Unmasking Fraud

Dynamic Controls for an Ever-Changing Threat Landscape

FINTRAIL

resistant.ai

Unmasking Fraud:
Dynamic Controls for an Ever-Changing Threat Landscape

This white paper demonstrates that tackling fraud needs a layered defence; there is no single solution or control in the customer lifecycle that alone will tackle the growing threat of fraud. Financial services firms need a clear view of where their fraud weaknesses are and how technology will help. In this paper we draw out different fraud profiles and how firms can look to tackle them. Through practical examples and case studies we highlight how layering controls and taking a holistic approach can provide an effective solution to fighting fraud. Crucially we believe that one control on its own is not a silver bullet; firms need to look across the customer lifecycle to understand where they can deploy dynamic and targeted controls to protect their consumers and assets from fraud.

A fraud epidemic

We are in the midst of a global fraud epidemic which is having a devastating impact on our people, our businesses, and our economy. In the UK over £1.2 billion was stolen by criminals in 2022, the equivalent of over £2,300 every minute.[1]

Fraud was the most common crime in England and Wales in the period from April 2022 to March 2023, with an estimated 3.5 million incidents during this period[2]. And these statistics may only be the tip of the iceberg; it is thought that only 1 in 7 incidents of fraud in the UK is reported. Due to the scale of fraud, the destabilising effect it has, and the harm it brings, there are calls for it to be reclassified as a national security threat in the UK.[3]

With increasing regulation, more stringent enforcement from regulators, and increased political pressure, the expectation and requirements on firms to up their fraud fighting game has never been higher. The UK's Financial Conduct Authority (FCA) noted that firms need to do more *'to detect, manage and reduce fraud and losses more effectively'*[4] and that they will be more assertive in their supervision of how firms tackle it.

Existing measures that have been taken by firms are helping; advanced controls deployed by payment services firms stopped £651 million from being stolen in the first half of 2023[5]. Yet it is clear that more needs to be done. Tackling fraud needs a response that incorporates detection, prevention and redress, underpinned by a clear understanding of where fraud can manifest.

[1] UK Finance

[2] National Crime Agency

[3] UK Fraud strategy

[4] FCA

[5] UK Finance

> *It goes beyond just knowing where your fraud risks sit and what controls you need. There is a real cultural issue that needs to be addressed on how firms commit to managing that risk and if they are prepared to fund and invest in the controls for it.*
>
> Helena Wood, Head of Public Policy and Strategic Engagement, Cifas

The fraud arms race

The political will and agenda to fight fraud in the UK has never been clearer. The UK Government Fraud Strategy,[6] presented in June 2023, aims to cut fraud incidents by 10% and demonstrates a decisive step towards fortifying defences against fraudulent activities. An extra £100m has been committed to bolster law enforcement resources and to empower enforcement agencies, enabling them to tackle fraud with increased efficiency and effectiveness.

> *Fraud is no longer the poor cousin of AML, everyone is now talking about it; it now forms a key pillar of high-level government policy.*
>
> Helena Wood, Head of Public Policy and Strategic Engagement, Cifas

The resounding call to 'block fraud' at its source underscores a fundamental shift towards anticipatory and preemptive measures. Importantly, the regulated financial sector is positioned as a key player in this endeavour, with a clear expectation that it will play a pivotal role in tackling and mitigating the problem. New mandatory reimbursement requirements introduced by the Payments Service Regulator (PSR)[7], which become effective in October 2024, will include mandatory reimbursement for victims of fraud on a shared basis between UK firms sending and receiving proceeds of authorised push payment (APP) fraud via Faster Payments. And government focus to tackle fraud goes beyond the UK; in Europe, the revised PSD3 framework[8] aims to enhance collective efforts to combat fraudulent activities.

The publication of fraud data through the PSR 'league tables'[9] reveals the significant variance across types of payment firms and the role they play in either receiving fraudulent frauds or banking customers who are victims, bringing attention to vulnerabilities and inadequate controls that have been exploited by fraudsters. On the flip side, the performance tables will give firms that are successfully reducing APP fraud losses a competitive advantage, as they will allow customers to see how well individual firms perform in reducing fraud and how well they treat victims.

[6] Home Office

[7] PSR

[8] European Commission

[9] PSR

> *Financial services firms of all sizes are now being held accountable; whether its public perception, data from the PSR, or scrutiny from regulators. This will demand time and resources, and create a greater focus on controls that may have been neglected, such as transaction monitoring, which is often less developed.*
>
> **Kathryn Westmore, Senior Research Fellow, RUSI**

It is important to remember that despite the efforts that the financial sector is making to tackle fraud, success requires a wider approach across all elements of the ecosystem, including social media and telecoms firms. A report by Ofcom, the UK's communication regulator, found that nine in ten online users encountered suspected scam activity, and 25% of them fell victim to a scam.[10] The Online Safety Act brings much needed measures for firms to put in place 'proportionate measures' to tackle fraudulent advertising. And the Online Fraud Charter[11] will take the measures further - some of the biggest names such as Amazon, TikTok and Instagram have pledged to take additional measures to better protect users, including verifying new advertisers and promptly removing fraudulent content.

To paraphrase an old proverb: 'It takes an *entire network* to *fight the fraudster*'. It is vitally important that all industries across both the public and private sector come together to tackle this issue.

