Data: Your superpower in fighting financial crime

sardine

FINTRAIL

Financial crime is a shape-shifter

Executive Summary

Smart and sophisticated criminal networks are leading the charge in using technology to facilitate fraud and financial crime. As the Financial Action Task Force (FATF) have stated, 'digitalisation and the development of new technologies serve as key drivers underpinning the growth of cyber-enabled fraud'.[1]

Yet today, many anti-financial crime processes are still manual and batch based. With an estimated 30% of a financial institution's workforce dedicated to compliance[2], set against a backdrop of increasing submissions of suspicious activity reports (in 2022, a 21% increase in the UK[3] and a 28% increase in the US for depository institutions[4]), firms need to get smarter and more innovative with their prevention and detection strategies.

It is increasingly evident that to fight against today's threats, standard KYC data points and batch rules-based transaction monitoring are not enough on their own. Firms need to look across the customer and anti-financial crime controls lifecycle to build up holistic and comprehensive pictures of typical account behaviors.

> "I think to succeed in the long term in the future, all controls and teams across the firm need to be talking to each other and working together in a real time manner."
>
> JOHN WIETHORN, AML/BSA OFFICER
>
> gusto

With fraud and money laundering intrinsically linked, breaking down silos to tackle them collectively is key. Creating a core financial crime center that converges fraud with AML to create a holistic risk management approach can bring efficiencies, cost benefits and innovation benefits across a firm.

[1] FATF
[2] Sardine
[3] National Crime Agency
[4] FinCEN

Data is a fundamental component to successful holistic risk management. Data is essential to understand the precise nature of the risks faced and whether controls are working - i.e. risk problems are data science problems. Firms need to ensure they're using as much data as possible, and that the data is clean, normalized and consistent - i.e. they have to get the basics right.

> "The basic fundamentals of data infrastructure and modern warehousing is the thing that unlocks all of the behavioral biometrics and other cool stuff we talk about in fraud prevention.
>
> ANTHONY M. JERKOVIC, DIRECTOR OF DATA

And finally, moving towards real-time continuous monitoring of customer activity, supported by AI and machine learning, is vital to improve fraud and money laundering detection and support more timely SAR submissions. This is especially true with the rise of real-time payments - in the UK in 2022, 98% of authorised push payment (APP) fraud was sent via Faster Payment Services.[5]

> "I don't see why AML efforts should be post-transaction versus fraud monitoring at the authentication stage.' The industry could be even better at preventing money laundering and identifying typologies by looking into transactions real-time.
>
> HANNAH BECHER, FRAUD LEAD & SME TO THE PLEO AI LAB

Financial institutions who take an innovative approach to fighting interconnected fraud and money laundering will better manage the new threats from real-time payments and emerging typologies. By implementing the strategies in this report, leaders can reduce losses, minimize compliance costs, protect consumers, and build trust. The time to reevaluate defenses against evolving financial crime is now.

[5] PSR

Who is ahead in the fraud game?

Fraud is one of the most dominant crimes globally. In 2022 it accounted for 40% of all crime in the UK, with over 3.7 million incidents reported that year[6]. In the US a staggering $8.8billion was lost to scams alone in 2022, over 40% more that the prior year[7]. And Singapore has seen scam cases rise by 400% since 2018[8]. Many governments, including the UK[9], believe that fraud crimes are grossly underreported, begging the question how far and how deep does the 'fraud epidemic' go?

The cost of fraud is a significant and persistent area of concern for financial services including banks, FinTechs, and e-commerce firms. It accounts for a lot more than just the actual losses incurred; it is the resources, legal fees and time spent on investigating, reporting, and recouping funds. And with fraud levels and losses remaining high (UK Finance recorded over £1.2bn ($1.47bn) stolen through fraud in 2022, a staggering £2,300 ($2,800)per minute[10]) the bottom line is that firms need to get smarter, faster and more innovative at preventing fraud in real-time.

While financial services firms continue to explore the use cases of advanced technology, such as artificial intelligence (AI) and machine learning (ML), it is evident that fraudsters are already ahead of the curve in harnessing the power it can bring to their criminal enterprises.

Malevolent actors are refining established techniques such as phishing (spam) emails and social engineering to convince a victim to send money under false pretenses. They are harnessing generative AI and advanced language model (ALM) technologies to create properly formatted emails that are highly convincing and contextually relevant - ones that actually sound like they could be from your CEO. Enhanced programs such as Auto-GPT can automate the prompt delivery process used to make requests of ALMs, using Auto-GPT in conjunction with bots to automatically create and distribute phishing campaigns with minimal effort and human interactions.

