Signals

Intelligence Behind the Fraud Patterns that Matter

SYNECTICS SOLUTIONS

Acknowledgements

Signals draws on insight from National SIRA along with partners and colleagues from across the fraud and financial crime community. We are grateful to the many practitioners and experts, both within Synectics and from the broader industry, who shared their perspectives, experience and challenge throughout its development.

In particular, we would like to thank Nick Maxwell, Katriona Cunningham, and Matt Gilham for their valuable input and enthusiasm to engage in discussion on the evolving fraud landscape.

Fraud is an increasingly complex challenge that no single organisation can address alone. Ongoing dialogue and collaboration across the industry are essential to improving how we understand and respond to emerging threats, both domestically and internationally.

We look forward to continuing to work collaboratively with partners across the industry and bringing the community together to better understand and combat fraud.

The changing conditions of fraud

Fraud has always evolved. What has changed is its **scale, persistence** and the way **exposure now compounds** across **markets and organisations**. It has become industrialised.

The underlying drivers remain familiar: incentives and the exploitation of weak points still shape activity. **The difference is the operating environment.**

Automation has lowered barriers to entry, reducing the need for specialist expertise. Synthetic identities have increased plausibility. Scams are more sophisticated across products and sectors. AI supports fabrication and testing at scale, and compromised identities circulate more widely and for longer.

These shifts are visible across connected datasets. The signals and data show activity is moving across sectors, escalating after application and increasingly moving beyond any single organisation's line of sight.

Our *Signals* report draws on National SIRA intelligence to examine and interpret those critical fraud patterns impacting financial services organisations.

Across five chapters, we explore how scaled, persistent fraud adaptation creates compounding exposure, and what that means for fraud leaders as risk ownership shifts across the fraud lifecycle.

Contents

Chapter 1: Cross-sector travel

22% of fraud an organisation encounters is already visible elsewhere. As adaptation unfolds in parallel across markets, position within an MO matters more than point of detection.

Chapter 2: Early warning signals

Nearly half of the most serious fraud is preceded by warning signals. Exposure stems not from failure to detect at entry, but from hesitation to act once credible signals build.

Chapter 3: Synthetics beyond application risk

Synthetic ID use in repeat offending has grown by 40%. What appears isolated at application stage is increasingly part of broader KYC challenge.

Chapter 4: Strategic deployment of fake documents

Fake documents have surged by 26%, driven by AI quality and distribution capabilities. More fraudsters deliberately fail controls to trigger fallback routes that rely on documents.

Chapter 5: The afterlife of an ID fraud victim

Two thirds of compromised identities are reused across products and sectors. Identity theft is now a lifecycle governance responsibility shaped by foreseeable harm.

Cross-sector fraud: familiar journeys, new conditions

01

Cross-sector fraud: familiar journeys, new conditions

Repeat offending is rising, and cross-sector fraud journeys now extend much further.

Fraudsters operate in parallel, deploying operations and MOs across multiple sectors, organisations and products. In this environment, understanding movement – and where you sit within a wider fraud journey – matters more than any single event.

22%

22% of fraudsters encountered by an organisation have been identified as fraud elsewhere.

50%

Half of motor finance fraud signals have associated intelligence from insurance.

75%

Investigations can complete 75% faster when using cross-sector risk intelligence.

1 in 4

25% of current account frauds have pre-existing risk indicators.

What the data tells us

Cross-sector targeting is not new. For decades, organised fraud has moved deliberately across industries, products and organisations, often originating in sectors where controls may be more relaxed before progressing toward higher-value targets.

Across connected National SIRA datasets, **22% of fraudulent actors encountered by a single organisation have been identified elsewhere. That figure rises when synthetic IDs are involved.**

This indicates that a significant proportion of fraud exposure sits within a shared pool of offenders actively operating across products and sectors rather than within one. In fact, when looking at a cross-section of these repeat offenders, activity was equally distributed across targeted sectors.

One environment is used to build credibility, another to extract value. Movement between them is deliberate and patterned.

Challenger or digital-first banks focused on growth and rapid customer onboarding can directly benefit from accessing the collective insight from established banks. One example highlighted that **25% of current account fraud had visible pre-existing indicators linked to money muling and synthetic identities.**

In motor finance, the visibility benefits are equally compelling. One business alone saved £millions in fraud losses in 12 months by leveraging fraud signals from insurance.

Almost 50% of fraud signals in motor finance have associated intelligence from the insurance sector.



The anatomy of a repeat offender

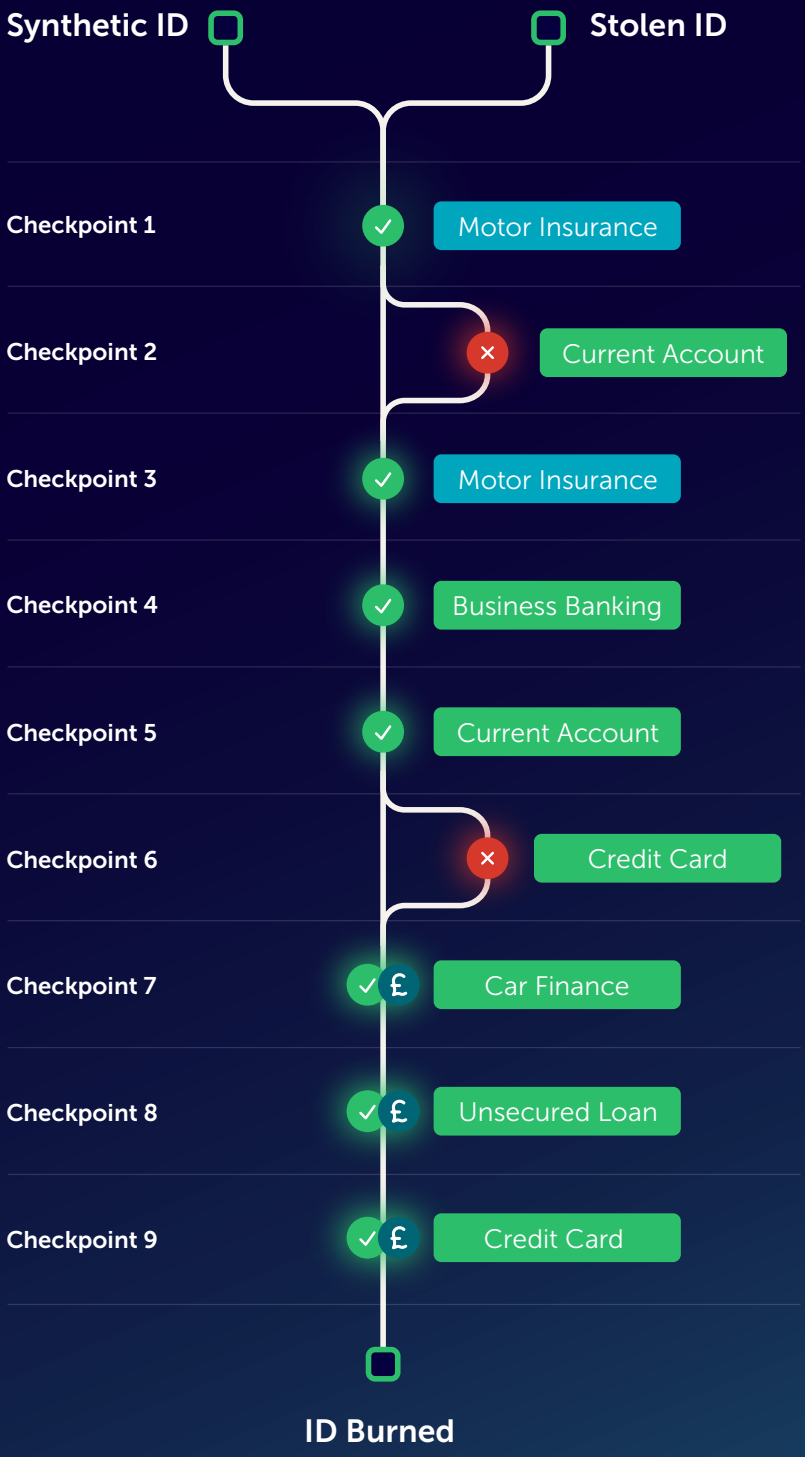
Over a 13-month period, a repeat offender targeted multiple providers across a range of products. Their activity appeared to build strategically* toward high-payout targets, such as business banking and loans.

