TransUnion

Optimising Performance in the FinTech Industry:

Countering Fraud and Financial Crime Threats in 2023

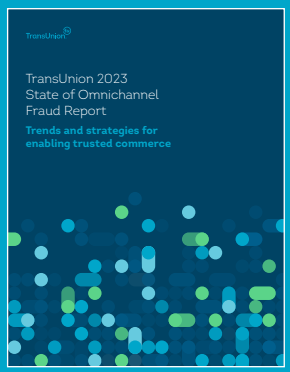
TransUnion

The real cost of fraud:

Understanding the impact of digital crime on the UK FinTech industry

In the 2023 State of Omnichannel Fraud Report, TransUnion brings together trends, benchmarks and expertise from across our identity and fraud prevention organisation. It provides insight and recommendations to those responsible for preventing potential fraud and streamlining online experiences to deliver better business outcomes.

The financial services industry experienced a 39% increase in suspected digital fraud attempt rates between 2019 and 2022[1]



Download

The real cost of fraud:

Understanding the impact of digital crime on the UK FinTech industry

Globally, in 2022, fraud returned to something closely resembling pre-pandemic levels. That said, with increased digital transaction volumes, the risk to organisations and individuals was even greater than before. Cybercriminals and fraudsters continued to show increasing sophistication – with stolen identity information at the centre of their strategies.

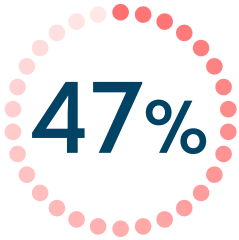
This trend continued at home. Currently worth over £174bn per year and making up over **8%** of the UK's economy,[2] it's no surprise the UK financial services sector remains a prime target for organised crime and fraudulent activity. As economic uncertainty sustains and consumers adapt their spending behaviours as a result, instances of both first- and third-party fraud continue to test lenders' fraud controls and impact bottom lines.

Of course, fraudsters don't respect national boundaries, as evidenced by the global financial services industry experiencing a **39%** increase in suspected digital fraud attempt rates between 2019 and 2022.[3] This represents the third highest of all the sectors our global device intelligence network reports on — with identity theft, loan default and first-party application fraud being the most prolific.

As many UK FinTechs look to defend their existing business in challenging economic times, there's a golden opportunity for organisations to reduce their fraud risk and improve the overall customer experience (CX) through cutting-edge, multilayered fraud and identity solutions.

In this guide, TransUnion brings together proprietary research, prevailing digital crime trends, and actionable guidance to help FinTechs and credit providers mitigate the risk of fraud without sacrificing the safe, seamless transactions consumers have come to expect.

One in seven people have committed first-party fraud or know someone who has[4]



47% of UK consumers said they were targeted with online, email, phone call or text messaging fraud attempts between Sept. and Dec. 2022[5]

Top fraud and digital crime trends facing the FinTech sector

There are many different types of fraud impacting the FinTech industry, meaning it's crucial to identify emerging trends and provide tips to help spot them. Working with our own data sets and research and partnering with customers, TransUnion FinTech SMEs identified several key criminal threats currently facing the UK industry. These occur at different stages of the customer lifecycle, underlining the importance of knowing your customer (KYC) and building trust during transactions.

TransUnion

Top fraud and digital crime trends facing the FinTech sector

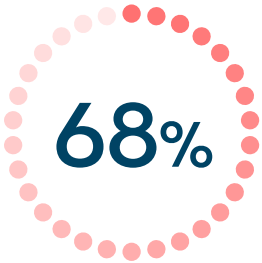
First-party fraud

One in seven British adults have admitted to committing first-party fraud.[6] And with up to **20%** of Britons thinking some types of fraud are 'reasonable',[7] research suggests a significant pool of people may also be willing to commit first-party fraud in the future.

These findings are backed by TransUnion research which indicates **68%** of UK consumers would modify their identity attributes when signing up for a service.[8] Statistics that are perhaps unsurprising given that economic pressures, such as rapidly rising food prices and energy costs, are driving changes in consumer behaviour.

