiv showed that 86 percent of companies consider that the benefits outweigh the risks for sharing information when collaborating against financial crime, yet 82 percent say data privacy regulations are restricting their ability to do so.

Despite this, there does still seem to be some appetite to pool knowledge, intelligence and resources. For instance, FATF's recommendations on fighting money laundering (which include identity verification procedures) have so far attracted commitment from 205 countries around the world.

There is also an opportunity to share anonymised data and leverage developing technologies, such as blockchain, to build insight across organisations, without the risk of exposing sensitive data. In the fraud space, some solution providers are also now able to facilitate the exchange of confirmed fraud intelligence between both financial institutions and merchants, to create a broad, timely and accurate view of emerging fraud across the payments chain and between sectors.

"Each year, an average of 1 percent of criminal proceeds are detected"

Sharing expertise and best practice is equally as important as sharing data. The Merchant Risk Council, Emerging Payments Association and many other independent organisations have been working for years to build bridges across the payments ecosystem to help support better collaboration through knowledge-sharing forums.

Some private businesses (see the news announcements from PayPal and RedCompass p3) are also now stepping up and offering their expertise and solutions as part of wider efforts to fight financial crime from the ground up using data-driven technology.

The question is whether regulators should now turn their attention from technical standards towards supporting (or perhaps even mandating?) better collaboration across the financial and payments ecosystems. Establishing the parameters for working groups and collaborative technology solutions may serve as a more practical way to achieve the end goals of reducing fraud and financial crime.

Advancing the war on financial crime

While the complete abolition of fraud and financial crime is a utopia we can only dream of, there are strides that, as an industry, we can make towards dramatically reducing it. It will take a large-scale change of mindset and undoubtedly of technology - but it is undeniably a change that would benefit all – except, of course the criminals at the centre of it.

"82 percent of businesses say data privacy regulations are restricting their ability to collaborate"

Going forwards, the focus must not be purely about preventing chargebacks, avoiding fines, or even about compliance, (although obviously that is a 'must' too) but about getting to the root of the problem and taking preventative action and proactive measures wherever possible.

One thing is for sure, constant evolution and innovation will continue to be at the core of the fight against financial crime – criminals will always look for new ways to hide their activities and exploit opportunity. As an industry we cannot afford to rest on our laurels – because criminals won't.

Banks, merchants and many other types of businesses still have a pervasive problem with data and siloed legacy technology – and these issues will certainly need to be tackled before real progress starts to happen.

It will be vital for financial institutions and merchants to work with relevant technology providers, regulators and government authorities to engineer more convergence around financial crime initiatives and intelligence. This will create the opportunity to identify and take down bigger organised networks of criminals and reduce the societal, economic and business impact of financial crime.

Of course, it will be critical for each business to create a sustainable approach to fighting financial crime – one that doesn't drain resources or create a negative impact on the customer experience. This will certainly be a delicate balancing act for most.

It's also worth noting that, while these efforts will cost businesses time, money and resources to implement, the benefits will extend beyond the much-needed impact on financial crime. The very concept of customer identity is at the heart of weeding out criminals, but this same knowledge can also help to serve genuine customers better – giving FIs and merchants the ability to understand and protect their customers more closely.

Fighting Financial Crime with Hybrid AI:

Combining Knowledge-based AI with Machine Learning

Author: Roy Prayikulam, Senior Vice President, Risk and Fraud, INFORM

Machine learning is nothing new. In fact, many of the algorithms used to make predictions have been around for decades. Nevertheless, there is a current hype around the topic of Artificial Intelligence and Machine Learning that spans across nearly every industry, and banking is no exception.

One reason for the increased interest in machine learning is the expanded availability of data. Every transaction can now be supplemented with card information, IP and device data, merchant information, user behavior, delivery addresses, known fraud patterns and much more. However, manually analyzing all this data in a split-second to make a decision about whether it is fraudulent, is not humanly possible. A digital decision-making engine is therefore a must, and by integrating both best practice, knowledge-based rules with data-driven methods, this engine can become a powerful fraud and financial crime-fighting solution.