[6] Financial Conduct Authority
[7] Federal Trade Commission
[8] Global Anti-Scam Alliance
[9] National Crime Agency
[10] UK Finance

Case study

This story from the UK highlights the very real and traumatic impact fraud can have on its victims[11]. A sophisticated email hack resulted in one individual losing their £240,000 ($294,000) house deposit, while another victim lost £308,000 ($377,500). The fraudster had hacked into the email exchanges between them and their solicitor and sent a fake email from the same address as the solicitor, directing the victims to pay their money into an account under the fraudster's control. These types of frauds are known as 'Friday afternoon fraud', as they often strike then as there will be limited correspondence over the course of the weekend and victims won't find out they have been duped until the Monday morning.

And the threat doesn't stop there - cybercriminals are leveraging generative AI technology to bolster their activities and launch business email compromise (BEC) attacks at rates which are higher than previously seen - the FBI report it as a $50bn industry[12]. Tools such as FraudGPT, WormGPT and DarkBERT, that are available on the dark web, are based on their legitimate counterparts (ChatGPT and Google Bard) and provide instant access to the dark web's underground knowledge base of scams, stolen identities, and fraud tactics.

The lines are becoming even more blurred as the rise of synthetic fraud creates both a fraud and cybersecurity risk for firms. As one of the most difficult crimes to detect, synthetic 'Frankenstein' identities, purchased or created in dark web marketplaces, use real information from different individuals along with fictitious information. The aim is to hold enough legitimate profile indicators to cultivate and build a 'legitimate profile' to bypass KYC checks. With an estimated cost of over $6bn to US banks alone, this type of fraud is fueled heavily by a booming 'fraud-as-a-service' industry. Research from Chainalysis indicates that ransomware crimes are at a record-breaking high in 2023, further highlighting the risks in linked fraud rates.

[11] The Guardian
[12] FBI

AI driven scams are also becoming increasingly realistic and sophisticated. Methods such as voice cloning and deepfake technology are being used to attempt to bypass traditional security controls. Audio samples found online via public sources, such as Instagram or TikTok, can be 'translated' into a target's voice. The power of holding someone's 'voice' alongside their stolen personal and bank details creates a whole new area of controls firms need to consider. The complexity and speed at which generative AI has evolved over the past few years means that further advances in these methods are inevitable in the near future.

The scale of the problem doesn't just affect financial services firms. A recent VISA report noted e-commerce merchants and third party payment gateway providers are particularly vulnerable to cybercriminals looking to acquire payment account data or to bad actors targeting merchants for fraudulent activity[13]. The report stated that e-commerce merchants were responsible for 58% of total fraud and breach investigations in Q1 2023. One law enforcement case from Europol in Europe saw 59 scammers arrested in a multi-operation sting across 19 countries after stolen credit card information was used to order high-value goods online[14].

Criminals also target vulnerabilities in other areas such as telecommunications to support attacks on financial services. One case in Singapore identified malicious actors gaining unauthorized access to the systems of overseas telecoms providers, allowing them to modify the geolocation data of victim's mobile phones, which in turn meant they could divert the SMS one-time passwords (OTPs) sent by the banks. Having already illegally gained their card details these bad actors made fraudulent online 'authenticated' payment transactions affecting 75 customers and totalling S$500,000 ($368,000)[15].

The rise of persistent, agile, and technologically savvy criminals means identifying and stopping fraud and money laundering becomes more difficult.

In this context, how can firms and their anti-financial crime compliance teams effectively combat the rising tide of fraudsters and money launderers? New tools and approaches are clearly needed to keep up with increasing sophistication of attacks.

