TransUnion

TransUnion 2024 State of Omnichannel Fraud Report

Trends and insights for enabling trusted commerce

Introduction

This is the second State of Omnichannel Fraud Report I've contributed to in my role as General Manager, Fraud and Identity for TransUnion UK.

Our report brings together trends, benchmarks, and identity and fraud expertise from across our organisation. It provides insight and recommendations to those responsible for preventing fraud and streamlining customer experiences to deliver better business outcomes. Studying the trends — and overlaying them with recent client conversations — four key priorities for fraud fighters and stakeholders involved in delivering safe growth for their organisations include:

Delivering friction-right customer experiences

Being successful means aiming to be customer-centric in every decision you make. Therefore, organisations must aim to create confidence through data, insight and technology to maximise pass-through of genuine customers with limited friction — which can be contrasted with using the same tools to identify and mitigate fraud through robust checks and increased friction for potential bad actors.

Understanding and responding to criminal capabilities

The flipside of being customer-centric is the requirement of being 'criminal-centric'; understanding how bad actors are using technology and consumer behaviour to evolve their attack methods and then probe and exploit systems is critical. Artificial intelligence is the latest piece of kit criminals are deploying free of rules and regulations — through mass-generated social engineering to deepfake identities and supporting documentation (such as shallow-fake photos used for insurance claims). It presents an increasing challenge to the underlying integrity of the whole economy and must be countered with an evolving solution-set and dynamic strategy response.

Continued optimisation of fraud prevention and onboarding strategies

Teams responsible for safely onboarding new customers are faced with an ongoing dilemma of driving conversion and top-line growth versus reducing fraud losses and associated costs. To do this, ongoing tactical and strategic performance improvements are required, along with collaborative engagement with internal stakeholders. On the former, we're seeing technology improvements like performance monitoring and machine learning models being deployed to complement policy rules and scorecards. Whilst effective, some of these controls are often managed by different teams, which can create internal challenges. For example, fraud prevention teams, financial crime teams and digital teams need to improve ways of working to optimise identity verification and fraud prevention solutions to unlock real growth — while minimising operational overheads.

Seek out the economic value upside and effectively influence stakeholders

Investments associated with improving fraud controls are often seen as overhead or a cost — or more concerningly — the cost of fraud is perceived as a cost of doing business. Fraud fighters are faced with the challenge of mobilising internal investment and resources; successful organisations are able to incorporate the CX and top-line benefits when assessing these business cases.

It would be remiss to not acknowledge perhaps the most important defence against the rising tide of fraud: people. When engaging with clients, partners and industry stakeholders at summits, forums, roundtables and directly with clients, I continue to be filled with optimism by the genuine and almost-universal desire of fraud and financial crime practitioners to collaborate across organisations and sectors to enhance our understanding of emerging threats and improve our collective defences.

I encourage you to use this report to:

- Increase awareness of global and local trends in consumer perceptions and potentially fraudulent transactions
- Leverage these contextual insights and recommendations to evaluate and enhance your fraud prevention strategies
- Share this information with key internal stakeholders and use as a basis to align on the most appropriate organisational strategies

Finally, we must continue to remember the vast majority of consumers and transactions are genuine; this provides an ideal foundational principle to pursue friction-right strategies that will help consumers and organisations transact with confidence — and enable trust across all touchpoints.

Chad Reimers
General Manager – Fraud and ID, TransUnion UK

All data in this report blends proprietary insights from TransUnion's global intelligence network, a specially commissioned TransUnion consumer survey in 18 countries and regions globally, and other third-party research.

Contents

TransUnion

Consumer Sentiment

Honouring expectations for security and convenience is a winning strategy

With turbulent levels of inflation, the erosion of real incomes, and waning economic growth, now is an uncertain time for both consumers and organisations across the country. As households are curbing their spending and businesses continue to face increasing operational costs, many organisations are looking for new ways to attract and support customers while delivering safe growth. For many, the answer could lie in their fraud prevention strategies.