Strategies making full use of cross-sector intelligence and proactive account monitoring would have detected this fraud earlier, before the identity was burned.

This repeat offending pathway involved 10 organisations, 8 products and 8 different fraud types.

Over 50% of activity was concentrated in Business Banking and Motor Insurance in equal proportions, with targeting becoming more selective in high-gain, credit-based products like unsecured lending and car finance. Impersonation and synthetics were the dominant fraud types, and were used in equal concentration.

- Insurance
- Finance
- Approval
- Decline



*Please see Methodology

Cross-sector intel as an efficiency unlock

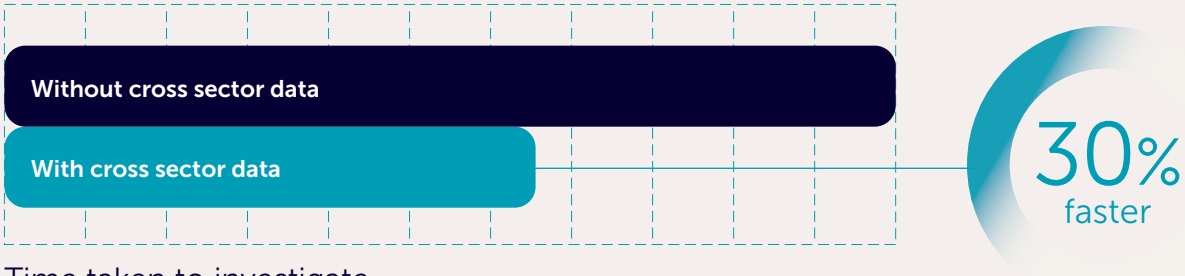
On average, fraud investigations complete **31% faster where cross-sector intelligence is applied** alongside an organisation's own data.



Shared intelligence improves efficiency as well as detection rates. The benefits are greatest for specific high loss cases, particularly in motor insurance, banking and lending.

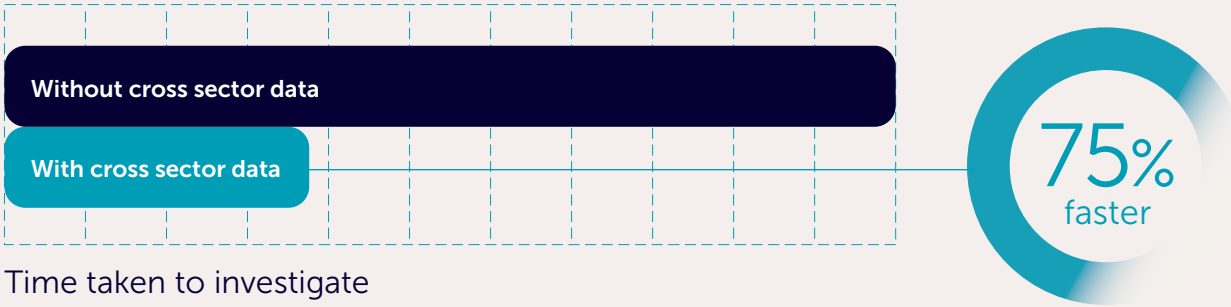
These contrasting timelines show a clear cost tied to over-reliance on siloed account or policy-based risk insights.

Motor insurance investigations



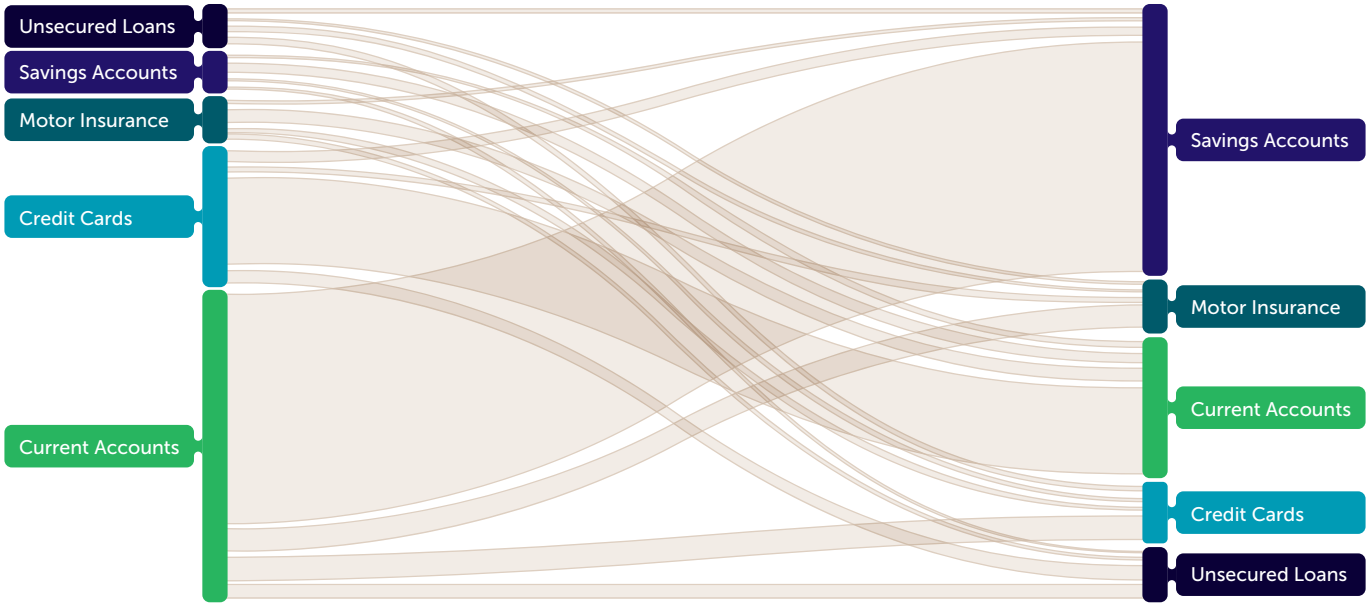
Time taken to investigate

Current account investigations



Time taken to investigate

Seeing movement rather than moments



Cross-sector analysis reveals progression patterns that are not visible within isolated organisational data.

Three features stand out:

01

Journeys run in parallel, not sequence.

Automation and synthetic identity construction means credibility can be built across multiple organisations at once.

02

More of the journey now sits outside any single sector view.

Finance and insurance increasingly represent the point at which impact becomes measurable, not where the journey begins.

03

Visibility at entry point is not a given.

By the time activity surfaces within high-value financial products, identities and actors may already be established across several organisations.

Why this matters now

Outcomes are shaped primarily by when fraud is recognised within the journey rather than where it ultimately crystallises. Fraudulent identities detected later in a lifecycle, having built credibility across multiple organisations, carry materially greater exposure.

When activity is assessed locally:

- Known patterns are re-investigated repeatedly
- Early losses are absorbed unnecessarily
- Actors look "new" when they are not

Where cross-sector intelligence is incorporated, organisations appear less frequently in structured repeat journeys and resolve risk faster.

In a connected economy, staying resilient depends on how quickly businesses track and respond to activity across different sectors. When one organisation identifies a fraudulent ID and notifies others, the entire network benefits.

> Working in isolation, different businesses in the private sector have just a small glimpse of the data relevant to detect and prevent fraud and scams affecting their customers and their enterprise. Fraudsters are highly networked and operate seamlessly across these information gaps to exploit weaknesses.
>
> In 2026, we see innovation around the world as different countries seek to grapple with this problem. New capabilities are emerging to support collaborative analytics to detect fraud risk across businesses and across sectors. Synectics is driving innovation in this field and supporting the Royal United Services Institute explore how these principles can apply at the cross-border level, with appropriate safeguards and data governance."
>
> **Nick J Maxwell,**
> **Head of Future of Financial Intelligence Sharing (FFIS)**

Market implications

The challenge is no longer whether fraud can be detected at the point of application. Modern controls already surface high volumes of risk.