There is no one size fits all fraud approach

The fraud phenomenon is the result of the rise of opportunistic and sophisticated criminals leveraging technology, abusing weak controls, and deploying social engineering to commit fraud on a widespread basis. A recent report by the Financial Action Task Force (FATF) highlights the sophisticated organisation and structure of transnational organised crime groups (OCGs) who are executing cyber-enabled fraud and associated money laundering, outlining that their schemes are often multi-layered and complex and *'are regularly composed of well-educated and technically competent professionals.'*[12] Many OCGs have turned fraud into a professional industry complete with 24/7 call centres to facilitate their activities.
At one end of the spectrum there is the notorious 'KK Park' - a Chinese-run fraud factory in Northern Myanmar often using victims of human trafficking to scam unsuspecting victims online or by telephone[13]. At the other end of the spectrum, online document template farms which produce fake IDs and bank statements, are making fraud-as-a-service available to anyone with a simple Google search, with some sites racking up millions of visitors a month. These are nowhere near as complex, but they remove barriers to entries to first party fraud at a massive scale, making it much more accessible.

More often than not, firms are facing career fraudsters, whose full-time job is to devise new and innovative ways to commit fraud and seek out weak defences in organisations. Criminals will employ

[10] Ofcom

[11] Home Office

[12] FATF

[13] BBC

different strategies for different types of fraud, often deploying a combination of tactics - a shell company, the use of money mules and document forgery - to conduct their activity. Firms seeking to reduce fraud must bear in mind that each tactic may require different controls or combinations of controls, meaning that focusing on one control area alone will not be enough.

Fraud prevention is not a one-size-fits-all exercise; it is a dynamic and multifaceted strategy that demands a holistic approach. Firms must address fraud throughout the entire customer lifecycle and across various control domains, to identify potential issues and address weaknesses and gaps. It is crucial to recognise that a specific control, while effective against a particular type of fraud, may not necessarily provide adequate protection against other forms of fraudulent activities.

Strengthening your fraud defences

Adaptive detective and preventive controls at every stage of the customer journey will build a proactive defence against the ever-evolving landscape of fraud and stop both fraudulent transactions and mule accounts in their tracks. But the key is to remember that no one individual control will make a difference across the fraud spectrum - deploying a combination of behavioural, detective and real-time monitoring controls across the customer lifecycle will all contribute to weeding out that corporate account being used to receive the proceeds of fraud, or the credit card opened with a stolen identity, or the account that has been subject to account takeover. Below we outline the core components that financial institutions need to be thinking about when assessing their fraud vulnerabilities and controls.

> *Bringing together a holistic understanding of different types of fraud, how they are evolving, how they overlap and what the controls are that deal with that type of behaviour is essential.*
>
> **Kathryn Westmore, Senior Research Fellow, RUSI**

1. Start with the right foundations

Tackling fraud isn't a one-step process or even a discrete component of an anti-financial crime programme. It is important to get the foundations right, which means starting with a clear fraud risk assessment and a defined risk appetite statement. Unlike other areas of financial crime, it is easier to put a tangible financial cost against fraud risk. This can help define your risk appetite statement, drive priorities and help manage resource allocation.

Firms gain insight into their fraud vulnerabilities by assessing their exposure to specific types of fraud, pinpointing gaps in existing controls, establishing risk tolerance, implementing targeted solutions for specific issues, and continually refining the strategies through iterative processes. It is not enough to have two line items in your risk assessment - one focusing on internal fraud and the other on external fraud - and listing a range of generic controls. A risk assessment should involve a comprehensive understanding of potential weaknesses to different fraud types, a careful examination of control deficiencies, and a clear articulation of the organisation's risk tolerance.

Understanding the evolving fraud landscape, including the latest scams and digital threats, is crucial in building a resilient defence. Staying alert to trends shown by your own data, keeping abreast of alerts from law enforcement, sharing typologies across communities, such as the FinTech Financial Crime Exchange (FFE)[14], and leveraging data across the industry from bodies such as Cifas[15], will keep you informed on what fraudsters are doing so you can assess the robustness of your controls against known typologies.

> *You are always one step behind the fraudster. Be aware of what solutions are out there and keep monitoring fraud trends. Just because you don't have an issue with a type of fraud now, it may not stay that way. Lay the groundwork and get ahead of fraud trends by knowing how you would tackle it when you do see it.*
>
> **Charlie Davis, Fraud Manager, Capital On Tap**

Case Study:

Know your enemy

Challenge

A cross-border money transfer business that focuses on offering online banking services to migrants worldwide wanted to review its fraud controls and make programme enhancements to help it scale safely.

Solution

The company gained an in-depth understanding of its specific fraud risks and fraud-related controls through initiating a desktop review of its financial crime documentation and running a series of thematic workshops. This generated observations on areas of good practice and actionable recommendations for areas of improvement by theme (onboarding controls, transaction monitoring, risks, governance). These included implementing a customer risk assessment methodology that reflects fraud risk, defining a fraud-specific risk appetite, scaling governance and oversight operations in line with business growth, technical enhancements to the onboarding process, and new inputs into the transaction monitoring system.

Outcome:

The firm was able to benchmark its current controls against best practice and identify areas for improvement and new technical capabilities to enforce the key control areas of onboarding and transaction monitoring.

[14] The FFE is a global network of fintechs collaborating on best practices in financial crime risk management.

[15] Cifas is a not-for-profit organisation working to reduce and prevent fraud and financial crime which runs the UK's largest cross-sector fraud sharing database.