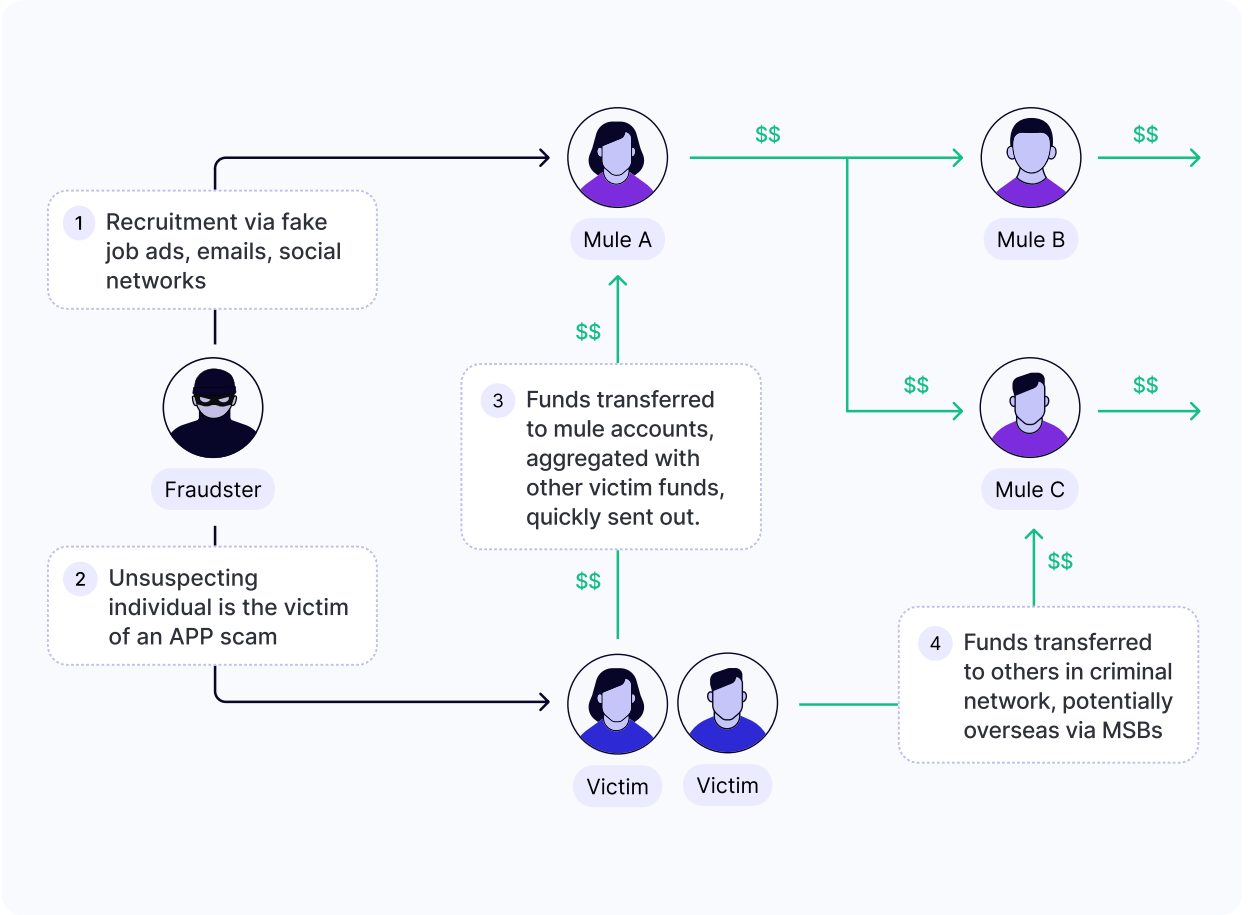
[13] VISA Biannual Threats Report
[14] Europol
[15] Monetary Authority of Singapore

Money mules - the criminal's 'must have'

According to Europol[16], more than 90% of money mule transactions are linked to cybercrime - often using illegal funds siphoned from the activities mentioned above such as malware attacks, phishing and BEC. The UK's National Crime Agency[17] defines a money mule as "someone who lets someone else use their bank account to transfer money, often keeping a little bit for themselves". Money mules have long been synonymous with money laundering, enabling organized crime groups to remain anonymous while moving funds around the world.

When you "work back" from a money muling scheme, a lot of it can be picked up early as low-level fraud, as outlined below:

1. A fraudster runs a scheme to get victims to send them money under false pretenses.
2. To avoid being caught, the fraudster may recruit money mules, often via deceptive methods such as fake jobs, or by targeting vulnerable individuals.
3. The fraudster uses the money mules to receive the fraudulent funds into their accounts.
4. It is then quickly dispersed onto other accounts, ultimately making its way to the fraudster, minus commission fees for the mules.



The illustrative example below of a cyber-enabled fraud (CEF) criminal structure, from FATF's recent report on 'Illicit Financial Flows from Cyber-enabled Fraud'[18] clearly depicts the complexity and connectivity of the structure behind organized criminal gangs, fraudsters, cyber-criminals, money mules and their victims.