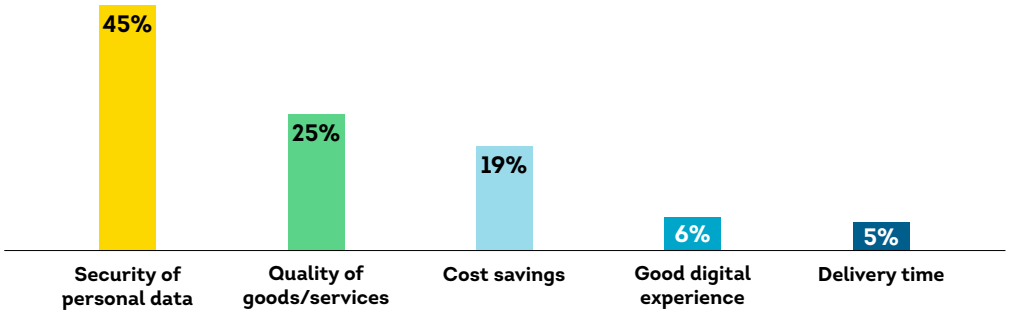
The volume of risky transactions in the UK has increased by 16.81% since 2019, an unsurprising statistic at a time when fraudsters seek to exploit loopholes in digital journeys and perpetrate fraud. In parallel, consumers have increasingly high expectations for organisations to protect their identities and keep their data safe. In fact, nearly half (45%) of consumers ranked personal data security as the top reason to do business with an online company, while 90% said confidence their personal data will not be compromised was the most important factor when choosing with whom to transact online.

Yet, the desire for security only tells half the story. As the digital-first Gen Z and Millennial generations make up a larger proportion of the UK population, the demand for convenient digital transactions has also increased. Forty-five percent of UK consumers reported they'd switch companies to receive better digital experiences. This increased to 57% for Millennial users and 61% for Gen Z consumers, showcasing how streamlined experiences to these populations could be a winning strategy for businesses in 2024.

Significantly, the vital balance between security and ease of use is one many businesses struggle to achieve in practice, creating 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 organisations open to fraud losses, reputational damage and regulatory fines.

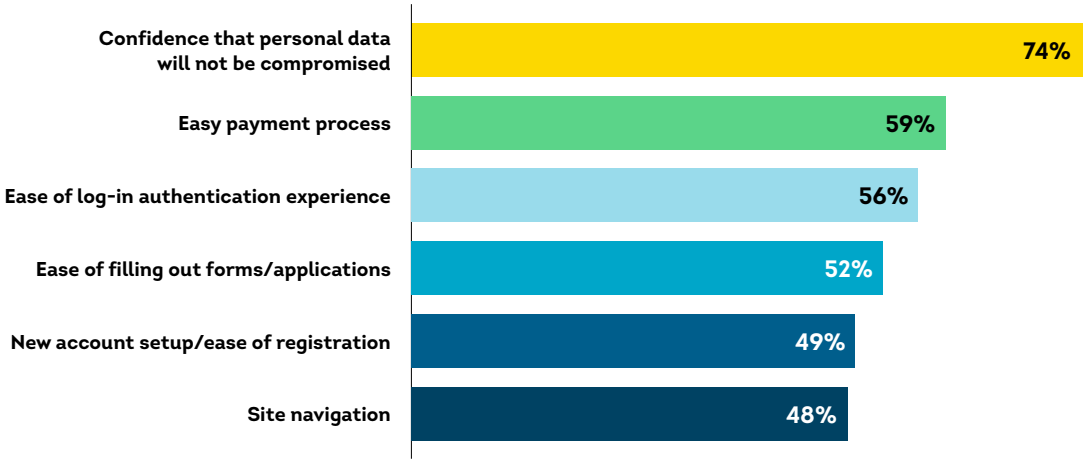
Ranked Expectations or Qualities in Preferred Online Companies

Top answer chosen



Stated Important Features When Choosing Who to Transact With Online

Very important



Source: TransUnion consumer fraud survey

Trust and safety are critical to conversion rates

The balance between security and convenience isn't just a digital challenge. Few consumers (43%) reported conducting more than half of their transactions online in 2023, down from 44% in 2022 and 50% in 2021. As consumers slowly shift back to in-person journeys, it's vital fraud prevention leaders look to secure in-person and call centre engagements as fraudsters explore paths of lesser resistance. Customer support is often the area of a company's network perimeter most susceptible to a successful breach.[1] In fact, social engineering is on the rise and, because of its success rates, is being used in two-thirds (65%) of all attacks in the phone channel.[2] Social engineering occurs when a fraudster psychologically manipulates a customer support agent into skipping a part (or parts) of the authentication process or divulging confidential details.