2. Know who your customer *actually* is

One of the most effective ways to tackle fraud is at onboarding - restricting bad actors' access to your firm will reduce the risk of your products being abused for illicit financial gain or being used as a mule account to receive the proceeds of fraud. Stolen or falsified identities, fake companies, and forged documents are tools fraudsters are using at scale to access financial services. Onboarding truly is the first line of defence in tackling many types of fraud. Standard controls, such as, electronic identity verification tools and verifying data against government recognised websites, will provide some protection. But given the sophistication of fraudsters, their use of technology, known problems with corporate registries and the ease with which shell companies can be established, standard checks in their own right will not be enough.

Firms should consider additional techniques such as:

- Deploying tech-enabled IDV checks to identify synthetic identities and fake selfies and videos.
- Using document forensics to uncover digital alterations to documents and analyse them for forgeries.
- Implementing tools to identify patterns such as reused documents like forgery templates and stolen identities.
- Conducting pre-onboarding checks to assess behavioural indicators, such as bots used for application form submissions, or device attributes that can help detect repeated or automated attempts to create accounts.
- Capturing data points at onboarding to be used in ongoing monitoring e.g. device identifier, geo-location data, expected account usage.

> *Customer behaviour analysis is an important control in looking for anomalies. Fingerprinting your typical customer behaviour at onboarding, such as their device ID and geolocation data, and using that over the customer lifecycle to identify unusual variance can be a key tactic in identifying fraud.*
>
> **Jeremy Williams,**
> **VP Compliance, Silverbird**

Fraud profile: Burner firms

Fraudsters are using apparently legitimate companies to convince unsuspecting victims of their credibility and dupe them into sending them money. Due to widely reported issues with the UK corporate registry Companies House, fraudsters can create shell companies in minutes for just £12. The creators of these so-called 'burner' firms use stolen names and addresses to set up companies that give the authenticity needed to trick people into believing in products and investments they are being sold that are literally too good to be true.[16]

[16] The Times

Fraud profile: Identity fraud

In 2022, Cifas reported that identity fraud had reached unprecedented levels - 68% of all fraud reported in 2022, with the majority of cases occurring through online channels.[17] Identity fraud, also known as 'ID theft,' occurs when someone uses stolen personal information to commit a crime. Many victims remain unaware of how their details were obtained, and the problem is growing as cybercriminals become more sophisticated, and personal data becomes increasingly available to purchase on the dark web.

Fraud profile: Synthetic identity fraud

Synthetic identity fraud involves combining real people's personal details, such as their date of birth or address, with other falsified data to create a new identity. Criminal organisations can generate tens or even thousands of fake accounts/profiles at once, operating on a large scale for maximum impact. The fact there is no identifiable victim to associate to the account makes this harder to identify and detect. Accounts with either credit card or e-commerce firms can be run for months with small purchases and regular repayments, building to a higher credit limit and leading to a significant purchase or transfer of funds which is never repaid.

Case Study:

Synthetic money mule accounts receiving the funds of APP scams

Challenge

A global B2B online payment merchant encountered instances (up to hundreds per day) of synthetic money mule profiles being used to open accounts to receive the proceeds of authorised push payment (APP) fraud.

Solution

A combination of document fraud detection and behavioural analysis revealed links between apparently different identities. It exposed recurring document templates being used, instances of document forgery and consistent behavioural traits exhibited by customers (mules) during the application process.

Outcome

Through the combination of the controls implemented, the firm now rejects approximately 2% of its applications due to fraud. The firm now has such high levels of confidence and accuracy in rejecting such applications it can reduce other measures which create unneccessary friction for genuine customers. This has led to significant cost savings, reducing over 1,200 hours spent on onboarding checks, offboarding and compliance reviews. Furthermore, it minimises the risk of potential regulatory scrutiny and claims under the UK's upcoming reimbursement model.

[17] Cifas

Fraud is a numbers game

Fraud is often conducted at scale; firms are facing large scale industrial attacks using efficient and sophisticated models which are hard for analysts to detect with the human eye alone. This can occur via 'retail' fraud-as-a-service models which distribute editable fraud templates on platforms like social media and online marketplaces. It can also be seen in more mature, sophisticated, startup-like operations. These enterprises use automation and iterative experimentation to bypass controls, enabling organised crime at an unprecedented scale.

To combat this, financial institutions must deploy comparative systems that assess all incoming documents and associated behaviours. While human oversight remains crucial, it needs to be complemented by advanced technology capable of identifying and clustering related fraudulent activities. Humans alone cannot detect all types of fraudulent documents, particularly with unstructured documents, such as utility bills or bank statements. It is more challenging to achieve consistent manual results across multiple jurisdictions and languages against sophisticated document templates. Scalable and faster solutions, such as AI-led document forgery detection models, can remove friction, reduce human intervention, and increase automation.

Case Study:

Fighting fire with fire

Challenge

A global B2B payments provider experienced attempts to bypass multiple onboarding checks using AI. This included the generation of fake faces for ID and liveness checks and generation of text in the application forms.

Solution

The implementation of advanced AI technologies designed to fight AI-enabled fraud was a key tool for this firm. By being able to distinguish fraudulent profiles through ID and liveness checks, the model was able to filter out non-existent entities, identifying discrepancies and inconsistencies that indicated fraudulent behaviour.