The question is how organisations interpret and act on what they already see.

In an environment where fraud travels across sectors and products, isolated decision-making increasingly produces false confidence. Perceived strong internal controls can mask broader exposure, while fragmented intelligence allows repeat offenders to persist and adapt.

The organisations that perform best in this environment are those that learn faster where risk overlaps and intervene earlier as a result.

Fraud leader focus

Across our client network, we see the clearest reductions in repeat exposure amongst organisations that:

- Identify the earliest point at which a fraud typology can be detected
- Quantify the proportion of activity already visible elsewhere across connected datasets
- Incorporate cross-sector intelligence into decision-making before escalation
- Treat investigation-to-action time as a strategic metric rather than solely an operational KPI

02

UP NEXT...

Early signals and escalating exposure

Early signals and escalating exposure

02

Early signals and escalating exposure

44% of serious fraud is preceded by identifiable early warning signals.

This pattern unfolds at a time when more fraud is developing on the customer book, and demographics we once trusted become higher risk. These early warning signals create an opportunity to confidently intervene before fraud escalates.

36%

Over one in three money muling cases show warning signs at the point of application.

20%

The proportion of mules aged over 35 has grown by 20% in one year.

108

For the most serious frauds, suspicious activity begins 108 days before a confirmed crime.

52%

Over half of organised crime cases are flagged for suspicious behaviour first.

What the data tells us

The difference between pre- and post-onboarding is fundamental. At the point of application, the objective is prevention: determining whether risk should be admitted at all. Once a customer exists, that objective changes. The question is no longer whether risk should be permitted, but **how it should be treated**.

Resolving this question is an urgent one. Across National SIRA, we see 44% of frauds with **clear regulatory exposure preceded by identifiable early warning signals**. The timing is equally significant. On average, there are **108 days between first suspicious signal and confirmed serious fraud.**

Over 1 in 3 confirmed money muling cases are preceded by observed suspicious behaviour. The situation is more severe still in organised crime, where early warning signals are present in 52% of cases.

At the same time, suspected mule filings are falling, even as suspicious facility use rises. This disparity points to a **growing classification hesitation** rather than declining activity. Signals are being seen – but maybe not always confidently interpreted.

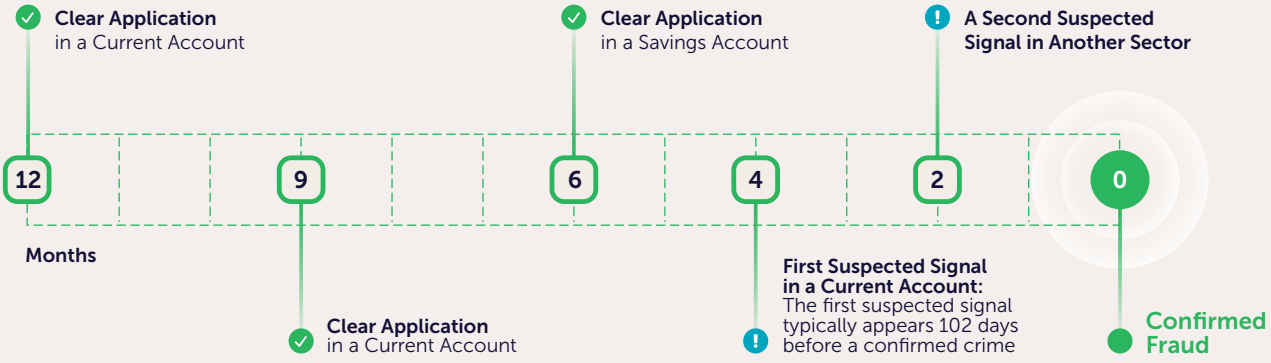
Profile shifts reinforce the pattern. The **proportion of "older mules" (individuals over 35) has increased by around 20%** year-on-year. As application checks have become more stringent, fraudsters are targeting a different demographic; people who already have accounts and a trusted reputation.

44% of serious fraud is preceded by identifiable early warning signals.



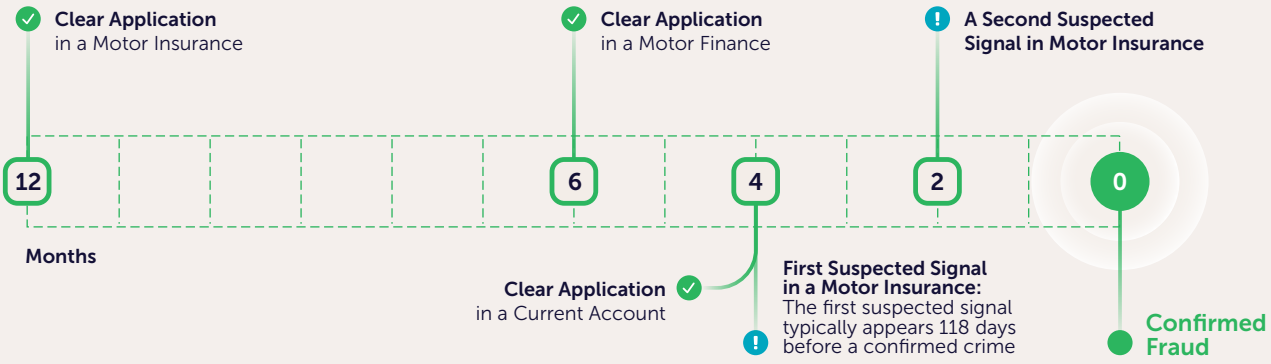
The money mule early warning timeline

The money mule early warning timeline shows that **36% of cases are flagged for suspicious behaviour, on average 102 days** before a report of confirmed fraud is made. Throughout a 12-month period, an individual typically makes genuine applications for various products* across different providers.



The organised crime early warning timeline

The OCG early warning timeline shows that **52% of cases are flagged for suspicious behaviour, on average 118 days** before a report of confirmed fraud is made. Throughout a 12-month period, the individual typically makes genuine applications for various products* across different providers.

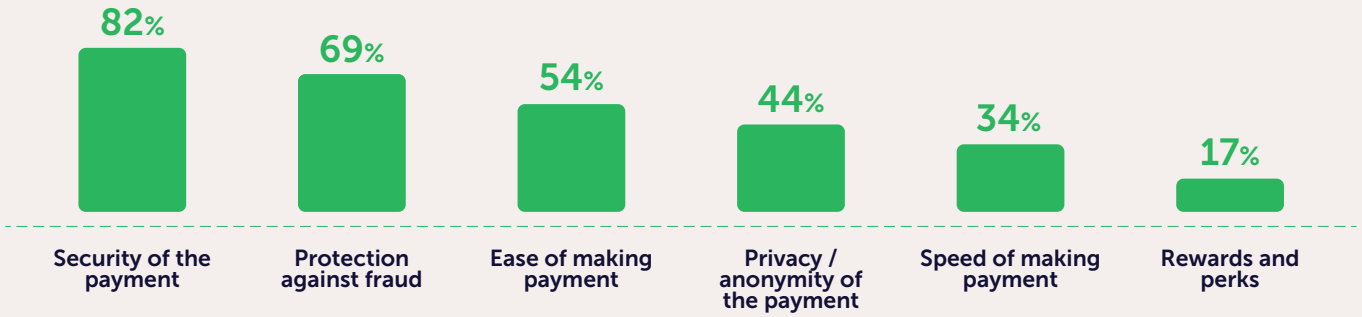


*Please see Methodology

Friction reframed

Concern over customer experience has historically limited earlier intervention. However, Payment Systems Regulator (PSR) research indicates that increasingly fraud protection and security are among the highest priorities for consumers.

Important factors when making payments (all UK adults)



Consumers demonstrate willingness to accept additional checks when framed as protective (ie. their data secured and their money protected) rather than obstructive. The barrier lies in how and when friction is applied.

Early warning signals, when interpreted in context, create an opportunity for proportionate intervention that protects both customer and organisation.