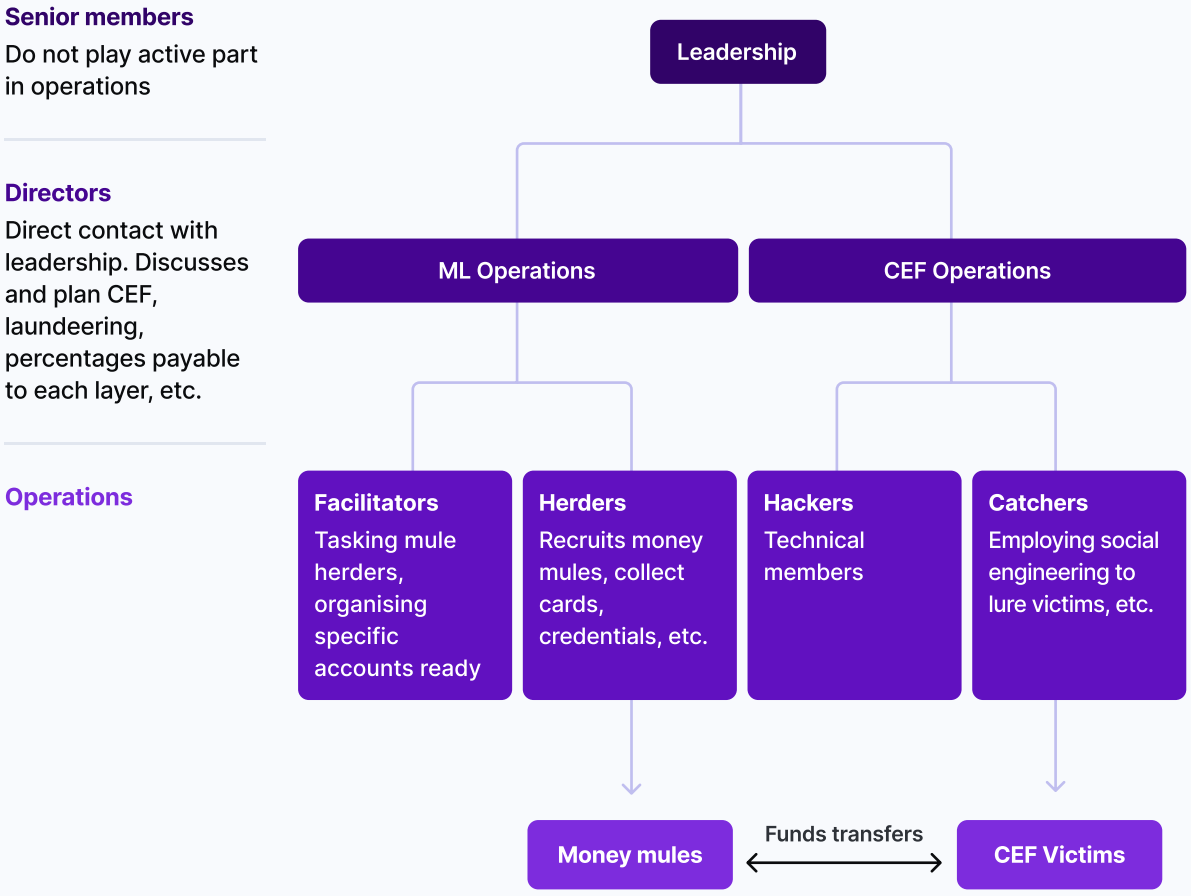


FIG 2: CYBER ENABLED FRAUD CRIMINAL STRUCTURE

[16] Europol
[17] National Crime Agency
[18] VISA Biannual Threats Report

Case study

A global sting operation by Europol[19] shows the scale of criminality through social engineering fraud, with significant criminal assets, recruiting money mules to move the proceeds of the crimes. Criminal-run call centers, suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, e-mail deception, and connected financial crime, were raided by police across 1,700 locations worldwide, resulting in the arrests of over 2,000 fraudsters and money launderers, and the interception of nearly $50m of funds. The Singapore Police Force arrested individuals who were running 'ponzi-like' job scams to recruit victims and using 'money mule herders' to launder money through the victims' personal bank accounts.

Recruiting and managing real individuals to move money requires both time and costs, so sophisticated criminals increasingly use synthetic identities to "mule" the money themselves. They have more control over the funds transfer process, remain totally anonymous, and don't have to pay fees to real-person money mules. Historically, synthetic identities have played a significant role in committing lending fraud. A Federal Reserve paper[20] noted it accounted for 20% of credit losses in 2016, but the newer trend of using synthetics to create mule accounts introduces additional risk to firms as there is no actual person to pursue for payment when fraud occurs. Regardless of whether money muling is conducted by an actual individual or not, firms must have the controls in place to identify and stop this activity.

The UK regulator the Financial Conduct Authority (FCA)[21] recently conducted a review of payment services firms' systems and controls against money mule activity. It noted that in 2022, UK firms reported more than 39,000 accounts linked to mule activity, with criminals using these accounts to transfer and conceal the proceeds of fraud. The FCA noted some positive steps in the industry to enhance controls to spot this activity including facial recognition, device and geolocation profiling, training for staff and customers, data and intelligence sharing, and data and transaction analytics.