To clarify, knowledge-driven methods are based on human intelligence and expertise, for example fuzzy logic, statistical profiling, scorecards and other mathematical algorithms. Data-driven methods include data mining and machine learning. Machine learning models require ample data to be able to learn accurately and the necessary volume of data may not always be available, especially with new platforms. This is one of the reasons why the knowledge-based approach simply cannot be disregarded and replaced by machine learning. Combining the best human intelligence-based AI and machine learning technology into a single solution sums up the Hybrid AI financial crime fighting strategy.

Before jumping into a machine learning project, it is of utmost importance to define your goals and determine what questions are being addressed. What are the prediction goals and is there enough data to feed to the machine?

The next step is to start preparing the data. In a typical machine learning project, approximately 80 percent of resources will be invested into data preparation, which encompasses data transformations and feature engineering. Machine learning-ready data can then be split into training and testing sets and a suitable model chosen, commonly either a supervised or unsupervised model.

With supervised learning, the data provided to the machine for learning purposes has clear labels. For example, transaction data can be labeled either as fraudulent or legitimate based on feedback from customers and investigation results. This information is passed on to the machine which seeks commonalities across these labels so fraud predictions can be made and applied to future transactions.

In unsupervised learning, the input data does not have labeled responses - instead clustering and anomaly detection algorithms are used to identify suspicious activity. For instance, imagine that a merchant applies for an account at a bank as a bakery. When assessing the application, the bank can take data from other bakeries and feed it into the machine to search for any unusual activities or behavioral patterns for the new merchant, compared to other bakeries. This approach can highlight application fraud, and can also prove useful for AML compliance topics such as ongoing Customer Due Diligence.

Evaluating a model using a test data set is an important next step. This helps assess performance before exporting the model to real-time production. The move to a real-time engine is often a stumbling block for financial institutions. It is one of the key steps we simplify for our clients with our RiskShield Machine Learning (ML) solution.

When it comes to integrating machine learning into fraud and financial crime fighting efforts, it is important not to try and tackle everything at once. Start with a specific area of business, such as fraud in cards payments or internet banking, and slowly expand after experiencing success. It is an iterative process that should not be underestimated.

RiskShield ML provides everything needed for a smoothly functioning Hybrid AI approach, encompassing both knowledge-based and machine learning methods. The RiskShield Machine Learning environment is used to create and test models that can be implemented in real-time within the RiskShield decision engine. These models can be used to supplement the scorecards, statistical profiling, fuzzy logic and other knowledge-based methods. This results in fewer false positive alerts and enhanced detection of new modus operandi, which increases accuracy. The predictive models used within RiskShield Machine Learning also come with interactive visualization features that make them easy to interpret.

ARE INSTANT PAYMENTS INVITING INSTANT FRAUD?

HELEN OWEN

Consumers and businesses want fast, convenient payments and in the always-on digital economy, real-time, or instant payments are increasing in popularity. While instant payments gained early adoption for one-off (and often large) bank transfers, bill payments and business payments, they are starting to gain ground in the merchant payments environment, as well as for peer to peer (P2P) transactions and mobile payments.

As we've seen with numerous other emerging payments trends, fraudsters always look to exploit the weakest points in the payments chain - and they adopt new methods as quickly as genuine consumers do. While the global adoption of real-time payments has soared in recent years, fraudsters have also moved to capitalise the on the opportunity for instant payouts.

Fast-working fraudsters

There are several areas where real-time payments have opened the door for instant fraud. Authorised Push Payment (APP) fraud, is a perfect example as a form of fraud which is growing rapidly and lends itself particularly well to using instant payments. In an APP fraud, a criminal tricks his victims into sending money directly from their bank account to an account controlled by the fraudster. It is particularly difficult for a bank to prevent, since the ultimate payment is authorised by the genuine account holder, rendering the robustness of a bank's rules-based defences almost useless.

One example of APP fraud is invoice fraud - where a criminal sends an invoice, posing as a legitimate supplier, but instead includes their own bank account details. This often hooks unsuspecting consumers who receive a seemingly genuine request for money, which they may choose to pay by instant bank transfer. This choice loses the customer their money irrevocably, before they have any chance to discover the deception.

Account takeover fraud is another area where instant payments can benefit fraudsters. Once a criminal has managed to gain access to a genuine customer account, they can use the instant payments facility to quickly transfer money between accounts, making it difficult for authorities to track and even harder for banks to stop.

Application fraud is also a common method for criminals who want to make (relatively) quick and easy money. Using stolen or synthetic identities, fraudsters can open new accounts to help extract money and move it on quickly, with the help of instant payments.