Used precisely, friction might now become a trust-strengthening measure rather than a growth constraint.

Attitude to banking and fraud

"I am happy to accept slight delays in my payments if it means they are secure and I am protected from fraud"



Why this matters now

As fraud adapts at scale, escalation increasingly unfolds across on-book customers.

Signals that once appeared isolated or low-severity should inform account-level controls to mitigate serious fraud typologies.

In this environment, timing determines impact. An identity or account identified later in its lifecycle, after credibility has been built or limits increased, carries materially greater exposure.

The regulatory lens has also evolved.

Under the FCA's Consumer Duty framework, firms are expected to prevent foreseeable harm and consider lifecycle outcomes. Where credible early warning signals exist and are not embedded into account-level monitoring, exposure may increasingly be interpreted as foreseeable rather than unavoidable.

Market implications

Fraud prevention has reached an inflection point.

When up to 44% of cases are preceded by visible signals, exposure increasingly stems from hesitation to intervene – or uncertainty about how to do so proportionately – rather than from the absence of detection.

This shifts emphasis from decision to treatment. **Lifecycle monitoring must gain parity with onboarding controls.**

Classification also becomes more complex. It is becoming harder to tell who is an unwitting victim versus a complicit actor. Stronger cross-product and cross-organisation context will increasingly support confident, defensible intervention.

Fraud leader focus

We're seeing proactive strategies begin to reduce on-book risk, particularly where our clients are:

- Identifying which fraud types are most consistently preceded by early warning signals
- Measuring the time between first suspicion and confirmed fraud as an exposure indicator
- Implementing event-driven monitoring where patterns emerge
- Embedding point of application insights and continuous account monitoring controls into ongoing decisioning

Reimbursement changed who pays. Let's change who wins



Chris Lewis, Director,
Strategic Solutions & Analytics

APP reimbursement may have changed who pays, but not yet who profits.

Mandatory APP reimbursement went live in October 2024, introducing an £85,000 cap and a 50:50 liability split between sending and receiving PSPs.

Victims are now reimbursed in most cases, ending the long-standing imbalance where individuals carried the financial cost of scams.

For a crime that strips not only savings but confidence and dignity, shifting the burden away from victims is a clear policy success.

But policy changes do not alter the incentives behind the crime itself.

Fraud is shifting toward higher-value scams

H1 2025 saw APP losses reach £257.5m, up 12% year-on-year. Case volumes fell by 8%, yet total losses increased.

That shift suggests a change in strategy. Fraudsters are increasingly prioritising higher-yield typologies that deliver larger returns from fewer victims.

Investment scams illustrate this pattern. They typically involve larger transfers and longer engagement, with fraudsters building credibility over weeks or months before funds move. This is often tied into government rhetoric regarding investment into the UK, further building credibility for the fraudsters.

The Home Office Fraud Strategy clearly identifies scams as the primary fraud use case from a prevention perspective, and the Online Crime Centre brings some much-needed investment to the table to disrupt perpetrators. However, this will not solve the issue overnight.

Why payment controls alone are not enough

Social engineering continues to circumvent payment controls. Victims are groomed through convincing narratives, often supported by cloned websites, impersonation and sustained digital contact.

By the time payment occurs, the deception is already embedded. The transaction itself can appear entirely legitimate because it aligns with the story the victim has been persuaded to believe.

In these circumstances, transaction-level friction alone is unlikely to stop the most damaging scams. Warnings or prompts may interrupt opportunistic fraud, but where trust has been carefully engineered the payment often appears routine.

As a result, many institutions are shifting focus from single-payment intervention toward broader contextual intelligence: understanding relationships between accounts, behavioural patterns and network connections that indicate fraud already in motion.

What we find when we follow the money

Reimbursement does not remove the profit motive for fraudsters. If funds can still be extracted and routed through intermediary accounts, the criminal economics remain intact.

Fraud does not occur in the payment itself. It occurs through people using accounts to receive, move and monetise stolen funds. The decisive control point is therefore not only the outbound transaction, but the receiving and relaying accounts that enable proceeds to move across the system.

Follow the money and the structure of scams becomes clearer.

Money mules remain the central infrastructure of APP fraud. FCA data consistently shows them as the primary recipients of scam proceeds.

National SIRA analysis indicates mule activity rising across multiple products:

- 25% in current accounts
- 12% in savings accounts
- 23% in credit cards

The pattern reflects deliberate displacement. Fraudsters move funds through whatever products allow the easiest receipt and onward transmission. This is continuing to diversify into new product types such as asset finance and non-traditional banking products.

For institutions with tech stacks organised around product silos, this creates structural exposure. When onboarding data, transaction monitoring and product systems operate independently, signals remain fragmented and intervention becomes partial.

What effective intervention looks like

Reducing scam losses requires institutions to intervene earlier and across the full customer relationship. Three priorities stand out:

1. **Treat mule detection as a core scam control.**

   Mule accounts are the monetisation layer of fraud. If that layer remains intact, scam economics remain viable.

2. **Monitor risk continuously, not just at onboarding.**

   Customers can become mule accounts after they are opened. Behavioural shifts, network connections and unusual transaction patterns often signal that change.

3. **Coordinate controls across products.**

   Fraudsters already operate across product boundaries. Effective prevention requires the same coordination on the defensive side, so signals from one product inform decisions in another.

This does not require blanket friction or intrusive controls. Targeted intervention, applied when behaviour shifts and funds begin to move, is far more effective.

The next phase of APP scam prevention

Reimbursement has corrected an important imbalance. Victims are no longer left to absorb the losses alone.

The next phase of APP strategy is not about who pays, but whether fraud continues to pay at all.

03

UP NEXT...

Synthetics: beyond application risk

Synthetics: beyond application risk

03

Synthetics: beyond application risk

The volume of synthetic IDs in repeat offending has surged. This means that one in three of all synthetic IDs are now linked to repeat fraud.

As AI tooling, public data theft and siloed onboarding checks lower the barriers to creating, testing and reusing synthetics, risk increasingly compounds beyond onboarding. The speed of growth – up to 152% in some products in a single year – is proof of how quickly synthetics move once in the system.

350k

There are 350,000 distinct synthetic ID signals in National SIRA. The number of synthetics has grown 50% in 2 years.

1 in 3

One third of synthetic IDs are now linked to repeat offending.

40%

The volume of synthetic IDs used repeatedly has grown 40% in one year.

50%

50% of all identity fraud in National SIRA is synthetic IDs. The other half is impersonation.

What the data tells us

Synthetic identity fraud is a **persistent and growing threat,** no longer confined to the moment of application.

AI-enabled tooling, combined with public data exploitation and siloed onboarding systems, has lowered the barrier to constructing credible synthetic identities. Fraudsters will make small tweaks, resubmit and refine to test – and they are now able to do so at scale.

Within National SIRA, one in three synthetic identities are now linked to repeat offending. They increasingly act as the engine powering broader fraud strategies, particularly as ramps and bridges into serious crime.

More concerningly still, we see that nearly one in five stolen identities repeatedly used for crime ends up embedded in a synthetic identity. Offenders often switch between fully artificial or impersonated identities depending on what works within current controls – raising new challenges around victim classification, duty of care and foreseeable harm.

It's clear that synthetic identities are not always short-lived. The networked effect of local intelligence is undermined when synthetics are present in the ecosystem.