As a result, the typical profiles of first-party fraudsters are changing significantly. As consumers attempt to appear more creditworthy or look for new ways to cope with the cost of living crisis, it's important FinTechs be aware of the growing risk first-party fraud poses to the sector, and take meaningful action to help protect vulnerable consumers and their brand reputations from this type of crime.

20% of Britons think some types of fraud are 'reasonable.'[9]



68% of UK consumers would modify their identity attributes when signing up for a service.[10]

TransUnion

Top fraud and digital crime trends facing the FinTech sector

First-party fraud issue 1: No intent to pay (NITP)

The financial services sector has noticed an uplift in instances of no intent to pay in recent years. Despite this, no intent to pay is still widely considered to be a hard-to-reach issue within the FinTech sector. With no real ownership over who's responsible for remedying these crimes, resulting losses are often written off as credit risk as many lenders fail to diagnose or learn from this growing problem.

Difficulties in identifying which individuals are defaulting with intent is one of many reasons this type of fraud continually goes unchecked. Other reasons, such as lack of clarity regarding whether no intent to pay should be considered fraud or credit risk, and lack of resource to work what would be timely referrals, also contribute to this issue.

What results is a perfect storm of financial crime. On one hand, fraudsters continue taking advantage of changing consumer habits and opt to default with intent. On the other hand, some increasingly desperate consumers may be driven to commit acts of first-party fraud they would never have considered previously.

Steps to detect and prevent no intent to pay

As the prevalence of no intent to pay fails to wane, fraud prevention leaders must take immediate action to curb the impact of this type of crime. **To achieve this, FinTechs should consider:**

Internal ownership:

One of many reasons no intent to pay continually goes undetected is lack of ownership from internal personnel. With teams working in siloes, many do not acknowledge NITP as their problem to solve, allowing fraudsters to repeatedly commit such crimes without consequence. Tasking an existing team (or creating a new one) to tackle this specific type of fraud could be an important first step in addressing criminals who default with intent and cost FinTechs millions each year.

Validate income information:

Our Income Verification capability is a robust and extensive set of variables that can be used in conjunction with our confidence factors to quickly decide which customer declared incomes you're happy to verify against.

Implement no intent to pay models:

FinTechs should leverage data from anti-fraud and credit solutions within analytical models to better segment consumers who present higher risk of NITP. For those higher-risk consumers this could drive more cautious credit limit decisions or underwriting reviews regarding credit and affordability risk.

TransUnion

Top fraud and digital crime trends facing the FinTech sector

First (and second) party fraud issue 2: Money mules

Sixty-eight percent of misuse of facility cases on bank accounts have intelligence indicative of money mule activity.[11] An unsurprising statistic given one in five Britons believe some types of fraud are 'reasonable' — with money muling ranked highest among these.[12]

While FinTechs broadly agree the younger generation is most vulnerable to this type of crime — with the majority of mules recruited between the ages of 17 and 24[13] — older groups are also increasingly susceptible. Lloyds Banking Group reported a **29%** increase in people aged over 40 involving themselves in muling[14] (a particularly sharp rise), showcasing how cost of living pressures continue to squeeze household funds and drive crime in new demographics.

However, not all money mules are recruited, which can make identifying and preventing these crimes even more difficult. There are purpose-opened mules, which are accounts fraudsters open with the pure intention of using them as money mules. There are also unwitting money mules; once-legitimate customers who fraudsters convince they're receiving funds for a legitimate purpose. Those customers then become a conduit for moving fraudulent funds through the system.

Steps to detect and prevent money mules

Money muling is a difficult crime to trace — an issue only compounded by consumer tolerance of it as a low-level crime.
However, despite these growing challenges, there are strategies FinTechs should consider to mitigate the impact of these crimes:

Consumer education:

With 1 in 10 young people stating they'd move money through their bank accounts in return for cash,[15] educating consumers on money muling and its impact has never been more important, especially given most are unaware of the possible 14-year prison sentence this crime can carry. Educating consumers on money mules and how to spot these schemes can help decrease incidences of this type of fraud, helping protect both your customers and your organisation.