Tracking the trends: the UK and India

The UK is an interesting case, since it's one of the most established instant payments environments. The Faster Payment Service (FPS) was launched in 2008, with an initial limit of £10,000 per transaction. In response to strong market demand, this limit has since been increased several times, now sitting at a hefty £250,000 (although individual banks and building societies set their own limits based on their appetite for risk). As a result, instant

"Faster Payments were used for 95 percent of APP fraud in the UK last year"

payments in the UK have rocketed and volumes are predicted to reach more than 1.8 billion FPS transactions by 2025.

It is no surprise that the UK has also seen a rise in associated fraud losses alongside the rise in adoption of instant payments. According to UK Finance, losses due to Authorised Push Payment scams were £207.5 million in H1 2019. Invoice and mandate scams were the second most common type of APP scam seen in H1 2019 and accounted for the largest share of losses, at £55.9 million. The Faster Payments Service was used in 95 percent of cases and accounted for 75 percent of losses by value. In terms of channel, internet banking was used in 68 percent of cases and accounted for 76 percent of losses incurred.

The really interesting place to watch though, is India; a leading light when it comes to payments innovation and strong consumer adoption. Instant payments have exploded there and it's estimated that today nearly 50 percent of all real-time payment (RTP) transactions globally are processed in India. What's as yet unclear is whether their fraud figures are responding in the same way as the UK.

Damon Madden, Principal Fraud Consultant at ACI Worldwide warns that banks and merchants in India must "react at the speed of the market... it demands rapid speed of correlation and decision-making in fraud systems: it's an obvious use case for machine learning. Without it, it's unlikely that any organisation could keep pace with the changes in fraud; as India experiences rapid innovation in real-time payments fraud threats will accelerate at the same pace, so strategies must quickly evolve to combat them."

Think fast, act faster

Across the board (and the globe) there is a need to modernise fraud prevention to match the increasing speed and sophistication with which fraudsters are adapting their methods. Staying on top of changing trends is critical, as is the ability to tailor and scale fraud strategies as needed.

Since fraud teams in both financial institutions and merchants have no real hope of manually intercepting fraudulent instant payments, the reliance has to be on technology that can work at lightening speed and accuracy to detect and block fraudulent real-time payments.

Accuracy is just as important as the speed of decisioning. Instant payments can deliver many benefits to banks, merchants and consumers, but it is also a payments method that many consumers are still tentative with when it comes to everyday transactions. False positives can destroy loyalty and hamper adoption, so it's vital for any screening solution to be finely tuned to avoid blocking genuine customer transactions.

Multi-layered fraud solutions are useful in ensuring optimal accuracy and efficiency, using multiple data sources and screening techniques to give the best possible decision and minimise both false positives and fraud.

When it comes to more difficult trends such as APP fraud, there are now a range of tools specifically engineered to help detect the nuances of this fraud type. For instance, behavioural biometrics combined with APP detection technology that is specifically geared to detecting APP fraud as quickly as possible.

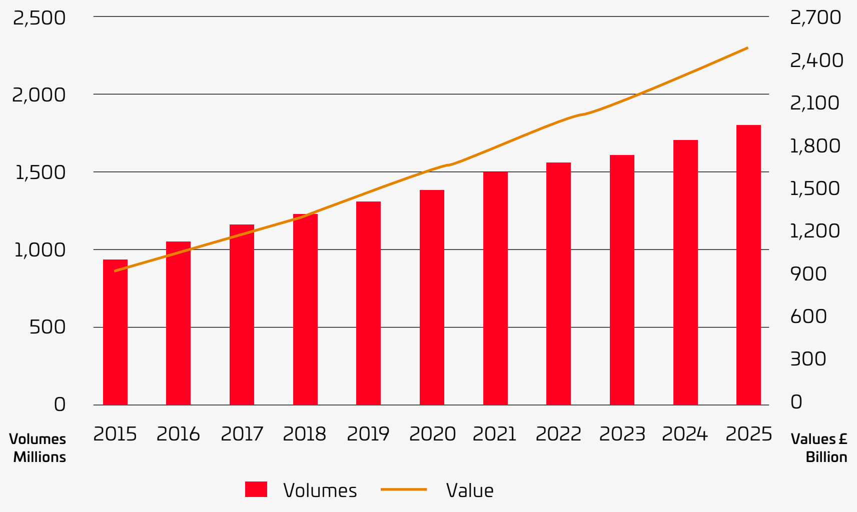
"where there's rapid innovation in real-time payments, fraud threats will accelerate at the same pace"

Behavioural biometrics technology can analyse thousands of characteristics of online banking users in real-time, by testing and profiling tiny nuances in the way a customer interacts with devices and applications. These tests remain invisible to the user, helping to build a strong and sophisticated picture of genuine customer behaviour, without compromising the customer experience.