[19] Europol
[20] Federal Reserve
[21] FCA

Crucially what the report noted was the (explainable) use of technology, particularly innovative technology to support identifying this activity. *'Investing in machine learning systems helps reduce the inherent risks of static rules-based systems....which lack adaptability to evolving fraud tactics, often resulting in high false positives, and missing sophisticated fraud schemes.'*

Notably the FCA drew out a few key areas for success in tackling this activity. This included:

- The need for both inbound and outbound transaction monitoring
- A combined approach of using device and geolocation profiling and behavioral biometrics alongside transaction monitoring
- The importance of timely updates to rules upon identification of new typologies and risks.

Staying ahead in the fraud game

Below we explore some of the forward-thinking approaches firms should take to tackle problems of fraud and money laundering. We draw on the importance of a holistic approach to financial crime risk management, understanding the data and behavioral indicators open to firms, and the value of real-time monitoring as key controls in tackling fraud and associated money laundering.

The convergence of fraud and money laundering

> "It is critical to understand that fraud is a predicate offense, so, if there's fraud at your institution, by the very nature of it, there's going to be money laundering."
>
> JOHN WIETHORN, AML/BSA OFFICER
>
> gusto

Historically, fraud and AML in financial services have operated independently, driven by different needs and goals:

- **Fraud prevention**

  The primary goal is real-time detection of potential fraudulent activities. Teams aim to detect and block any suspicious transaction or add an extra layer of verification before a transaction goes through.

- **AML compliance**

  In contrast, AML operations focus on identifying intricate patterns of transactions and activities that could suggest coordinated illicit action by crime rings or sanctioned entities. This often requires analyzing transactions retrospectively, rather than stopping them happening up front.

The consequence is different processes, teams, and priorities, each operating in silos. These silos occur when there is limited communication, collaboration, and information sharing between the two teams, resulting in fragmented insights and missed opportunities to detect interconnected fraud and money laundering activities. Illicit funds gained through fraud or other criminal enterprises will undoubtedly become laundered funds - if your firm is experiencing fraud, it will also see the associated laundering of the money.

The term “FRAML” (fraud and anti-money laundering) is not universally popular, but whether you love it or hate it, the reality is that creating a core financial crime center that converges fraud with AML to create a holistic risk management approach can bring efficiencies, cost benefits and innovation benefits across a firm. It doesn’t have to mean that you only have one team to do it all - but breaking down silos by sharing insights, data and typologies will enable a better understanding of how risks manifest and how to tackle them. By working in tandem, these functions can gain a more comprehensive understanding of both fraud and other financial crime. Patterns and trends that may indicate potential fraud or money laundering schemes can be identified more quickly and effectively. The teams can streamline investigation processes, combining the expertise of both functions.

Bringing together intelligence and data of fraud and AML can enhance data utilization, increase adaptability to evolving threats, and ultimately produce better outputs.

> ‘I don't see why AML efforts should be post-transaction versus fraud monitoring at the authentication stage. The industry could be even better at preventing money laundering and identifying typologies by looking into transactions real-time. There are a lot of synergies in terms of investigation that can speed things up; there are often red flags identified in fraud investigations that are very relevant for AML teams.’
>
> HANNAH BECHER, FRAUD LEAD & SME TO THE PLEO AI LAB

Data: Don’t just aggregate it, curate it

Data is a fundamental component to successful holistic risk management. As Sardine’s CEO Soups Ranjan states, ‘All risk problems are data science problems. And all data problems start by getting more data, cleansing it, normalizing it, and then being able to run an analysis over it’.

In short, all data science problems are data engineering problems, meaning firms have to get the basics right. They need large, clean, and accessible data sets to effectively manage their risk. This will have a significant impact on the effectiveness of anti-financial crime controls, especially those that have incorporated machine learning.

> ‘The basic fundamentals of data infrastructure and modern warehousing is the thing that unlocks all of the behavioral biometrics and other cool stuff we talk about in fraud prevention.’
>
> ANTHONY M. JERKOVIC, DIRECTOR OF DATA @ NOVO

The quality of data and capturing the right details is key. Firms need the best data from the best providers to be available when they need it, in the form they need it. This could be phone numbers, email addresses, physical address, credit card bank account details, or social security or local ID numbers.