Once successful, a bad actor can gain access to a target account, leading to the risk of unauthorised payments or utilisation of credit. As a result, the target may be left vulnerable to both financial and psychological harm.

This type of fraud could evolve over time as many UK companies look to block caller line identification (CLI) from non-UK originating numbers. While this will reduce instances of call centre fraud and scams whereby a fraudster misrepresents themselves as a business representative or consumer, it could give rise to fraud across other channels like WhatsApp or chat bots. Technology, such as ChatGPT, could also be a key risk here as new "prompt engineered" attack profiles could be used to facilitate the exposure of customer details and enable further instances of fraud.

However, whilst fraudsters are exploiting this slow shift but noticeable trend towards in-person and telephony channels, it's important to understand the reason behind this changing consumer behaviour. While the drop may be due in part to more physical locations being open in the wake of the COVID pandemic, TransUnion research suggests it's also in response to increased fraud risk awareness. Sixty-nine percent of UK consumers reported fraud concerns were the top reason they wouldn't use a site again, up from 62% in 2022. A further 47% also reported abandoning an online shopping cart due to concerns about fraud and/or security, demonstrating how improving perceived security can have a huge impact on business performance and conversion rates in 2024.

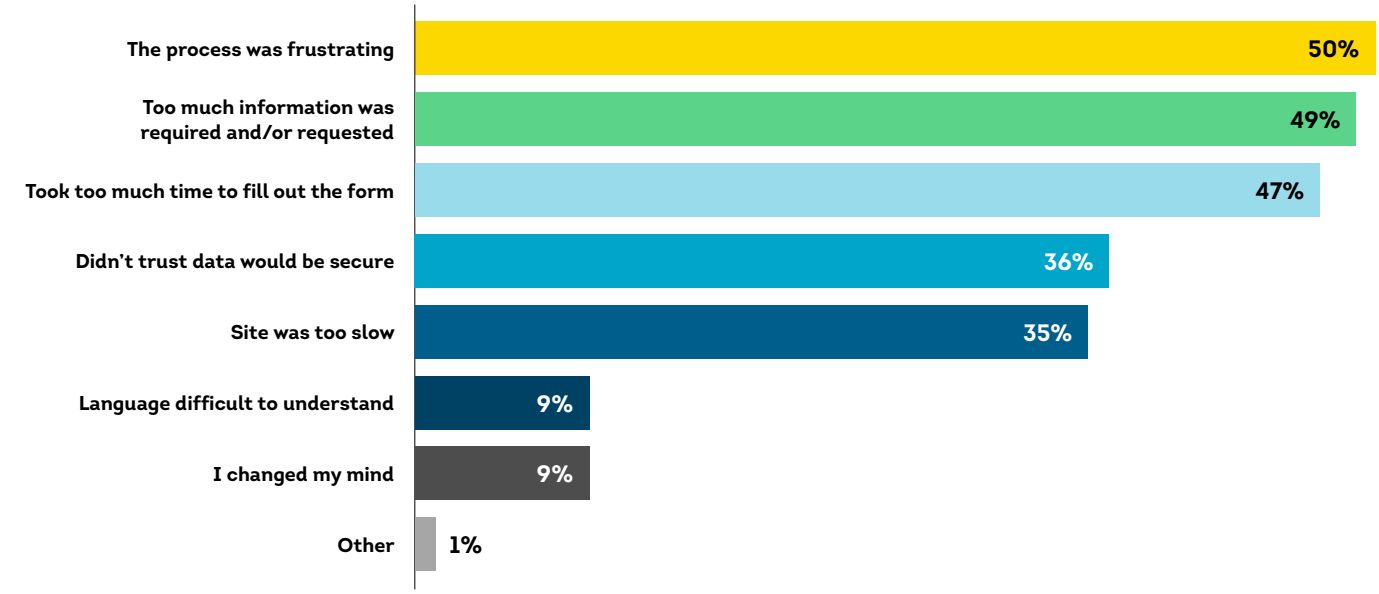
Perceived security, though, doesn't seem to be the only instigator of abandonment. When asked why they'd abandoned an application for a financial or insurance product, the majority of consumers cited friction as their primary motivator: The process was frustrating (50%), too much information requested (49%); and too much time to complete (47%) were the top reasons for abandonment.