"Invoice fraud can render the bank's rule-based defences useless"

Instant payments will undoubtedly continue to grow as more customers seek ever more convenient ways to pay and to manage their money. As Open Banking begins to gain traction and more use cases are developed for B2B, B2C and P2P payments, we can expect to see more payment providers leveraging the instant payments rails to deliver a fast, efficient Open Banking service. This further driver for adoption of instant payments will also undoubtedly create more opportunity for the fast-thinking fraudster looking for quick rewards and the industry will have to adapt just as fast to stay one step ahead.

Faster Payment Service Volumes and Values Forecasts



Your Customer’s Account Details Are More Valuable to Criminals Than Their Stolen Credit Card

By Michael Reitblat, CEO and Co-Founder at Forter

In the first six months of 2019, UK consumers experienced fraud losses through UK-issued cards, cheques and remote banking services totalling over £400 million. However, there’s a new threat on the horizon, as data breaches continue to dominate. In 2019 alone, over 100 million credit card application records were compromised through a credit card company data breach, the personal information of over 808 million Facebook users were left unsecured, and over 218 million account log-in records were hacked from mobile game producer platform, Zynga.

As reported in our Seventh Fraud Attack Index, this exposure of personal information led to a 200 percent increase in the number of people who have had accounts opened in their name. Account takeover (ATO) attacks occur when fraudsters gain access to consumers’ personally identifiable data. To a fraudster, stolen account credentials generate a greater value, leading to a variety of illegal activities such as making purchases, altering personal details or leveraging loyalty schemes.

Fraudsters are exploiting the strong links between online accounts and a user’s wider digital identity. Consumers who log in to retail services through social media or re-use passwords for multiple profiles are especially susceptible to these attacks. Since many consumers reuse login details, as they can be reused across several accounts.

Ultimately, ATOs negatively impact merchants – whether it’s taking away from the bottom line through card chargebacks, or reducing the lifetime value of a customer because of lost trust. To protect themselves from this growing threat, retailers cannot afford to look to prevent fraud at the transaction stage alone – they must understand how to detect fraud throughout the customer journey.

Classic ATO

In one ATO attack vector, cybercriminals access an account through stolen user credentials and conduct transactions with the account’s default payment method. The order is then shipped to an address of the fraudster’s choice, which can be either direct delivery or delivery via a mule. Online merchants will typically avoid declining such a purchase if the account has a good reputation, due to the risk of frustrating a seemingly loyal customer. Rejecting a legitimate transaction can result in reputational damage for merchants, with good consumers opting to use alternative retailers.

Added financials ATO

Another common variety of ATO is where the cybercriminal takes things a step further by gaining access to a customer’s account, and then altering the payment method with stolen financial details. This is an especially effective attack method, since many online merchants don’t have the means to identify changes in payment methods, allowing criminals to avoid detection for an extended length of time while repeatedly exploiting a vulnerable account. Detection becomes even harder when an account with a good reputation is hacked and combined with the stolen financial details from another credible account.

Loyalty ATO

Retailers are increasingly offering benefits to loyal and returning customers, but loyalty programmes such as reward points can unfortunately attract unwanted attention. Fraudsters view these schemes as ‘free money’ which they can leveraged by exploiting a vulnerable account. Loyalty ATO comes with only a small chance of detection by the customer, given that the majority of shoppers don’t keep track of their rewards as they would their bank balance.

Automated attacks on a greater scale

Fraudsters will employ sophisticated methods to exploit consumer accounts on a greater scale with the use of bots. Criminals can run code to automate the attack process, which streamlines their operation and allows each step of an attack – from log-in, to altering account credentials, and leveraging loyalty programmes – to be fully automated. Advanced models can even mimic consumer behaviour; a system becomes acclimated to multiple visits by a bot before a purchase is attempted, leading to a greater chance of order authorisation.