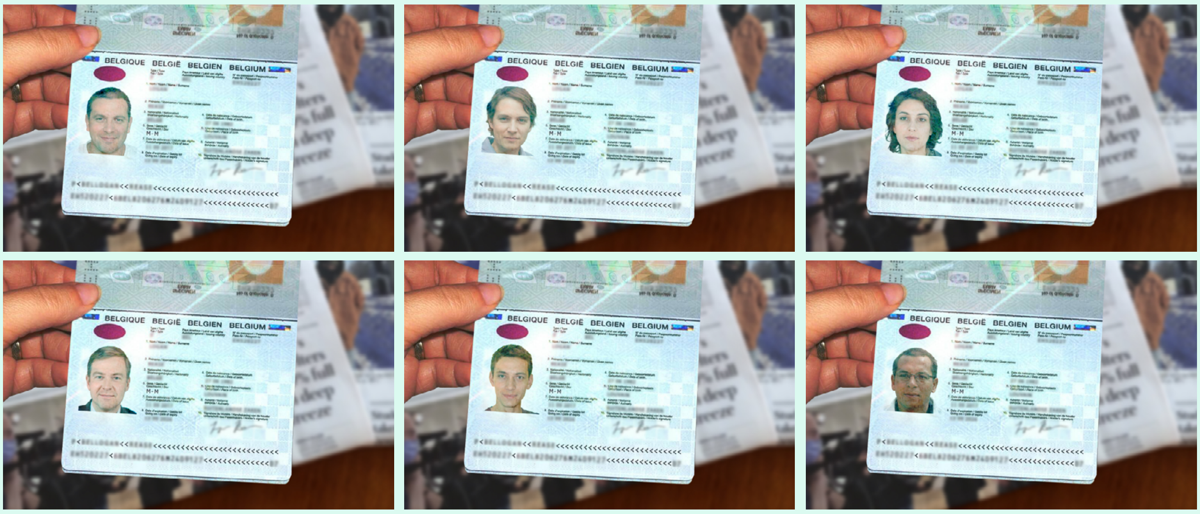
Outcome

Document fraud detection found 0.5% of application forms had repeated generated copy - given the hundreds of thousands of applicants a month, this created a significant positive impact in weeding out false applications.

Continued overleaf

The image below shows Belgian passports with 100% computer generated faces. With the right technology these types of scalable attacks are still relatively simple to detect since the criminals make the same mistakes over and over when producing them.

Gen-AI ID fraud



3. Fraud controls are for life not just for onboarding

Firms need to understand the way in which accounts/products can be abused after onboarding to commit fraud or receive fraudulent funds. To ensure the control framework is robust firms should regularly update and review customer information to ensure the accuracy of information on file. Firms should understand how the information and data obtained at onboarding can be used to identify anomalous behaviour or potential account takeover during the course of the customer lifecycle. Controls such as 2 factor authentication, one-time passcodes, and customer education should work alongside tools such as device and behaviour monitoring to build a deeper layer of defence and identify issues before it is too late.

Firms should consider techniques such as:

- Monitoring customer behaviour compared to historical baselines to look for significant changes that may indicate account takeover.
- Using device and geolocation profiling to match expected customer interactions against those that may be unusual.
- Using device binding for ‘protected actions’ such as gaining access to funds, changing card addresses or provisioning cards to Apple wallets.

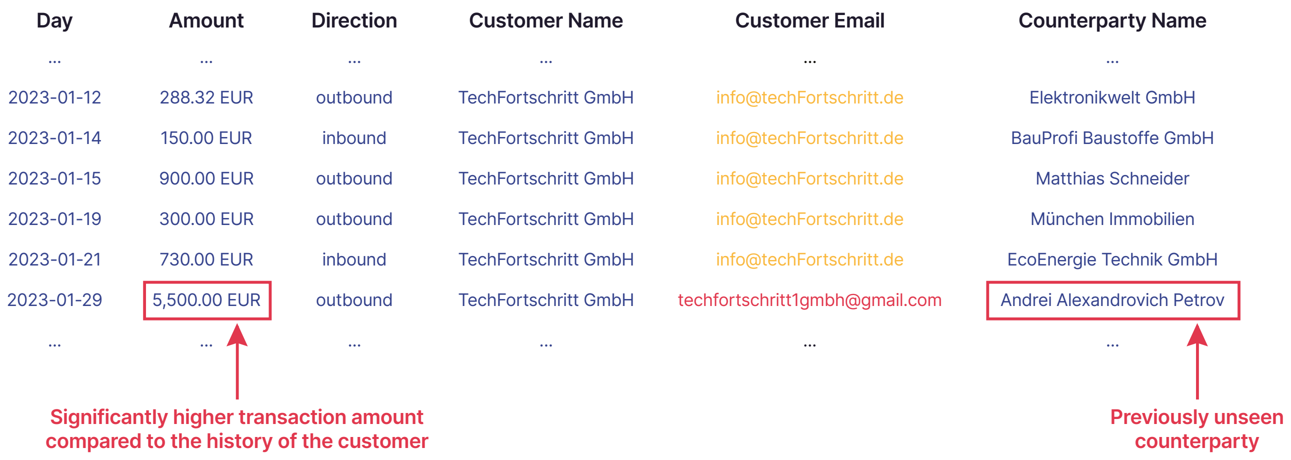
These controls become more powerful by working alongside each other and by sharing information and data across the control framework. Using a combination of controls both at onboarding and ongoing monitoring, complemented by robust transaction monitoring will create the strongest defence in tackling fraud.