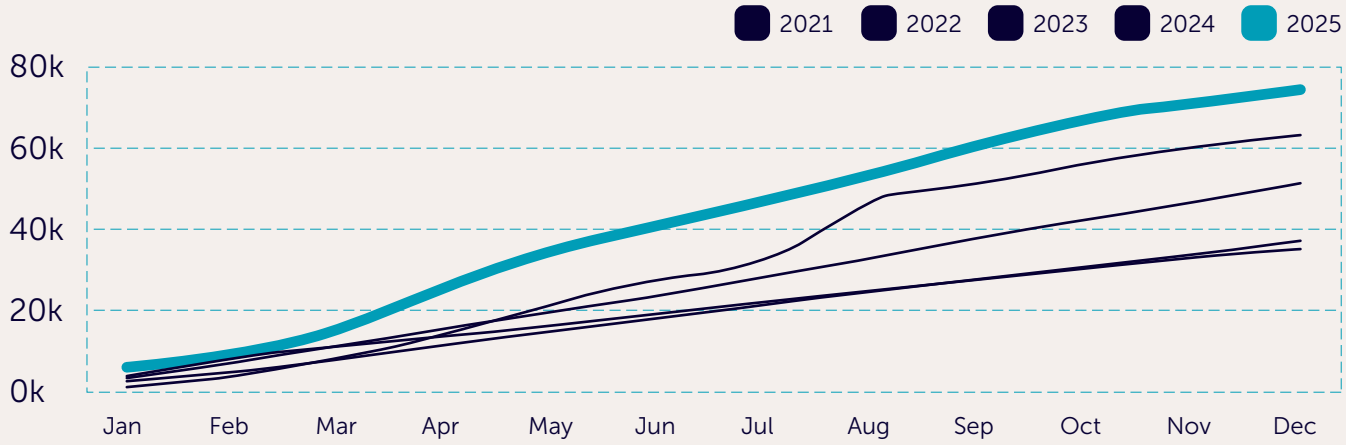
The volume of synthetic IDs used repeatedly has surged by 40% in one year.



A multi-year acceleration in automated fraud

The five-year trajectory of synthetic ID fraud reveals a relentless, compounding growth pattern that mirrors the scale of automated, AI-enabled threats.

Rather than seasonal fluctuations, the data shows a consistent month-on-month increase every year, with volumes **surging by as much as 152% in specific product lines** and showing no sign of plateauing. This upward trend has **propelled synthetics to a 50% share of all identity fraud** reports in National SIRA.



Synthetics and a growing KYC crisis

Research by The Payments Association describes synthetics as the driver behind a seismic shift in how fraud is executed. This evolution is unlike anything previously experienced in financial services. It threatens the very foundations of KYC and, consequently, the future integrity of customer portfolios.

Concerns and challenges related to synthetic ID fraud



Why this matters now

Ultimately, when synthetic identities are approved and remain undetected, exposure is compounded inside the portfolio. Synthetics begin to shape the environment around them as they build transaction history and interact with products.

A growing synthetic presence inside the book increases the likelihood of downstream default, bust-out activity, chargeback abuse or laundering exposure. It also increases investigative workload as repeat offending then surfaces across products.

These consequences highlight why we must share data on the volume, type, and quality of synthetics, alongside the multi-sector MOs they employ. Without this collaboration, stalling their trajectory becomes significantly more difficult.

> Sharing data for the collective fight against fraud is pragmatic and sensible, but faces entrenched resistance operationally and strategically.
>
> We need to overcome the enduring paradox in collaborative data sharing. Organisations recognise the need for data sharing to better identify and tackle organised fraud. This is increasingly supported by government drive for public-private data sharing. But at the same time, barriers exist though the operational challenge in realising financial benefits from cross-sector sharing (e.g. would a bank treat intelligence from an insurer as truly actionable) and also more strategically in how to empower an accountable body to collect, analyse and action scale combined intelligence."
>
> **Matt Gilham,**
> **Director of Whitelk Consulting**

Market implications

Unless synthetic density inside on book customers is measured and actively managed, exposure compounds invisibly until it reappears either as loss or reputational damage.

Synthetic fraud, left untreated, becomes embedded risk. It is not simply a typology, rather a persistent, adaptive layer or network within organised fraud.

If it is treated as isolated noise, it will continue to drive repeat exposure.

Fraud leader focus

Within our client community, we see synthetic ID risk being effectively controlled when organisations are:

- ☐ Reviewing onboarding journeys to identify any silos
- ☐ Considering back-book screening to qualify exposure
- ☐ Identifying repeat offending patterns linked to synthetic identities
- ☐ Integrating public sector intelligence into identity decisioning strategies
- ☐ Moving from individual checks toward network-level analysis of identity

04 UP NEXT...
Strategic deployment of document fraud

Strategic deployment of document fraud

04

Strategic deployment of document fraud

Document fraud has risen in products where financial gain is greatest. AI is compounding this growth, and increasing the frequency and speed of document fraud attacks.

Detecting forgeries is more difficult, attack scale is increasing, and fraudsters are deliberately failing checks to trigger fallback journeys that depend on document verification.

As a result, far more pressure is being placed on document review processes and wider evidence capture. In this environment, understanding the document fraud risk associated with a particular customer pathway has become increasingly important.

12%

12% more fake documents are being reported at policy stage.

26%

Document fraud has risen by up to 26% in the highest-risk financial products.

68%

Suspected fabricated claims have risen by a staggering 68% in motor insurance.

9%

False statements made to motor insurers at policy stage are up 9%.

What the data tells us

AI is not changing what fraud is, and fake documents are not new. What has changed is the **scale, plausibility and strategic deployment** of document fraud within journeys.

Across National SIRA, document fraud reports are rising, particularly in insurance claims and unsecured lending – environments where financial reward is greatest.

In parallel, **fabricated claims have increased by up to 68%**, concentrated in the same product categories.

Lower-level manipulation remains present. **False statements and non-disclosure at policy stage are up 9%**, indicating that AI is not replacing simpler tactics. Manual document editing and the use of commerical, off-the-shelf editing software is still highly prevalent across false document filings.

This pattern is also consistent with volume testing – repeated submission to identify which thresholds are passable.

Policy-stage document use has increased by 12%, demonstrating earlier deployment in journeys rather than confinement to terminal loss events.

Taken together, the data shows both a strategic and technological leap. AI reduces the cost of fabrication. Scale increases the frequency of deployment. Fraudsters deliberately target fallback journeys that rely on manual intervention.

Document fraud has risen by up to 26% in the highest-risk products.



The “fail on purpose” pattern

Digital ID&V controls across all financial services have strengthened significantly. In response, fraudsters are increasingly failing verification processes deliberately.

Once failed, fallback pathways are triggered that rely more heavily on document-based verification. AI-generated documents then enable those fallback routes to be passed with increasing plausibility.

The data showing a sharp rise in failed validations reflects increased detection and volume-testing behaviour; as creation costs fall, experimentation becomes easier to conduct at scale, and controls are studied as well as challenged.

Historically, document fraud was concentrated at high-loss points, particularly claims. That concentration has changed. They are now appearing earlier in the journey, at policy inception stages, while instances continue to surge at high loss points.

In insurance particularly, fabricated claims are rising in parallel with fake documents. But they are increasingly part of multi-step activity rather than isolated events – with documents used to justify a claim and sustain credibility.

Sequencing now commonly follows this pattern:

- Low-friction manipulation first
- Fabricated documentation introduced when challenged
- Escalation within already established credibility

AI improves plausibility and persistence, with documents embedded across the lifecycle rather than appearing only at the end.

Is document fraud becoming an early-stage tactic?

An emerging insurance MO* shows fake documents introduced earlier and combined with other fraud techniques – an approach that transfers beyond insurance.



Even when the above pattern is understood, operational handling may significantly impact how accurately a document is interpreted.

Metadata loss as files move between systems, authenticity checks conducted in isolation from behavioural context, and separation between document review and broader fraud intelligence can all weaken interpretation.

In some categories, high proportions of "suspected" rather than "confirmed" document fraud reports demonstrate increasing difficulty in confidently detecting false documentation.

*Please see Methodology

Why this matters now

Document fraud is no longer solely a forgery problem. As scale increases and plausibility improves, document verification and validation will not act as a silver bullet.

The risk lies in forgery quality and siloed fraud controls for document review. Where documents are assessed as standalone artefacts, organisations may validate authenticity while missing the role documentation plays within a wider fraud MO.

As false document deployment becomes easier to test and refine at scale, the strategic exposure increasingly lies in **when and where documentation appears within a journey**, not simply whether it passes technical checks.

Market implications

As plausibility improves, it is becoming harder to identify false document signals when interpreted in isolation.