How merchants can protect against ATOs

Understanding the threats and vulnerabilities is the first crucial step to defending against ATOs. Despite fraudster methods becoming increasingly sophisticated, online merchants can deploy equally sophisticated countermeasures. To accurately identify ATO attacks, retailers need to look beyond the point of transaction and evaluate 100 percent of the customer journey. They can maximise the accuracy of their fraud detection by analysing each action against past behaviours, from both the account in question and the wider consumer base.

Undertaking this process manually by reviewing the thousands of data points associated with each customer action leads to high rates of inaccuracy, and also increases friction in the path to purchase, resulting in increased drop-off rates and impacting revenue. To protect a loyal consumer base and ensure shopping baskets aren’t abandoned, identifying fraudulent transactions needs to be done in real-time. This requires a fully-automated process that can create and process a nuanced, holistic view of consumer behaviour.

Despite steps to protect e-commerce with incoming regulation focused on the point of transaction – such as PSD2 – the risk of ATOs is likely to continue rising. Cybercriminals are masters at adapting to the changing parameters of e-commerce payments. To protect their businesses, their customers, and their bottom line, retailers must adopt innovative techniques to ensure they keep one step ahead.

4, 5, 6... THE ANTI-MONEY LAUNDERING DIRECTIVE MARCHES ON...

On the 10th January 2020, the EU's Fifth Anti-Money Laundering Directive (5AMLD) came into force. Designed to build on the previous iteration of the regulation, AMLD5 has now brought into scope a variety of new requirements, extending its reach to additional businesses and even individuals.

In summary, the new version of the directive is intended to boost existing transparency rules and reflect changes in technology. This has translated into a number of important changes that have far-reaching impacts for many businesses.

Firstly, businesses such as estate agents, solicitors, accountants and financial services firms are now permitted to use approved electronic methods as their sole means of customer verification. This is good news for many smaller businesses who can now leverage more robust, cost-effective electronic processes within their customer due diligence approach.

The new directive also closes gaps left by it's predecessor, by lowering the transaction limit for prepaid cards, requiring due diligence on the sale of high value goods such as art, as well as changing the requirements around Ultimate Beneficial Owner (UBO) registers, which must now be publicly accessible and interconnected at EU level.

Decrypting crypto

One of the most significant changes is that the AMLD5 has changed the legal treatment of virtual exchanges or cryptocurrencies, which will now be treated the same as financial institutions for the purposes of AML law.

Payments lawyer, Nadja van der Veer explains: "The main reasons for this AMLD change are related to concerns that these exchange platforms had no legal obligation to identify suspicious activity and that the anonymity aspect of virtual currency (VC) allows potential misuse for criminal purposes." She notes, however, that: "the UK National Crime Agency in its latest risk assessment has determined that the use of cryptocurrency for money laundering and terrorist financing is currently low."

Negative impacts

Bottle Pay, a cryptocurrency payments provider from the UK, has been the most recent in a string of crypto startups who have closed their doors (or moved outside the EU) to avoid the impact of the directive's demands. Despite attracting funding and expanding its user base towards the final quarter of 2019, the company found it unacceptable to continue to work under the upcoming EU regulations. The startup, which was only launched in June 2019, developed a tipping service that allowed users to send small amounts of cryptocurrency on social media networks and messengers through its browser extensions. In a statement from the company, Bottle Pay said that "the amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community. We have taken the painful decision to shut Bottle Pay down completely rather than become subject to these new regulations".

The question this raises is whether the continuous raft of legislation is the most appropriate and effective measure, or if it has the potential to overly stifle innovation and add compliance burdens on to businesses that are not well-equipped to deal with the necessary complexity and administrative load.

Reflecting on this, Nadja van der Veer also suggested that "Perhaps the industry doesn't really need any more regulatory changes, but rather requires more focus on collaboration (not only between member states but also between obliged entities) and on how the obligations are to be fulfilled. Regardless, the 5AMLD is here now and the changes seem to be welcomed by the industry, since the regulation of these parties should reduce their vulnerability to criminal activity."

Falling behind

Although some companies may not be prepared for the inevitably difficult requirements that may come their way as a result of the directive, there are undoubtedly other businesses who may choose to capitalise on the opportunity to fill the gap. Banks and other financial services companies who are more accustomed to the burden of regulatory compliance, may seek to experiment with offering their own solutions as a way of innovating and differentiating themselves.