Fraud profile: Account takeover

One technique commonly used by fraudsters is account takeover. Criminals employ various methods such as credential stuffing, malware, mobile banking trojans, and phishing to gain unauthorised access to accounts. Once they succeed, they withdraw funds, make purchases or steal customer information, which is further misused and exploited. Research by Cifas showed that malicious actors are calling contact centres posing as customers to learn information about the verification process and are using this knowledge alongside social engineering to target consumers and gain access to accounts. 60% of account takeover fraud involves a ‘legitimate’ contact centre, even if the fraud attempt occurred through another channel.[18]

The image below shows that immediately after the password was changed on a customer’s account, an unusual amount was sent to a new counterparty indicating account takeover fraud.

Using customer behaviour changes to spot fraud



Day	Amount	Direction	Customer Name	Customer Email	Counterparty Name
...	...	...	...	...	...
2023-01-12	288.32 EUR	outbound	TechFortschritt GmbH	info@techFortschritt.de	Elektronikwelt GmbH
2023-01-14	150.00 EUR	inbound	TechFortschritt GmbH	info@techFortschritt.de	BauProfi Baustoffe GmbH
2023-01-15	900.00 EUR	outbound	TechFortschritt GmbH	info@techFortschritt.de	Matthias Schneider
2023-01-19	300.00 EUR	outbound	TechFortschritt GmbH	info@techFortschritt.de	München Immobilien
2023-01-21	730.00 EUR	inbound	TechFortschritt GmbH	info@techFortschritt.de	EcoEnergie Technik GmbH
2023-01-29	5,500.00 EUR	outbound	TechFortschritt GmbH	techfortschritt1gmbh@gmail.com	Andrei Alexandrovich Petrov
...	...	...	...	...	...

Significantly higher transaction amount compared to the history of the customer

Previously unseen counterparty

Automated alert summary: An account TechFortschritt GmbH sent an anomalous amount (5,500.00 EUR) to a new counterparty Andrei Alexandrovich Petrov immediately after a change of email. The customer recently updated their password.

> *Creating a dynamic approach to ongoing monitoring that responds to changes in customers behaviours or account activity, such as increased transaction monitoring or increased customer interactions, may stop fraud before it occurs or before it becomes a greater issue.*
>
> **Jeremy Williams, VP Compliance, Silverbird**

[18] Cifas

4. Focus on transaction fraud prevention and detection

A key component of your fraud control framework is transaction monitoring. With the mandatory reimbursement changes coming into play in the UK in October 2024, firms will have to focus on both ends of the payments cycle, both incoming and outgoing, to identify fraudulent behaviour. You don't need to start from scratch here. Employ real-time monitoring systems to scrutinise transactions and activities as they occur (prevention), and build on your existing transaction monitoring rules or models to align them to specific fraud typologies to support post-transaction monitoring (detection).

Case Study:

Combining documentation validation with transaction monitoring

Challenge
A European FinTech offering corporate banking services experienced high rates of fraudulent documents submitted in response to requests for information (RFI) relating to high-risk transactions.

Solution
Documents that were submitted in response to RFIs are now automatically assessed by a forgery detection engine for signs of fraud and modification. Given the variety of formats and geographies of the documentation received, the tool is more effective than the human eye in spotting forgeries.

Outcome
In addition to strengthening the identification of fraud, this also reduced the amount of time being spent by analysts manually reviewing documents.

Fraud profile: APP scams

APP scams are where individuals are deceived into sending money to a fraudster. This deception can take various forms, such as tricking someone into paying for non-existent goods or services, impersonation scams, romance scams, and fake investment opportunities. UK Finance stated that losses due to APP scams in 2022 were £485m . The media tends to focus on consumer APP fraud, but the figures are also stark for fraud against businesses and the public sector. The same UK Finance report noted that businesses accounted for 15.9% of APP fraud losses in 2022. Firms are often susceptible to business email compromise (BEC) and CEO impersonation scams.

Case Study:

Real time detection of BEC fraud

Challenge

A global B2B payments platform was able to identify over $1 million of previously undetected fraud linked to BEC scams by enhancing its rule-based detection.