This suggests to increase conversion rates and win over competitors in 2024, it's vital business leaders employ fraud prevention and identity verification solutions that secure both online and offline journeys without increasing friction for genuine consumers.

Some strategically minded organisations may even take this one step further by improving processes for those who opt to 'buy in to' security measures. As an example, a retailer may offer next day delivery to those who submit to a document verification or facial biometrics check, while those who do not submit must endure a longer delivery period. By using fraud checks as a behavioural nudge, businesses can incentivise the use of fraud checks to access rewards or improved services. In return, businesses can enjoy reduced fraud losses and increased consumer trust.

Discover how business leaders can balance fraud prevention with convenient customer experiences here

Reasons for Abandoning An Online Application or Form for a Financial or Insurance Product



Source: TransUnion consumer fraud survey

1 Social Engineering Call Centers White Paper
2 Social Engineering and Fraud in the Contact Centre

TransUnion

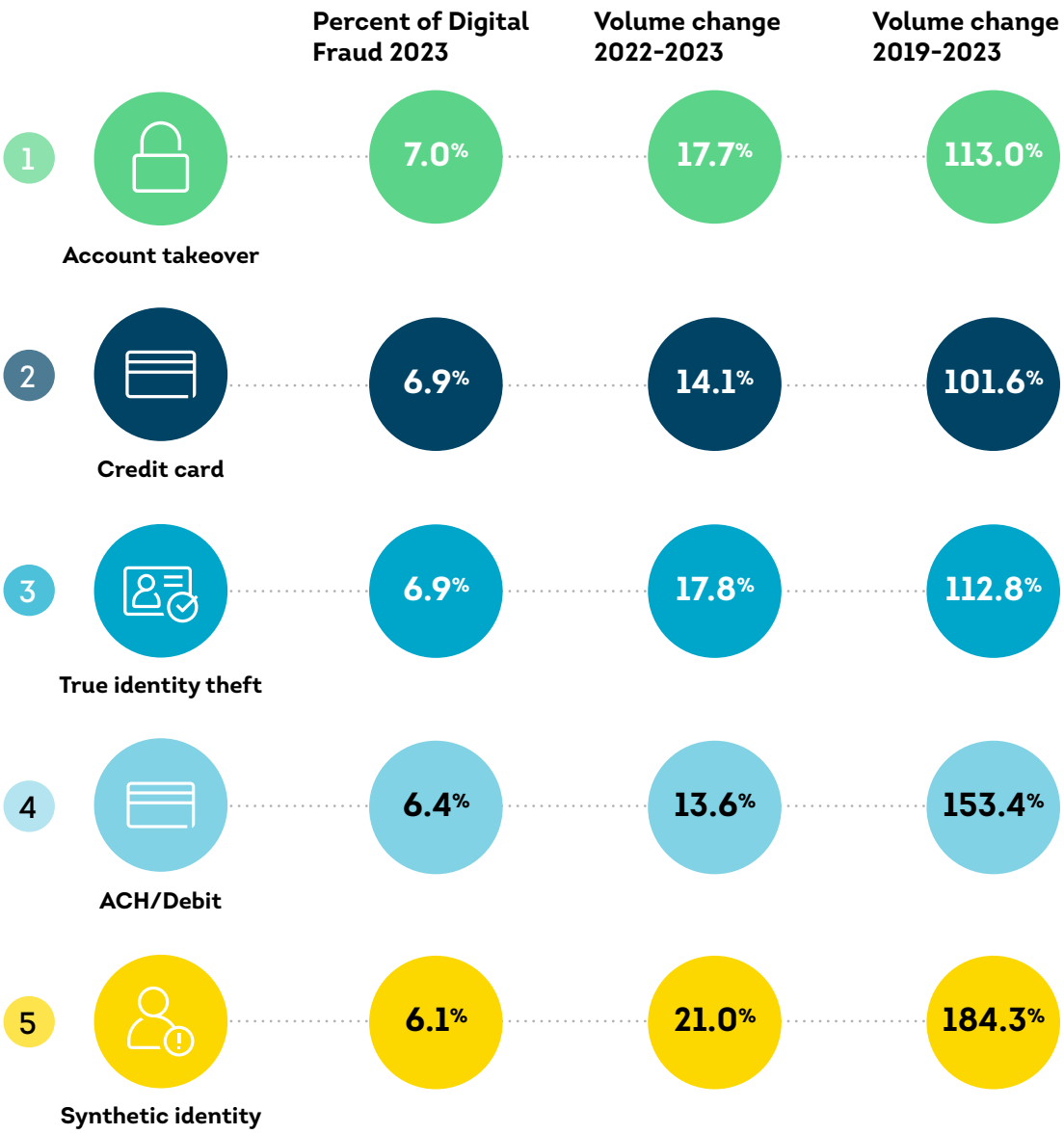
Global Digital Fraud Trends

Account takeover topped the list of most common fraud types

Digital fraud continued to grow in 2023, with the rate of suspected fraudulent digital transactions rising to 5% in 2023 — 8% higher than 2022.

Driving this increase in fraud was Account Takeover (ATO), which accounted for 7% of suspected digital fraud globally, slightly surpassing credit card fraud (6.9%) as the top type of digital fraud reported to TransUnion by its customers. However, synthetic identity fraud was the fastest growing type of fraud in 2023, increasing to 6.1% globally (from 5.3% in 2022), representing a 21% year-on-year growth and 184% over the last five years.

Top Fraud Types and Their Growth



Source: TransUnion TruValidate™

Digital fraud trends by global industry