One thing is for sure – many businesses – and even entire countries, are likely to have missed the deadline. It was certainly the case with AMLD4, (only 11 member states managed to meet the requirements in time) but this time the implementation lead time has been shorter.

Failure to comply could mean significant fines – and undoubtedly over the coming months we will start to hear of those who are paying the price.

No time to pause

Despite all this, the sixth iteration of the directive is due to take effect in December 2020, leaving no room to take a breath. Those who are already behind in meeting their compliance obligations may find themselves failing not one, but two deadlines as they play constant catch-up.

> "Those who are already behind may find themselves failing not one, but two deadlines as they play constant catch-up."

So, what has AMLD6 got in store?

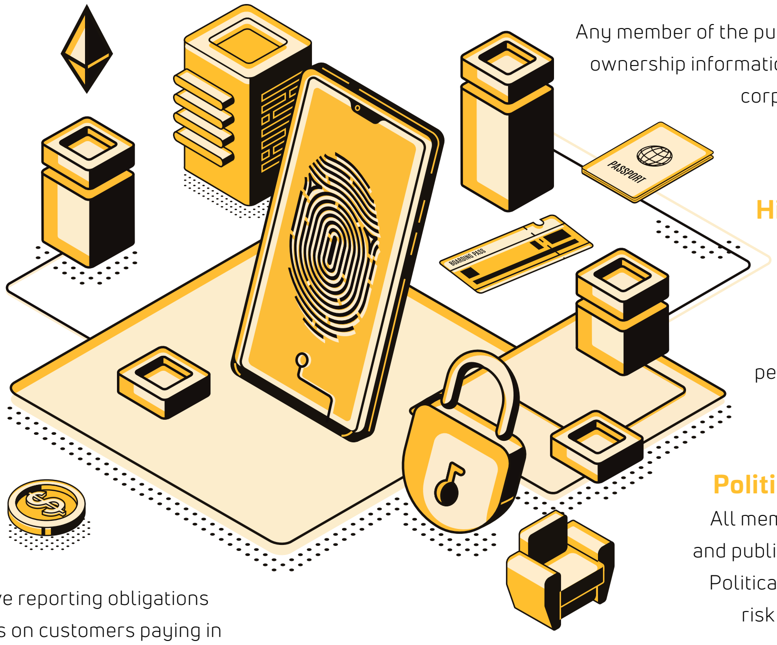
The sixth directive sets out minimum rules for defining what member states should consider 'predicate offences' where money laundering is concerned. It also details additional money laundering offences and even extends the scope of the directive to 'legal persons' or individuals in certain positions. There are tougher sentences for individuals too, with the minimum prison sentence for money laundering offences for individuals increasing from one year to four years, alongside a variety of other "dissuasive" sanctions.

As the speed of introduction speeds up with each iteration of the directive, it is clear that the EU has no intention of relaxing the rules any time soon. As Chris Clements, Partner at Deloitte Forensic, puts it: "The recent stream of anti-money laundering directives suggests the EU's appetite for rules to protect the integrity of the financial system and fighting against money laundering is larger than ever."

The question will be – who or what falls out? And will it strike the right balance in protecting against financial crime, while allowing innovation to flourish. Time will tell.

Who needs to comply?

A snapshot guide to the Fifth Anti-Money Laundering Directive



Cryptocurrency

Cryptocurrency exchanges and custodian wallet providers are now included under the directive as 'obliged entities', requiring them to implement customer due diligence and preventative measures.

Prepaid cards

The 4th AMLD introduced a €250 monthly transaction limit on prepaid cards before any due diligence had to be carried out, the 5AMLD has lowered this further to €150.

High value goods

High Value goods dealers now have reporting obligations including due diligence procedures on customers paying in cash for transactions of €10,000 or more.

Beneficial Ownership

Any member of the public can now access beneficial ownership information held in the UBO register for corporate and other legal entities.

High-risk third countries

Banks and other entities covered by AMLD are now required to conduct increased due diligence checks on any person or entity within the listed high-risk third countries.

Politically Exposed Persons

All member states must now compile and publicly release a functional list of Politically Exposed Persons – higher risk individuals with a high profile political or public role.