Monitor ongoing lifecycle risk propensity using money mule models:

Look for subtle changes in account behaviour and use that as a flag for investigation.

Utilising credit data:

FinTechs should use this data to identify new applicants who may be susceptible to become a mule at point of application.

TransUnion

Top fraud and digital crime trends facing the FinTech sector

Third-party fraud

Over 409,000 cases of fraud were reported to the National Fraud Database (NFD) in 2022[16] — the highest level ever recorded. Sixty eight percent of these cases concerned identity fraud,[17] suggesting it's not only first-party fraud being fuelled by changes in consumer behaviour; third-party fraud also poses a growing threat to the FinTech sector.

As of March 2023, **40%** of UK consumers reported being targeted by fraud within the last three months[18]; the majority of these cases being phishing (**52%**), vishing (**39%**) and smishing (**37%**), suggesting consumers are consistently being targeted by criminals in order to perpetrate financial crime.

These statistics show FinTech is one of many industries under increasing threat from third-party fraud. In order to mitigate losses and reduce risk, FinTechs should consider a two-pronged approach: enhancing their fraud controls throughout the entire customer lifecycle, and creating a first line of defence with effective consumer education.

40% of UK consumers reported being targeted by fraud within the last three months.[19]

TransUnion

Top fraud and digital crime trends facing the FinTech sector

Third-party fraud issue 1: Identity (ID) theft

Identity fraud continues to be a growing problem across the UK; identity theft directly impacted over **13%** of consumers in 2022.[20] And as consumers increasingly fall victim to this type of fraud, the number of businesses being targeted by these identities — including those in the financial services sector — also continues to increase. In fact, the highest ever volume of identity fraud cases was recorded in 2022, up **23%** from 2021.[21]

As consumer habits change, such as the shift toward online banking necessitated by the COVID pandemic, identity thieves continue to take advantage of the sector's rush to meet demand and digitise customer journeys, exploiting new ways of stealing personal information and perpetrating identity fraud.

In fact, so prevalent is this type of fraud, **52%** of UK consumers are concerned about falling victim.[22] In an age when consumer trust is a vital component in retaining existing business, leaders that successfully mitigate this type of fraud could enjoy more profitable, long-lasting consumer relationships.

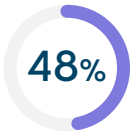
However, as our reliance on and usage of online products accelerates with the digital age, consumer expectations for convenient, secure transactions also continue to rise. In fact, **49%** of consumers have abandoned an online application for a financial product because it took too much time to fill out the form, while a further **30%** of consumers did the same because they didn't trust their personal data would be secure.[23] These findings emphasise the need for FinTechs to create consumer journeys that strike a vital balance between security and ease of use many struggle to achieve in practice.

This creates a proverbial Catch-22 for fraud leaders: Either increase fraud controls and strengthen KYC checks (and risk an increase in false positives that could deter genuine customers) or loosen these controls in favour of a better customer experience that could leave FinTechs open to fraud losses, reputational damage and regulatory fines.

Top Reasons UK Consumers Said They Abandoned Online Application or Form For a Financial or Insurance Product

Too much time to fill out the form

Site too slow



Too much information required and/or requested

Didn't trust personal data would be secure

TransUnion

Top fraud and digital crime trends facing the FinTech sector

Third-party fraud issue 1: Identity (ID) theft

Steps to detect and prevent ID theft

Eighty six percent of identity fraud now occurs online,[24] meaning FinTechs should pay close attention to strengthening digital journeys. While identity theft is prevalent across several industries, fraud prevention leaders can take learnings from one another to help curb this type of fraud. **Strategies FinTechs should consider include:**

Device Risk with Behavioural Analytics at application, and Device Risk at login:

FinTechs can utilise device history, user behaviour insights, device-to-device and device-to-account associations from our global network of billions of devices and transactions to better detect the use of synthetic or stolen identities. In instances where suspicious behaviours or devices are flagged, FinTechs can add additional fraud controls without impacting the CX of legitimate customers.