Across sectors, organisations are increasingly pairing document analysis with behavioural signals, identity history and cross-product intelligence to understand how documentation fits within an activity pattern.

In this environment, document fraud functions less as a discrete typology and more as supporting infrastructure within the broader fraud control environment.

Fraud leader focus

From working closely with leaders with more mature document fraud strategies, **we see the clearest reductions in document-driven exposure when approaches:**

- ☐ Review whether fallback and manual verification routes are governed with the same rigour as primary digital pathways
- ☐ Evaluate whether document review functions are structurally integrated with behavioural and cross-product intelligence
- ☐ Prioritise automating document classification to detect high fraud risk documents at scale
- ☐ Ensure operational handling preserves contextual metadata when using document forensics tools

Controlled-friction returns in the fight against organised fraud



Osman Khurshid, Chief Client Officer

For the past decade, financial services organisations have focused on reducing friction within customer journeys. Opening an account, setting up insurance or accessing credit now happens in minutes – progress the industry is determined to protect.

But across financial services, the conversation around friction has recently become more nuanced.

As risk across the market landscape increases, such as with scams, consumers are demonstrating a growing willingness to accept friction in the onboarding journey when it provides greater protection against potential threats.

Whilst the primary focus remains onboarding customers as effectively as possible, an increasing number of leaders are talking about this in terms of proportionality. Where friction should sit, when it should appear and what purpose it should serve. Many refer to this balance as "friction-right".

What sits behind that shift is a change in how fraud operates. As digital services have accelerated, so has the sophistication of fraud attempts – testing fraud controls and penetrating any perceived gaps.

In these conditions, controlled friction is becoming more present and deliberate within digital journeys. Not to slow customers down, but to shield them – and our businesses – from the harms of organised and automated frauds.

Organised and automated fraud vs the ecosystem

We're seeing more fraud move in parallel across sectors rather than remain contained within a single product or institution. The criminal aim is to blur boundaries and establish credibility before the main event.

Synthetic identity fraud illustrates this pattern clearly. Our latest research found that one in three synthetic identities are linked to repeat offending. At least 22% of these serial fraudsters target multiple sectors as they attempt to establish a credible persona that can circulate more widely.

This plays out regularly across National SIRA shared intelligence. In some cases, fraudsters who've exhausted robust banking controls pivot into insurance products, where onboarding checks may differ – potentially offering less resistance. We observed that over 50% of fraudsters within the motor finance sector have links to other sectors, including insurance, underlining the growing trend of fraudsters targeting multiple industries rather than operating in isolation. This proving-ground activity has surfaced as hundreds of cross-sector fraud attempts from a single individual.

Interrupting the repeated testing that organised fraud relies on is one reason friction is returning to digital journeys. But it's not the only force driving that shift.

Regulators and consumers join forces

Public awareness of fraud is far higher than it was a decade ago. Campaigns such as Take Five, alongside regular media coverage of scams, have increased vigilance among consumers. As a result, many are more accepting – and sometimes welcoming – of additional verification steps when the purpose is protection.

Regulation is taking the same direction of travel. Consumer Duty places greater emphasis on demonstrable behaviour to protect your customers.

Together these developments are creating the conditions for organisations to address risk earlier and more confidently.

Signals identified during onboarding or application stages are therefore increasingly shaping the journey from that point onwards, by influencing how relationships are managed across the customer lifecycle.

That shift is bringing renewed attention to how friction appears within digital journeys.

Applying friction with intent

Against this backdrop, organisations are looking carefully at how verification appears within digital journeys – and four themes consistently emerge:

1 **Journeys shaped around risk signals**

Across our client base, leaders are clear that the good customer journey must remain central while fraud controls continue to evolve. The focus is increasingly on defensible, intelligence-led friction. Introducing additional automated checks only where the evidence supports them, such as fraud indicators that cause concern. Investigations remain the exception.

2 **Controlled-friction evolving alongside fraud**

Fraud patterns evolve quickly, particularly where organised activity is involved. Organisations are therefore reviewing digital journeys more regularly, examining where customers exit a process, which checks surface meaningful risk and whether existing controls still reflect current fraud behaviour.

3 **Technology supporting verification**

Much of AI's current value lies in improving the mechanics of verification. Automated checks can be completed faster, manual investigation workloads reduced and communication with customers improved when additional steps are required. In some environments, AI is already helping interrupt scams while they are underway.

4 **Wider intelligence guiding where friction belongs**

Where organisations have access to wider intelligence – for example through shared industry insight – it becomes easier to apply tailored friction with confidence. When identities, devices or behaviours are known elsewhere, necessary checks can appear earlier and more precisely within the journey.

Financial services organisations will rightly continue to prioritise speed and accessibility within digital services. The aim is certainly not to reverse the progress made in customer experience.

Instead, organisations are becoming more deliberate about where friction belongs.

Applied carefully, friction protects genuine customers while disrupting the repeated testing that organised fraud increasingly relies upon. By interrupting that cycle, we preserve the speed customers expect while making the economics of organised fraud far harder to sustain.

05 UP NEXT...

Identity afterlife: incident risk to governance responsibility

Identity afterlife: incident risk to governance responsibility

05

Identity afterlife: incident risk to governance responsibility

Compromised IDs are persistently reused across the financial ecosystem, and 19% of those are now linked to synthetic identity construction.

These figures underscore the scale of harm that accumulates when responsibility is assessed in isolation rather than across the lifecycle. This "identity afterlife" reflects risk that persists long after onboarding – and recognising it is the first step to interrupting harm that affects customers, businesses and regulatory duty alike.

1 in 5

19% of stolen IDs that are reused are linked to synthetic IDs.

90 days

Most compromised victim identities remain active for at least 90 days.

66%

Up to two thirds of ID fraud victims have their identity reused across the financial ecosystem.

93%

93% more victims of ghost broking were reported in 2025.

What the data tells us

Misclassification of identity fraud victims is increasing regulatory scrutiny and impacting good customer experiences. This is leading to higher costs and lower onboarding rates, whilst negatively impacting vulnerable customers.

Across financial services, stolen identities circulate across multiple sectors, products and organisations long after initial detection.

National SIRA intelligence shows that **21% of compromised identities are reused**. In certain typologies, **associated reuse rates rise to 66%.**

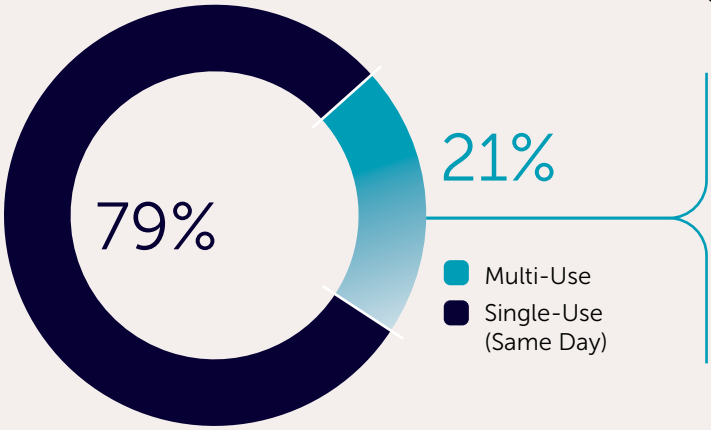
Approximately 19% of multi-use identities are also linked to synthetic identity construction, indicating that legitimate credentials are increasingly stitched into engineered personas.

Most reused victim identities remain active for **more than 90 days,** becoming a long-running source of collective risk as multiple organisations review the same underlying identity at different points in time.

As a result, harm accumulates for the same individual whose victim risk continues to be assessed in isolation rather than across the lifecycle of that identity.

Single strike or serial use?

While 79% of identities are used just once, **over 1 in 5 are reused**, opening the door to longer exploitation.



The lifespan of a multi-use victim identity

Of those that are reused, **many remain active for 30, 60, or even 90+ days**, offering repeated opportunity for abuse.