Firms need one real-time data set to better identify financial crime. This involves addressing a few key areas:

(1) Knowing and understanding your risk profiles across different types of activity. As Travelex Group Chief Compliance and Risk Officer, Daryl Norman, noted: 'You have to be really clear on the risks you are trying to address; if you do not understand your business and the risks that pertain to financial crime you cannot tackle them effectively. You need to clearly understand the modus operandi of those who may try and infiltrate your organisation and how you may be attractive to them.'

(2) Having the right data in the right place so you can identify and assess these risks. Anthony M. Jerkovic, Director of Data at Novo stated: 'My advice to firms thinking about data is if you can store it cheaply, capture everything that's possible - the more data that you have the better; there are countless future use cases for the information that you collect. You're not necessarily going to know today what the use case will be for a data point in the future. The key is ensuring you have the technical and legal grounds to make sure you're pulling in as much data as you can, when you can.'

(3) Doing this to enable more real time identification of risks, as echoed by John Wiethorn, AML/BSA Officer at Gusto: 'I think to succeed in the long term in the future, all controls and teams across the firm need to be talking to each other and working together in a real time manner.

The importance of real-time compliance

The trend toward faster, easier payment systems makes online fraud prevention much more challenging. Payments are becoming more real-time with established schemes such as the Faster Payments System (FPS) in the UK, Single European Payments Area (SEPA) Instant in the EU, and FedNow which launched in the US in July 2023. Instant payments offer convenience and speed to those who use them, but also introduce increased risks of fraud. The benefits they offer to

those using them legitimately are also afforded to fraudsters - they gain immediate, irrevocable control of funds and are able to transfer them to other accounts instantaneously 24×7, reducing the likelihood of recovery.

In 2022 in the UK, 98% of authorised push payment (APP) fraud was sent via FPS[22]. The UK's Payment Services Regulator (PSR) has introduced mandatory reimbursement requirements which are due to come into force in 2024. The new measures mean both sending and receiving firms will be held equally liable for reimbursing victims of APP fraud. The EU is following in the UK's footsteps with similar measures - a version of Confirmation of Payee, and refunds for victims of bank impersonation scams.

Instant peer-to-peer payment platforms such as Venmo, Payal CashApp, and Revolut are also vulnerable to this type of activity. In the US, a report released by US Senator Warren[23] shone a spotlight on the platform Zelle stating it is 'rampant with fraud and theft, with few customers getting refunded'. Due to Zelle being a faster payment person-to-person platform, it has seen scams increase by more than 250% to over $255 million in 2022, compared to $90 million in 2020. In response the US banks who operate Zelle have introduced refunds for victims of imposter scams[24]. This raises the question: as the US continues to embrace real-time payments, will a more holistic approach similar to the UK's reimbursement model be introduced?

> "The challenge when Faster Payments come to [the US] will be consumer expectation that money will be there instantly. There will be a huge need to be on top of real-time modeling when it comes to transaction monitoring, not just from an AML perspective, but from a fraud perspective, and being able to stop funds in-flight."
>
> JOHN WIETHORN, AML/BSA OFFICER
>
> gusto

[22] PSR
[23] Senator Elizabeth Warren
[24] Reuters

FedNow[25] have highlighted the need for participants to evaluate their own approach to fraud management, while highlighting some steps the scheme is undertaking to support it - such as transaction limits, negative lists, transaction reporting, and ISO20022. However, their expectation is clear - participating firms need to ensure their controls are intercepting suspicious activity as early as possible in the payment chain, by having a multilayered approach to fraud management.

While every regulator may have differing approaches to requirements for minimizing fraud, it is evident that with instant payments, you can't put compliance off until later; you must address it real time. As criminals use multiple payment and wallet types for both layering and placement, the use of real-time payments means investigations are made more difficult.

These risks are also evident in transactions that move across fiat currencies and cryptocurrencies, thus visibility across both is needed for effective investigations. A 2022 FBI report[26] noted that fraudsters are increasingly using custodial accounts held at financial institutions for crypto exchanges or having victims send fraudulent funds directly in cryptocurrency. The report noted that cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in 2022, an increase of 183%.

The scale of this activity is immense - Chainalysis research shows known illicit addresses sent $23.8 billion worth of cryptocurrency in 2022 (a 68% increase from 2021) and many illicit transactions that also involve fiat start or end with the use of crypto[27].

Case study: Win Coin[28]

In this particular scam a fraudster named "Lucy Cheong" connected with victims via Linkedin and subsequently cultivated a friendship with them. After a while Lucy suggested they invest together in crypto assets - she showed them how to create an account on crypto.com, transferring money from their bank into a "trust wallet" and then depositing their cryptoassets into an account on wincoin.com. The victims were repeatedly convinced to reinvest, but once they decided to cash out they were told they had to contribute a percentage of feeds to do this and so were unable to cash out. One victim lost $290,000, another $184,000.