Fraud vs Revenue: a costly battle

We know that merchants face an ongoing challenge to balance the fear and cost of fraud against the need for revenue growth.

No merchant wants to leave money on the table from good customers who want to buy their goods and services. Yet, research shows that 30 percent of declined purchases are actually from legitimate customers, having been flagged for violating overly rigid rules set by fraud prevention systems. With these false positives costing merchants 13 times the cost of card fraud, good customers are frequently becoming collateral damage in the quest to prevent fraud.

Traditional solution shortcomings

Having a properly configured, intelligence-based fraud prevention solution is vital. Whilst almost all PSPs and acquirers offer fraud prevention tools as a part of their services, the technical differences, frequency of updates and effectiveness of the different tools are unclear to the merchant. By contrast, the common element for all these fraud screening tools is that they only offer a score or an OPINION on whether a transaction is likely to be fraudulent. A real commitment is offered less frequently or only over a limited set of channels and methods.

As a PSP or an acquirer, does an OPINION provide enough (or any) differentiation or certainty in your offering to your customers, or do they all look broadly the same? Is it enough to make your merchants feel confident they are minimizing their risk and accepting the right transactions?

Fight fraud with no liability

At Vesta, we bring unparalleled accuracy to fraud protection. That's why we can guarantee every approved card-not-present (CNP) transaction. If we're wrong, the fraud is on us. We eliminate the fear and, most importantly, the cost of fraud—all with zero risks and zero liability. This provides peace of mind and a real COMMITMENT to merchants.

Vesta CNP fraud prevention is your new superpower!

With zero fraud liability for accepted CNP transactions, real-time decisions and protection, and no chargebacks or chargeback fees, Vesta can help empower merchants to focus on driving sales and delivering an exceptional buying experience to customers - all without fear of fraud. Plus, this can provide a new revenue stream to PSPs and acquiring banks.

Fraud as a Revenue Opportunity for PSPs and Acquiring Banks

At Money 2020 last October, Vesta announced a partnership where our Fraud Guarantee is promoted directly to merchants by Colombia's leading PSP/acquirer CrediBanco. The solution will help CrediBanco's e-commerce merchants boost their revenues through increased electronic transaction approvals whilst eliminating the risk of loss due to fraud and chargebacks.

This revenue-generating solution can also be provided to PSPs and acquiring banks as a white-label (or Vesta branded) service all around the world.

How do we do this?

Vesta has been a pioneer in processing fully guaranteed CNP payment transactions for nearly 25 years. This year we will guarantee more than $18Bn in payments.

Our solution utilizes:

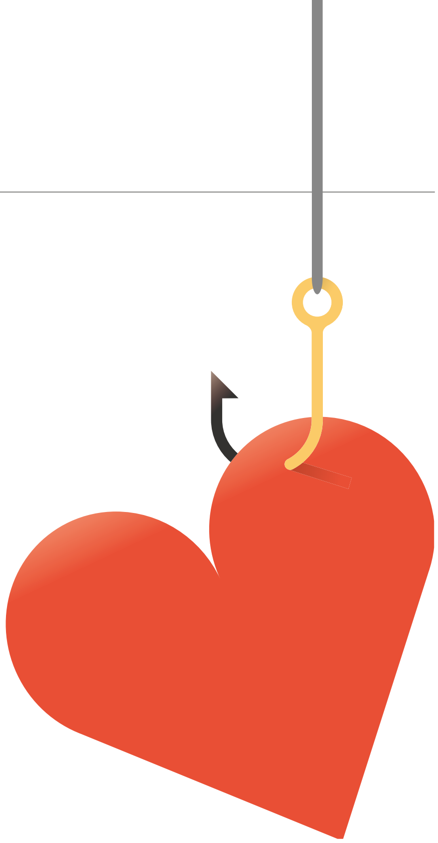
- Supervised and Unsupervised machine learning models
- Deep analysis of consortium data from multiple merchants in multiple geographies
- An expert team of data scientists who review and update models in real-time

vesta

✉ trustvesta@trustvesta.com

www.trustvesta.com

MERCHANTS BEWARE: LOYALTY FRAUD IS LURKING



Loyalty fraud is growing, causing damage to customer relationships and trust across many sectors. Though problematic, it remains a little-talked-about area of fraud suffered by merchants.