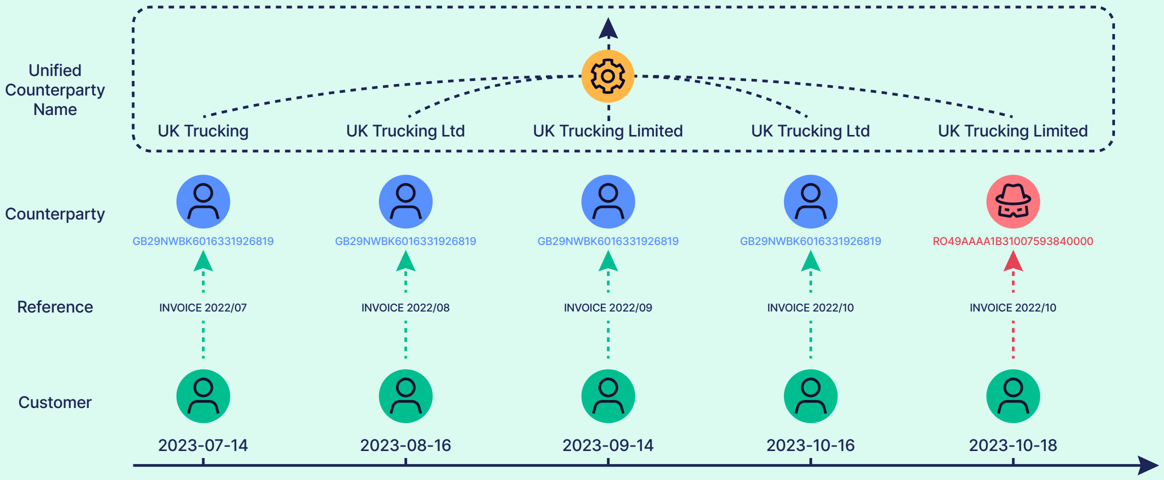
Solution

The AI-led detection demonstrated a heightened ability to perceive unexpected variations in payment patterns, particularly in scenarios where there were noticeable shifts in the counterparties associated with a series of transactions, such as changes to new but similar counterparty names.

Outcome

The firm could identify unexpected changes in customers' regular payments and flag these transactions for review before they were processed. For instance, the model flagged instances where the counterparty names underwent alterations, highlighting where payments had been compromised and altered at the request of fraudsters.

Payee amendments leading to APP fraud



Automated alert summary: Counterparty ID for a sequence of transactions with normalized counterparty name "UK Trucking" changed, which may indicate Authorized push payment (APP) fraud. The last transaction with "UK Trucking" was sent to RO49AAAA1B31007593840000, contrary to past 4 transactions using GBNWBK60161331926819.

Pre-transaction monitoring (prevention) is concerned with real-time processing of transactions with a view to blocking or holding transactions where there is suspicion of fraud or financial crime. This allows for immediate detection of unusual patterns or suspicious behaviour.

AI-driven real-time monitoring can spot anomalous behaviour e.g. statistical anomalies can flag suspicious money flow typologies and relationships between accounts — highlighting fraudulent accounts, account takeovers, and money mules and reducing your fraud exposure. It can also learn and adapt, ensuring your controls are continuously improving and customer friction is minimised. The use of large language models can predict and highlight discrepancies between payment references and the payment amounts, indicating fraudulent transactions. You can also use it to identify examples of payment beneficiary name changes to a company with a similar name - an indicator of APP fraud. Crucially, real-time transaction monitoring can inform decisions to preemptively block payments or accounts to stop the receipt of further payments or hold outgoing payments for review. Over time, AI-led transaction monitoring can learn from data it receives and from analyst decisions, adapting to emerging threats and improving the performance of the controls on an ongoing basis.

> *Being able to quickly deploy changes to transaction monitoring to respond to new threats and typologies is crucial for a dynamic and responsive fraud approach.*
>
> **Jeremy Williams, VP Compliance, Silverbird**

In terms of post-transaction monitoring (detection), firms should understand their fraud risks and align scenarios to capture the patterns of behaviour that may indicate fraudulent behaviour - e.g. inactive accounts with burst of activity; repeated receipt of unrelated transactions; movement of funds to high-risk jurisdictions. They can then implement timely updates when they identify new typologies and risks.

Post-transaction monitoring also presents an opportunity to look further than individual transactions. By using pattern recognition or trend analysis firms can take a broader view and focus on more organised networks and complex cases. It can be exploratory and identify evolving threats. Undertaking these types of review post-transactions will reduce friction and contribute to a more robust control framework.

5. The power of collective controls

Strategic investment in advanced technologies is the forward-looking approach to fraud prevention. By leveraging data and insights across the different layers of controls you can better protect your customers and firm against fraud. While transaction monitoring alone may identify an unusual payment, assessing it against the knowledge that a different device was used to make the payment, or a new payee was just set up on the account could indicate account takeover. With more information comes greater power in tackling fraud. But controls need to work in tandem and be designed to collect and disseminate this information across teams and processes. A combination of controls can also be used to enhance risk detection, remove additional friction in the customer journey, or reduce tasks that require manual review. An example of this could be using ID verification alongside bank account verification to confirm identity rather than relying on one source alone, alongside using document forgery technology for proof of address documents. This can enhance risk detection, remove manual processes such as document reviews, and take friction out of the customer journey.