Build controls to target specific vulnerabilities

As highlighted earlier in this paper, the correlation between organized crime, fraud and money mule activity is significant and firms need to build out their controls to tackle it. Several controls can be implemented either at onboarding or within ongoing monitoring to identify mule activity, many of which are already in common use, including:

- Controls at onboarding to spot application data points that may be consistent with mule profiles or synthetic identities, or inconsistencies with genuine data
- Monitoring outbound payments for spend that is inconsistent with previous account behavior or out of line with expected trends for the customer profile
- Reviewing inbound payment data alongside outbound payments to look for trends such as short turnaround transactions, or unlinked or overseas third party payments

Monitoring systems may detect unusual activity (e.g. quick and small transfers to multiple accounts or withdrawals that are atypical from the customer's behavior) and flag it as suspicious. When you conduct a thorough investigation with the right data, using behavioral and biometric indicators alongside transactional data, you can intervene earlier to stop money mule and suspicious activity. With the right network analytics you can potentially spot that activity that is part of a larger money mule operation, not just an isolated incident. With so much of the cost of managing fraud coming from false positive alerts, you can turn a deeper knowledge of your customers into a competitive advantage. By monitoring customer behavior to create a deeper understanding of customer intent, it can indicate if they need a new product or are likely to leave your company. Don't just look at red flags; understand and learn from all their behaviors.

[25] FedNow
[26] FBI Internet Crime Complaint Center report
[27] Chainalysis
[28] Department of Financial Protection and Innovation

Prevent fraud at every customer touchpoint

Case study: Know your customer before increasing your risk exposure

In this particular scam a fraudster named “Lucy Cheong" connected with victims via Linkedin and subsequently cultivated a friendship with them. After a while Lucy suggested they invest together in crypto assets - she showed them how to create an account on crypto.com, transferring money from their bank into a “trust wallet” and then depositing their cryptoassets into an account on wincoin.com. The victims were repeatedly convinced to reinvest, but once they decided to cash out they were told they had to contribute a percentage of feeds to do this and so were unable to cash out. One victim lost $290,000, another $184,000.

Passive risk detection uses a number of behavioral indicators that can be used to identify fraudulent or anomalous behavior in a real-time, frictionless way. Before you bring someone through the friction (and cost) of KYC, you need to understand if you have the risk appetite for the customer. In this digital age, firms need to look at digital data as well as the traditional documents used as part of KYC. Monitoring signals across the customer lifecycle can help predict the likelihood of a scam, or spot when a transaction is likely to be fraudulent.

- **Onboarding**

  Spotting synthetic accounts or accounts opened with stolen identities by detecting when mobile emulators and virtual machines are used to change IPs, MAC addresses or browser and OS environments, or identifying if device farms or automated scripts are used during sign-ups.

- **Account login**

  Identifying account takeover or unauthorized users by spotting excessive tab switching, copying and pasting of passwords, logins from unknown devices or locations, stressed typing or scrolling patterns, and suspicious changes to account settings.

- **Account login**

  Detecting fraudulent transfers such as use of compromised accounts and cards, linking multiple accounts or cards in a short time span, identifying

uncharacteristic movement of funds and money muling patterns, and spotting anomalous behavior such as card testing or high velocity transactions.

Case study

How proxy piercing can detect possible sanctions evasion
Device intelligence and behavioral biometrics such as proxy piercing can identify cases where there are high velocity sign-up patterns appearing to be in lower risk jurisdictions but are actually using proxy servers to disguise IP addresses from higher risk, or even sanctioned jurisdictions. Proxy piecing can identify if a proxy IP address is being used and can further pinpoint the location of the end user. One particular use case identified by Sardine found that upon inspection devices being used to sign up customers in short burst in Omaha, Nebraska, had a timezone mismatch and were actually found to be located in higher risk jurisdictions such as Russian and Iran.

Financial crime is a shape-shifter

It is increasingly evident that standard KYC data points and batch rules-based transaction monitoring are not enough on their own. Criminals have evolved, along with the way we transact, and so too should anti-financial crime controls. The powerhouses of criminal enterprises are more sophisticated, more relentless and smarter than ever before. Firms need to look across the customer and anti-financial crime controls lifecycle to build up holistic and comprehensive pictures of typical account behaviors.