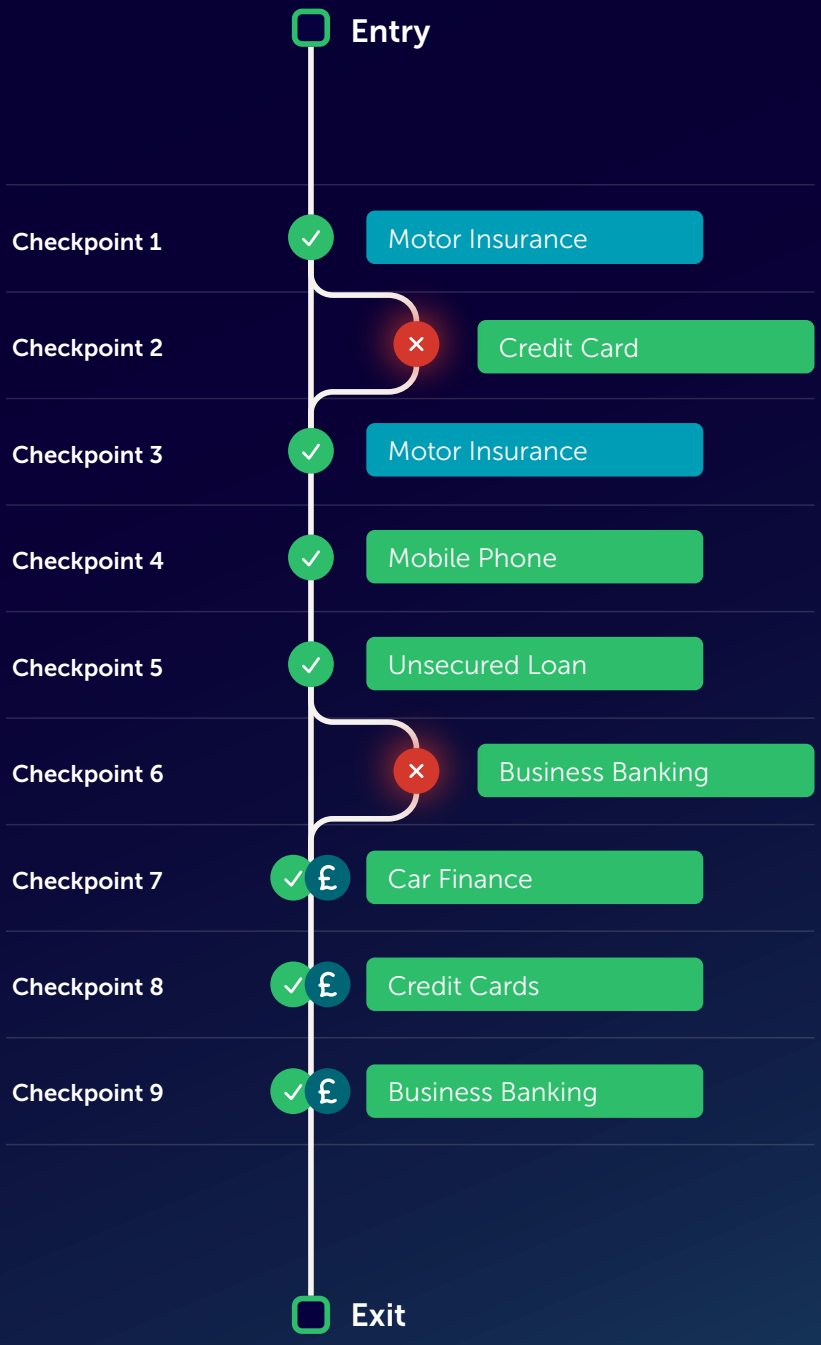


The victim hijack journey

In one observed case, a single stolen identity was used **10 times**, across **7 products**, involving **8 organisations**, spanning **4 sectors**.

Throughout this period, the legitimate individual continued normal financial activity, presumably unaware that a criminal double was operating in parallel*.

- Insurance
- Finance
- Approval
- Decline



*Please see Methodology

Ghost broking drives up victim reuse rates

Identity reuse risk is not evenly distributed. This is clearest in ghost broking, where **victim volumes have risen by 93% year-on-year**.

Demographic clustering – **predominantly male victims, aged 50–65**, often in lower-premium postcodes – demonstrates deliberate targeting.

Compare the reuse rate of compromised IDs associated with ghost broking – 66% vs the 19% average for fraud in general – and it is clear that ghost broking functions as a powerful identity harvesting mechanism.

When this fraud type is involved, it's increasingly likely that what appears as a contained insurance offence may signal significant exploitation.

Ghost broking victims have risen by

93%

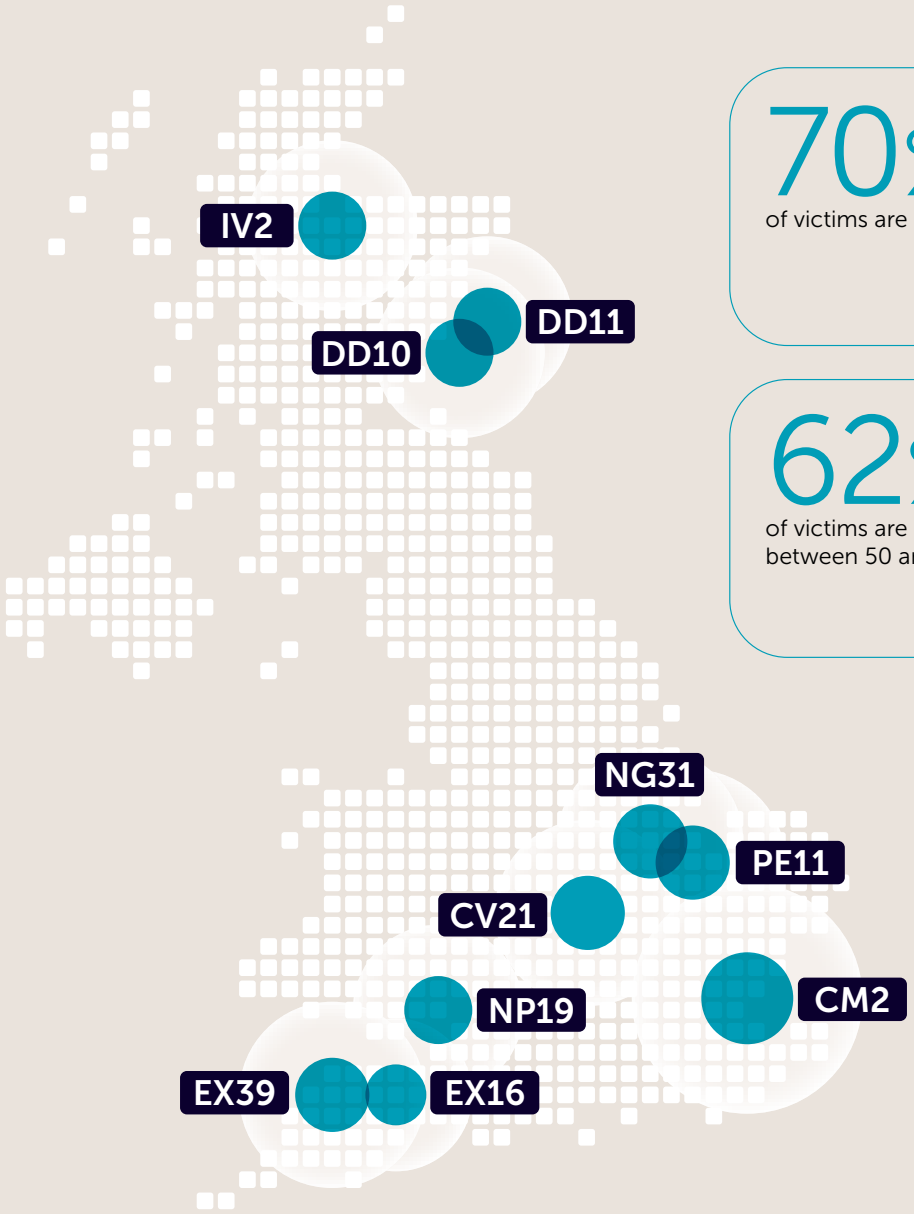
in one year

66%

of stolen IDs linked to ghost broking are re-used

Typical victim postcodes align with

low premium areas



70%

of victims are males

62%

of victims are aged between 50 and 65

"Where you buy your car insurance matters. We're increasingly seeing young drivers targeted on social media by ghost brokers who sell policies that don't exist, leaving people unknowingly uninsured. But the risk doesn't stop there. In consumer research commissioned by Aviva, we found one in six young drivers who bought insurance from someone on social media also had their identity stolen, exposing them not only to the risks of driving without valid cover but also to the wider financial and personal consequences of identity fraud.