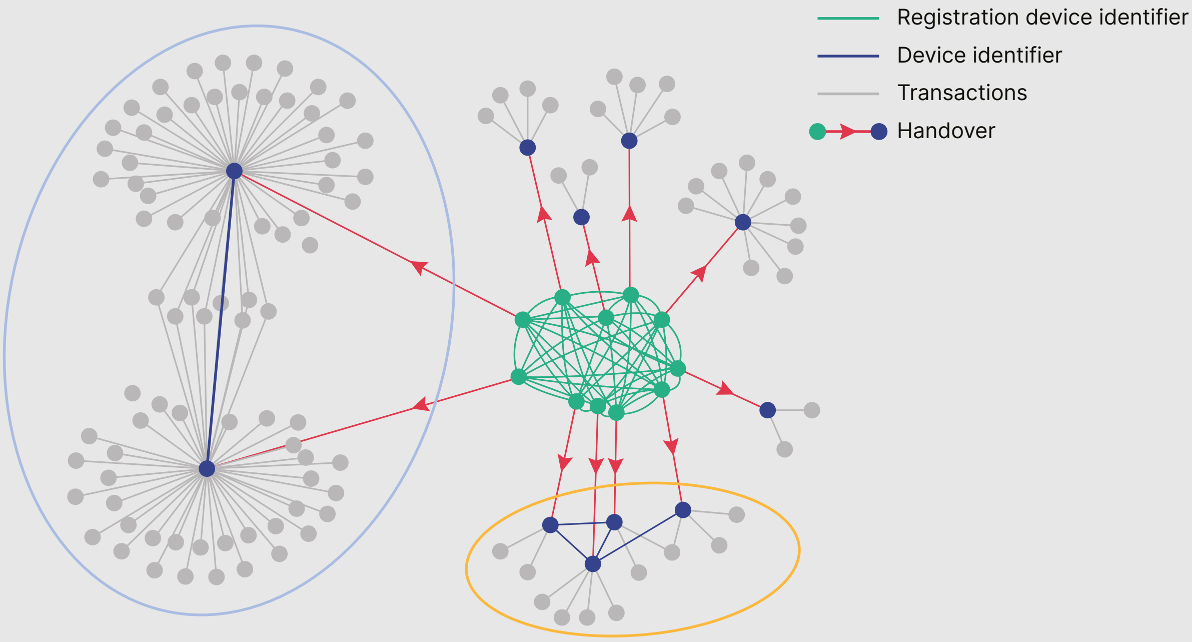
> *As you scale, reducing the amount of manual intervention in your fraud controls is important. You need to understand where fraud controls can be aligned or combined to assess scenarios where the risk is less, allowing less manual reviews and more automation.*
>
> **Charlie Davis, Fraud Manager, Capital On Tap**

Combining insights:

Using information from onboarding to spot account handover

Account handover is where an account or a group of accounts is created by one party and then willingly handed over to another party for money muling or other illicit purposes. The registration device used to complete onboarding (e.g. laptop) may be seen across multiple accounts. After onboarding, control of these accounts is passed to unconnected groups which use different devices to access the accounts, e.g. mobile phones. In the account handover scenario the account is created from one device identifier which is subsequently not used anywhere in the future, which can indicate potential mule or illicit activity. Having insight of this early in the account lifecycle can potentially identify fraudulent accounts before significant losses occur.

Muling by multiples



Staying abreast of evolving fraud tactics requires financial institutions to deploy smarter and more efficient solutions, such as AI and machine learning, to detect and respond to emerging threats in real-time. These become even more relevant when used to link together different data sources and information at various stages of the control framework. AI and machine learning can be used to enhance fraud detection across the customer lifecycle, such as:

- Pattern recognition: using AI algorithms for pattern recognition to identify anomalies in data and user behaviour, enabling the early detection of potential fraud.
- Behavioural analysis: employing AI to analyse user behaviour over time, creating profiles that help in recognising deviations from normal patterns.
- Predictive modelling: developing predictive AI models to forecast potential fraud risks based on historical data and evolving trends.
- Network analytics: identifying connections between transactions and accounts to identify possible mule networks.

> *Busting that myth that you need perfect data or 12 months worth of data for example to do anything with AI, helped us to start small there and think about how we wanted to move on from that and use AI elsewhere in our detections.*
>
> **Billy Pinder, Global Head of Transaction Monitoring, Currencycloud**

Data can play a huge role - and remember, you can get started with minimal data; it's an iterative process, you don't have to wait until you have 'perfect' data, and new data points can be added as they become available. Firms should start by having a clear view on what data they have access to, then assess what types of data they need to start collating, to build this into the fraud control framework over time. They don't need to change it all over night, but a plan and direction on how to get there will help.

> *Technology will be such a big part of how to manage fraud risk due to the sheer scale of the current problem - you need investment for the right tools and people, including data scientists.*
>
> **Helena Wood, Head of Public Policy and Strategic Engagement, Cifas**

Fraud profile:
The use of money mules

We can't talk about fraud without highlighting the role of money mules. Typically, vulnerable individuals are targeted as money mules, drawn in by scams such as jobs offering promising quick and easy money. Either knowingly or unknowingly, the money mules offer criminals access to their bank account to receive the proceeds of fraud, and quickly disperse receipts to other accounts, often in different countries. Money mules play a crucial role in cashing out the proceeds of fraud, and it is the ease with which they are doing so that creates a problem in tackling fraud.

Money Mules:

Connecting the dots

Combining data and information across different control areas can create a powerful and layered defence model.

Opening multiple accounts across a short timeframe, e.g one day, has been identified as one technique of OCGs in muling illicit funds. A typical profile shows a number of accounts being opened in one day all receiving the first transaction from the same counterparty. The accounts share the same identity features such as the same email format, registration IP and registration device. Connecting the data points obtained at onboarding alongside early transactional activity can help with early identification of potential mule accounts.

Identify, assess, mitigate... and repeat!

In addition to ethical motivations to mitigate the societal and human impact of fraud, firms have very clear drivers for improving fraud controls. There are direct financial losses (which will increase significantly in the UK with new reimbursement requirements), the impact of the loss of consumer trust and market share, and regulatory action. Through the implementation of targeted controls financial institutions will not only safeguard their assets and customers, but also bolster the foundational elements of trust and integrity.

Firms also need to recognise the natural tension that may exist between mitigating fraud and financial crime risks, and complying with other regulatory requirements and expectations, such as consumer duty. Thus, to ensure you are treating customers fairly and not inadvertently excluding certain profiles of customers, firms need to consider all their existing processes related to fraud - how models are built, how complaints are managed, the customer exit process, etc. It is crucial to balance managing the risks and financial liability against ensuring financial inclusion and mitigating against bias in fraud control frameworks.