> “
>
> You need to understand how the world is changing and continuously refresh your risk profiles and risk assessment to stay current. Look at technology to see how it can best support it and what it can and can not do - AI powered tools will look for things that humans won’t.
>
> DARYL NORMAN, GROUP CHIEF COMPLIANCE AND RISK OFFICER

This means going beyond simply completing account application checks, log-in checks and rules-based transaction monitoring:

- It means combining controls across all customer interactions - transactional and behavioral.
- It means building digital profiles of your customer's normal behaviors to benchmark unusual log-on or session use data.
- It means knowing your customer's devices and how they engage with you via device intelligence - employing controls such as device binding and Strong Customer Authentication (SCA) - a regulatory requirement imposed by the European Payments Services Directive (PSD2) guidelines, which requires two factor authentication.
- It means understanding the transactional information on payments and card usage based on what the customer and typical profiles normally do to flag anomalous transactions.
- It means using holistic risk profiling to score customers and activity to make risk decisions on applications, account access or payment activity and to block or restrict activity or onboarding.

> "What is key for me is connected data, because connected data is an input that you can use for connected information, and connected information means I get better information to make informed decisions. The use of artificial intelligence that can connect different data sources via network analysis will give a more holistic view of customer profiles to assist with investigations."
>
> HANNAH BECHER, FRAUD LEAD & SME TO THE PLEO AI LAB

These controls can provide a clearer, more holistic picture of your customers to narrow down the instances of abnormal activity and allow firms to focus resources in a more effective manner. Combining these while harnessing the real-time use of AI and machine learning can reduce false positives and allow you to

continually adjust your monitoring environment as new threats emerge. Adding in the use of network and graph intelligence to aid investigations and follow activity across multiple payment rails, such as instant payments, cards, or crypto, will ensure teams spend less time manually reviewing transactions and more time identifying patterns like the structure, layering, and placement of criminal proceeds. This will all have a positive impact on your bottom line, reduce fraud and associated money laundering, and have a direct positive correlation with the intelligence you share with law enforcement via suspicious activity reports.

Conclusion

Fraudsters and financial criminals will continue to innovate their operations to become more effective and negatively impact financial services, e-commerce firms and their customers. Investing in your people, by equipping them with the right data and technology, will keep them on a par with the threats they are trying to fight and ensure you can stay ahead of your peers.

> "I see compliance as a competitive advantage because it builds customer trust and it builds trust with regulators, and if you get that right over time you will avoid fines and have better conversion rates. People trust financial institutions with their money and they want to know it will be safe and it won't be stolen, therefore the trust component is an important area to consider. Investing in your compliance controls will foster this.
>
> HANNAH BECHER, FRAUD LEAD & SME TO THE PLEO AI LAB

The predictive powers of AI and machine learning, overlaying a rules-based system, and supported by creative humans will empower your firm with a balanced and flexible approach to fraud detection. At a time of rocketing fraud rates, when the cost of compliance is high and increasing, and the rise of instant payments, firms need to be smarter, more innovative, and faster at deploying AFC controls to free up teams to fight financial crime effectively.

Taking an innovative approach to fighting interconnected fraud and money laundering will better manage the new threats from real-time payments and emerging typologies. Reevaluating your defenses to ensure that they include the following can reduce losses, minimize compliance costs, protect consumers, and build trust.

1. Breaking down silos and bringing together intelligence and data on fraud and AML can enhance data utilization, increase adaptability to evolving threats, and ultimately produce better outputs.
2. Get the data fundamentals right. Firms need large, clean and accessible data sets to effectively manage their risk.
3. High quality, real-time data with real-time monitoring will enable more real-time identification of risks.
4. Understanding your risks and how criminals can exploit your firm will ensure you are better equipped to manage the risks and the vulnerabilities you may have in your controls.
5. Combining controls across your customer interactions - transactional and behavioral - will create a clearer, holistic understanding of customer risk and allow you to focus resources more effectively.
6. Harnessing the real-time use of AI and machine learning can reduce false positives and allow you to continually adjust your monitoring environment as new threats emerge.

FINTRAIL

Overview of FINTRAIL

FINTRAIL is a global financial crime consultancy. We've worked with over 100 leading global banks, FinTechs, other regulated financial institutions, RegTechs, venture capital firms and governments to implement industry-leading approaches to combatting money laundering and other financial crimes.

With significant hands-on experience, we can help you build, strengthen and assure your transaction monitoring programme to meet evolving regulatory requirements, use technology effectively, and stay competitive.

Contact us here.

sardine

Overview of Sardine

Sardine's approach goes beyond just analyzing data. It's about blending advanced technologies with human expertise to create a robust, adaptable system that evolves with fraud patterns.

We drive to have:

1. The best AI models that are constantly updated and consumable as you see fit
2. The most flexible and adaptable rules and rule engine
3. The human support that acts as an extension of your team

Contact us here.