As a responsible insurer, we believe we have a duty to truly know and protect our customers – and their data. That means using strong checks, trusted partnerships and real oversight to keep fraudsters off our books and help ensure our customers aren't exploited. Those selling bogus insurance online offer none of these safeguards, which is why our focus remains firmly on protecting customers from fraud and helping them stay safe."

Katriona Cunningham,
Underwriting Fraud Lead at Aviva

Why this matters now

Identity risk now sits at the intersection of fraud prevention, customer protection and regulatory duty.

Under the FCA's Consumer Duty framework, firms are expected to prevent foreseeable harm and consider lifecycle outcomes. When identity reuse is persistent and cross-sector, the governance question sharpens: **is identity theft being treated as an operational incident, or as a lifecycle risk?**

Victims are not abstract entities. They are customers whose financial lives may be disrupted repeatedly across institutions. When misuse of their identity is assessed at incident level, these victims may be misclassified as participants and repeat use goes unrecognised.

> Growing concerns over impersonation and how victims are classified has led to increased pressure from regulators.
>
> This offers an opportunity for organisations to reflect on their filing processes. Ensuring that victims – whether identified during onboarding or later in the customer lifecycle – are supported by safeguards that can help prevent repeat attacks.
>
> Integrating shared data into broader decision making is an important step in protecting individuals while identifying those truly responsible for identity theft.
>
> Ultimately, aligning these practices should support onboarding growth rates while demonstrating the clearest possible Consumer Duty commitment."
>
> **Jordan Roberts,**
> **Solutions Consultant at Synectics**

Market implications

Where identity reuse is visible across markets, organisations can no longer treat misuse as isolated or complete at the point of internal resolution.

Consumer Duty heightens scrutiny of foreseeable harm, classification decisions and the ongoing treatment of compromised customers.

This places greater emphasis on **identity-level visibility across time**, not only event-level detection. Risk persists beyond onboarding controls, and recognising that shift is the first step toward interrupting cumulative harm.

Fraud leader focus

Within organisations leveraging identity-level intelligence, stronger resilience emerges when teams:

- Take steps to classify victims and perpetrators separately to ensure fair, appropriate treatment for compromised individuals
- Strengthen cross-organisation intelligence sharing and classification clarity
- Develop processes to recognise and interrupt identity circulation rather than simply block events
- Treat identity compromise as a lifecycle governance issue as well as a fraud incident

UP NEXT...

Closing thoughts & methodology

The power of collective defence

Fraud has always adapted.

What has changed is the scale, persistence and sophistication with which these techniques are used to avoid organisational controls. Taken together, these conditions allow exposure to compound more quickly when signals remain isolated across organisations and markets.

Value lies less in individual statistics than in what they indicate about direction of travel: increasingly connected risk, more complex fraud journeys and the growing challenges of accurate interpretation.

For Synectics and the National SIRA community, the intelligence presented in *Signals* forms part of a continuous process of testing, interrogation and collaboration. New data is assessed, hypotheses challenged and emerging risks explored to understand not only what is happening now, but what is likely to follow.

This work exists to provide leaders across financial services and the public sector with something increasingly essential: clear, collective understanding of risk as it evolves.

By bringing together intelligence from across sectors and applying it with rigour, context and independence, we aim to ensure organisations can act earlier, respond proportionately and make fully informed decisions in a rapidly changing landscape.

As fraud and financial crime continue to adapt, so too will the intelligence and collaboration required to counter them. Our commitment – to clarity, context and collective defence – remains constant.

Methodology

The intelligence, insights, viewpoints and recommendations presented in *Signals* are developed from a combination of quantitative analysis and qualitative operational insight.

Data sources

Quantitative sources
Quantitative analysis is primarily drawn from National SIRA intelligence and from proof of concept studies conducted using National SIRA data. These datasets provide observed records of confirmed, suspected, victim and clear risk activity across participating organisations and sectors.

Qualitative sources
Qualitative insight is drawn from subject matter experts within Synectics and from operational intelligence shared through collaboration with Synectics' clients and partners. This includes frontline investigative, strategic and risk-management perspectives used to interpret quantitative findings and assess practical implications.

Use of National SIRA intelligence

National SIRA intelligence is used within *Signals* to test and answer key hypotheses in two principal ways:

- Time-period comparison: examining change over defined periods to identify shifts in behaviour, exposure and typology.
- Targeted data exploration: analysing specific patterns, journeys or behaviours using either the full aggregated dataset or defined segments and batches, depending on the hypothesis under examination.

The report draws on a defined *Signals* dataset derived from National SIRA intelligence. This dataset has been prepared specifically for research and strategic analysis.

Data credibility and quality

All data used has been subject to credibility and quality assurance processes. These include:

- removal or review of records assessed by subject matter experts as anomalous or unrepresentative
- application of minimum-volume thresholds to support statistical reliability
- validation against known operational patterns and market context

These steps are intended to ensure that analysis presented is representative of the markets to which it relates and delivers the greatest strategic value to readers. For this reason, some sectors in which Synectics operates are not included where available data does not meet the thresholds required for inclusion in a national-level analysis.

Interpretation and presentation

All written statistics – including volume figures, percentages and ratios – reflect directly observed analysis from the *Signals* National SIRA dataset and associated research. These figures are presented as recorded and interpreted within the methodology described above.

Given the scale and complexity of underlying datasets, raw data cannot always be presented in its original form without reducing clarity. Creative visualisations are therefore used to support interpretation and accessibility.

Visual representations in *Signals* fall into three categories:

1. Observed statistics: directly measured and presented as recorded.
2. Aggregated or derived visuals: simplified representations drawn from multiple observed records to demonstrate typical patterns, pathways or relationships.
3. Illustrative visuals: in a small number of cases, where specific data cannot be shared or visualised directly, illustrative elements are used to show how patterns are likely to operate in practice. All accompanying figures, statistics, products, fraud types and volumes are as observed in National SIRA (1). Visuals that feature illustrative elements are clearly marked with a (*)

This approach is intended to balance analytical accuracy with clarity, ensuring that complex intelligence can be understood and applied in strategic decision making.

About the dataset: National SIRA

National SIRA is the UK's largest cross-sector consortium of confirmed, suspected, victim and clear risk intelligence. Operated by Synectics since 1992, it enables organisations to share and access risk information to detect, prevent and understand fraud and financial crime more effectively.

The consortium brings together intelligence from across banking, financial services, lending, insurance, telecommunications, motor finance, vehicle hire and the public sector. This cross-sector model provides visibility of risk that extends beyond any single organisation, product or industry.

National SIRA currently provides extensive market coverage, including approximately 80% of Tier 1 UK banks and around 90% of the UK's largest insurers, alongside a wide range of lenders, fintechs, telecommunications providers and public sector bodies. This breadth enables analysis of how fraud and associated risks develop, connect and move across products, organisations and sectors over time.

The intelligence within National SIRA includes confirmed fraud, suspected fraud, fraud victims and clear records. This combination supports not only detection and prevention activity, but also broader analysis of behavioural patterns, emerging threats and risk trajectories. It allows participating organisations to identify linked activity, repeat offending and cross-sector exposure that would not typically be visible through isolated internal datasets.

Within *Signals*, National SIRA provides the primary quantitative foundation for analysing how fraud risk is evolving across the UK financial ecosystem, and how patterns observed in one sector may influence exposure in another.

BACK TO CONTENTS

SYNECTICS
SOLUTIONS

synectics-solutions.com