Loyalty programmes are undoubtedly a popular and effective way to reward merchants' most valued customers – any they're popular too. According to a report from Kobie Marketing, 86 percent of shoppers said they've joined a loyalty programme to collect reward points and 22 percent of consumers shop exclusively with brands where they are loyalty scheme members.

However, according to recent research by Forter, there has been an 89 percent increase in loyalty fraud attacks in the last year alone, with an estimated $1 billion worth of rewards fraudulently redeemed each year worldwide.

The impact of loyalty fraud is wide-reaching, with both customers and fraudsters using loyalty points as a way to buy goods or services from a variety of merchants. The cost of chargebacks, the lost goods, (often from merchants outside the company whose loyalty scheme has been compromised) damage to reputation and the administration expenses all add up, resulting in a cost far higher than just the reimbursement of lost reward points.

Essentially, one of the key initiatives that merchants are putting in place to create customer stickiness, could be a source of them coming unstuck.

The target on loyalty's back

So, why target loyalty programmes – how lucrative can they really be? An investigation by Connexions Loyalty found that travel loyalty accounts can be quite valuable on the dark web. For instance, they discovered that access to hotel loyalty accounts were being sold at between $1.50-$45 and airline loyalty accounts at $3.20-$208 each.

Loyalty programmes are specifically a favoured target for some fraudsters for several reasons. Firstly, they are often easy to access and use. Loyalty accounts are designed to have a simple redemption process and most accounts are not well protected, usually requiring only a username and password to gain access to and empty the account.

Also, loyalty points can often be redeemed for high value goods and services which have a strong resale value and are easy for fraudsters to offload. For example, airmiles can be exchanged for expensive flights that fraudsters can then sell on to unsuspecting consumers, by posing as a travel agent.

Finally, once fraudsters have accessed a loyalty account, they can often obtain the real customer's personal information and even their stored payment card information – a very valuable bonus that they can then use or sell onwards. In short, loyalty accounts are easy money for fraudsters.

Tackling the problem with payments expertise

Clearly, a customer education process would be of benefit for merchants operating loyalty programmes. Loyalty fraud often goes unnoticed by the owner of the loyalty account because many consumers don't check their balance as often as they would with a bank account or credit card.

A survey from Connexions Loyalty showed that 81 percent of customers treat loyalty and rewards points as cash, but an equal number said they have never really thought about the potential of becoming a victim of fraudulent activity. So, while points are considered as 'money', they are often not protected or monitored in the same way as other forms of payment – by consumers, or by merchants.

There is an argument that loyalty fraud should be proactively prevented in the same way as any other form of payment fraud – and it's safe to say that there are sufficient commonalities in both the fraudsters' modus operandi and the fraud detection methods available for both card fraud and loyalty fraud.

For instance, fraudsters attempting to misuse loyalty accounts will often test the waters to see if they can gain access and try out a small redemption first. If that works, they then proceed with higher value attacks. This is also a tactic that is used by fraudsters testing stolen payment card information. The sources of compromise also have a lot in common with payment fraud, and since it is fair to say that many fraudsters are only one component of a larger fraud scheme, it makes sense to unite all fraud intelligence, including that from loyalty accounts, to build a more complete fraud prevention approach.

So, perhaps the key is not only for merchants (and their supporting payment partners) to better gauge the scale of loyalty programme fraud in their customer portfolio, but also take the opportunity to monitor for suspicious activity, applying the same principles they do for any other payment type. For instance, e-commerce fraud prevention company Forter, specifically suggest using dynamic authentication, real-time screening and predictive modelling to protect customer loyalty accounts and prevent the abuse of loyalty rewards.

Peter Maeder, Co-Founder & Secretary, Loyalty Fraud Prevention Association (LFPA) also suggests merchants "use the experience gained in fighting credit card fraud" to close down on loyalty fraud. He also stresses the importance and value of collaboration; "Fighting fraud can't be a competitive issue – the criminals are not "brand loyal", highlighting that, as with any other type of payments fraud, this is a battle that the industry needs to fight together.

HYBRID
Ai
RISKSHIELD
1001
0001
1101
1011
1001
1101
1101
1001
1010
1100
1101
1111
1101
1001
1100
0101
1101
1001
1100
1101
1001
1100
0101
1011
1100
1101
1001
1100
0101
1011
1001
1010
1100
1101
1111