Fraud detection is an ongoing process, and implementing controls is not a one-time effort. There will be no assurance that controls will address all risks across every fraud typology. There is no silver bullet or bolt-on fraud control that will solve all your fraud issues. *However*, continuous improvement is key to the success of fraud prevention. Firms should adopt an iterative approach, regularly reassessing and refining their strategies to stay ahead of emerging threats. This ongoing cycle will support a dynamic and adaptive fraud prevention framework. It’s as simple as:

1. Identifying potential areas of fraud risk across your customer journey.
2. Clearly defining your risk appetite and establishing the fraud risk levels your organisation is willing to accept.
3. Assessing if there are gaps or vulnerabilities in existing controls.
4. Deploying tactical and strategic solutions tailored to addressing specific issues.
5. And repeat, on an ongoing basis.

**Fraud does not stand still;
neither should your controls.**

About Resistant AI

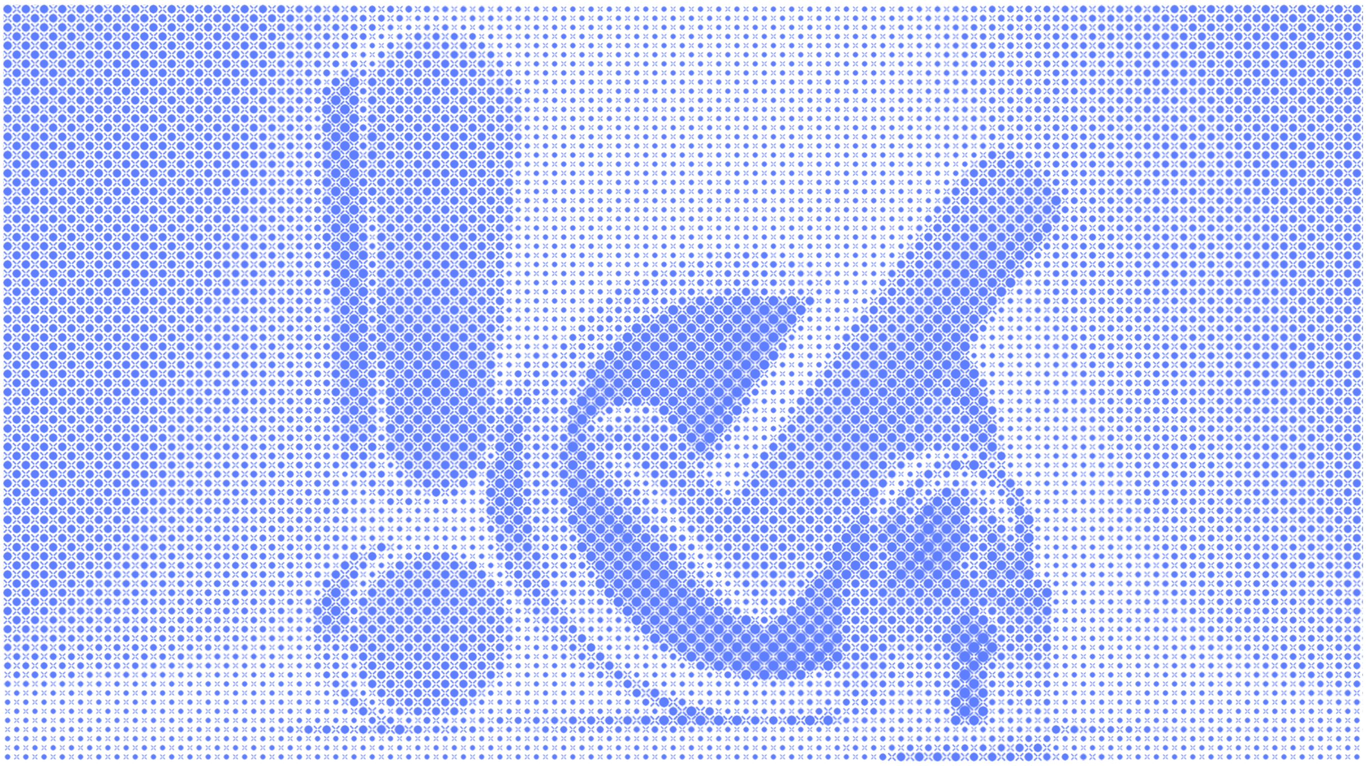
At Resistant AI, we've been using machine learning to hunt cybercriminals for over 16 years, and we've followed them into the field of financial crime. Our state-of-the-art machine-learning techniques make the AI and automation systems of financial services resilient to manipulation and attack. By analysing everything from submitted documents to ongoing customer behaviours, we uncover and prevent document forgery, serial fraud, synthetic identities, account takeovers, money laundering, and previously unknown financial threats that operate on a large scale. Backed by GV (formerly Google Ventures), Index Ventures, Credo Ventures, Seedcamp, Notion Capital and several angel investors specialising in financial technology and security, Resistant AI is headquartered in Prague with offices in London and New York. Our client roster includes Payoneer, Habito, Holvi and Finom.

Visit resistant.ai to learn more.

About 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 fraud programme to meet evolving regulatory requirements, use technology effectively, and stay competitive.

Visit fintrail.com to learn more.



resistant.ai

www.resistant.ai

Credo. G/ Index Ventures Seedcamp NOTION