Utilise consortia and previous search data:

Detect patterns and uncover anomalies by widening the use of consortia and previous search data.

Verification of bank account ownership:

Industry leading bank account ownership checks can deliver match rates up to **97%**. Not only does this support regulatory requirements around ownership checks and where funds are paid from and to, it also acts as a robust anti-fraud control during the onboarding process.

Email and mobile verification:

Risk profiling email and mobile details can validate connections, assess risk indicators and strengthen KYC checks to help identify and prevent instances where stolen and synthetic identities are being used by fraudsters.

TransUnion

Top fraud and digital crime trends facing the FinTech sector

Third-party fraud issue 2: Account takeover

Global instances of account takeover fraud (ATO) increased by **81%** between 2019 and 2022,[25] costing organisations billions each year. Often a direct result of ID theft, it's no surprise increased incidences of this type of fraud make account takeover a top concern for **41%** of UK consumers.[26]

As our reliance on and usage of online accounts accelerates with the digital age, consumer expectations for convenient, secure transactions continue to soar with security of personal data ranked as "very important" by **78%** of UK adults.[27] There is, therefore, increased pressure on FinTechs to provide secure experiences that help protect consumers from digital crime without compromising on the ease of use customers have come to expect.

Steps to detect and prevent account takeover

Consumer trust is essential to establish long-lasting and profitable customer relationships. With account takeover repeatedly being named as a top concern for consumers, banks should consider:

Device authentication at login:

21% of consumers named device authentication as one of their preferred online security measures.[28] Authenticating devices at login using Device Risk and Device-Based Authentication reduces the likelihood of a successful account takeover without adding unnecessary friction for the customer.

Utilise multifactor authentication, such as one-time passcodes (OTP):

One-time passcodes are a valuable tool in helping prevent incidences of account takeover. While adding an extra layer of protection to customer accounts, it's also favoured by most UK adults; **52%** named an OTP sent via SMS as their preferred security measure followed by email OTP (**40%**).[29]

Risk assess changes made to accounts:

Including email, direct debit or mobile, these are common elements of account takeover activity.

What's next for FinTechs wanting to fight fincrime?

Forty nine percent of UK consumers ranked the security of their personal data as their top expectation from online organisations.[30] As more of our lives move online, it's no surprise customers increasingly value the security of their information and expect more from the FinTechs that hold that data.

To successfully win over competitors and defend your existing customer base, an effective and robust fraud and identity strategy is key. To achieve this, FinTechs should renew focus on strengthening their efforts to better detect and prevent digital crime.

From a technology perspective, advances in data solutions are helping FinTechs better spot the signs of fraudulent behaviours. Our recent product release, Device Risk with Behavioural Analytics, helps enable fraud prevention leaders reduce false positives and identify risk by uncovering device behaviour, user behaviour and risk indicators in real-time based on our platform's knowledge of billions of devices and transactions and NeuroID's one trillion behaviour signals. In addition, our proprietary global device intelligence database and acquisition of businesses, such as iovation, Neustar and Sontiq, are helping FinTechs counter increasingly sophisticated criminal activities.

Like many industries, FinTechs are also susceptible to worldwide events and consumer trends. Macro events, such as Russia's invasion of Ukraine, can deliver seismic economic shocks, impacting both consumer and criminal behaviour. Their unpredictability underscores the importance of having robust fraud, ID and anti-money laundering (AML) solutions in place to better protect consumers and meet regulatory requirements. To overcome this, leaders in the FinTech sector should think about ways to link to other industries and share outcome data to better spot digital crime. Consumers consistently rank the security of their personal data (**78%**), ease of registration (**57%**) and ease of authentication (**62%**) as "very important",[31] further emphasising the business-wide benefits of working with partners that can support fraud analytics, diversifying data sources, and engineering optimal fraud prevention strategies.

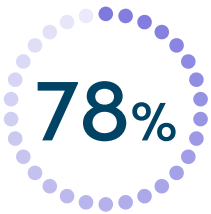
57% of consumers rank the ease of registration as "very important"[32]

What's next for FinTechs wanting to fight fincrime?

At a more strategic level, leaders in the FinTech sector should be thinking about the possibilities presented by the FCA's Consumer Duty and the upcoming Payment Systems Regulator's (PSR) APP scams regulatory change. As account providers plan for the potential costs associated with 50/50 liability, and more widely, FinTechs consider how they'll meet new requirements to better protect vulnerable consumers, these policies pose a golden opportunity for organisations to enhance their fraud controls and operational processes. This can be achieved through access to new data sources, implementing new fraud solutions, and taking renewed ownership of hard-to-reach issues like NITP.

The other key pillar for tackling fraud and digital crime is engagement with consumers. At TransUnion, we believe in Information for Good®, and the value of informing consumers of the risk of carrying out fraud should not be underestimated. For some, money muling may initially appear to be an attractive and relatively low-risk proposition, especially to those who are unaware they're engaging in criminal activity in the first place. However, educating customers on how to spot such activity and the possible repercussions could help deter them from ever considering engaging in financial crime. This education can be extended across various types of fraud, helping cut these crimes off at the source, and saving FinTechs time and money in resolving the problem later.

Readers should use this guide to evaluate their current fraud prevention programmes in the context of the broader market. This information and insight should be shared across the organisation with the goal of retaining customers and securing growth through effective fraud prevention and safer, more convenient customer experiences.



78% of consumers rank the security of their personal data as "very important"[23]

Time to take action?

If you'd like to get an expert view of how fraud and digital crime is impacting your business, or understand how our TruValidate™ solutions could complement your fraud strategy, get in touch:

Contact us

Glossary

This guide blends proprietary insights from TransUnion's global intelligence network, third party research, TransUnion UK's Consumer Pulse study, and a specially commissioned TransUnion consumer survey in 18 countries and regions globally. TransUnion TruValidate™ suite comprises identity and fraud products that secure trust across channels and deliver seamless consumer experiences.

1 TransUnion TruValidate™ global intelligence network data
2 Hutton, 2022
3 TransUnion TruValidate™ global intelligence network data
4 Is it okay to commit fraud? Cifas
5 TransUnion Global Fraud Survey
6 Tackling first party fraud | Statistics and Examples | Cifas
7 Tackling first party fraud | Statistics and Examples | Cifas
8 Tackling first party fraud | Statistics and Examples | Cifas
9 Tackling first party fraud | Statistics and Examples | Cifas
10 Tackling first party fraud | Statistics and Examples | Cifas
11 Fraudscape 2023 - Cifas
12 Is it okay to commit fraud? Cifas
13 Money muling - National Crime Agency
14 Money mules are getting older – with serious penalties for those caught moving scam cash - Lloyds Banking Group plc
15 Fraudscape 2023 - Cifas
16 Fraudscape 2023 - Cifas
17 Fraudscape 2023 - Cifas
18 TransUnion Consumer Pulse Survey
19 TransUnion Consumer Pulse Survey
20 TransUnion Consumer Pulse Survey
21 Fraudscape 2023 - Cifas
22 TransUnion Global Fraud Survey
23 TransUnion Global Fraud Survey
24 Fraudscape 2023 - Cifas
25 TransUnion TruValidate™ global intelligence network
26 TransUnion Global Fraud Survey
27 TransUnion Global Fraud Survey
28 TransUnion Global Fraud Survey
29 TransUnion Global Fraud Survey
30 TransUnion Global Fraud Survey
31 TransUnion Global Fraud Survey
32 TransUnion Global Fraud Survey

TransUnion

TransUnion TruValidate™

Our TruValidate™ solutions encompass identity, device and behavioural insights to help organisations confidently and securely engage consumers at each stage of the customer journey, helping improve conversions, reduce fraud losses and deliver enhanced, friction-right user experiences.

For more information on how to enhance your fraud prevention strategies, get in touch:

transunion.co.uk