The **retail industry** experienced the largest percentage (8.7%) of suspected fraudulent digital transactions globally in 2023, a 21% increase over 2022. Promotion abuse was the most reported type of fraud for retail transactions.

Despite retail's overall exposure to fraud, the **gaming industry** experienced the highest rate of suspected fraudulent transactions in 2023 in the most (six) markets: Colombia, the Dominican Republic, Kenya, Puerto Rico, Spain and the US. This is an important statistic to be aware of for gaming operators looking to expand into international markets. It's also important for business leaders in this space to recognise the susceptibility to fraud typologies across sectors.

Digital fraud trends by UK industry

The **gaming sector** experienced the second largest percentage (7.25%) of suspected fraudulent digital transactions in the UK in 2023, with promotion abuse being one of the most prolific fraud types experienced by operators. In fact, bonus abuse costs top tier gaming operators millions each year. While fraudsters have increased the sophistication of their bonus hunting, they continue to rely on impersonation techniques and loopholes in onboarding checks.

The UK **insurance industry** also felt the impact of fraudsters with the volume of suspected fraudulent transactions increasing by 29.8% between 2022 and 2023. This statistic was driven by a combination of first- and third-party application fraud — which continues to accelerate at both quote and application stages. Quote manipulation and fronting also remained significant issues to insurers with 22% of parents admitting to insuring their child's car in their own names.[3] This is just one example of how motorists may be unknowingly or (because of cost of living pressures) knowingly committing acts of insurance fraud.

7.25%

increase in suspected digital fraud transactions in the UK gaming sector

3 Almost one-quarter of parents of young drivers could be committing insurance fraud

Global Digital Fraud Attempts by Industry

- Suspected Digital Fraud attempt rate 2023
- Top fraud type 2023
- Percent change in suspected Digital Fraud volume 2022–2023

Retail

2023
8.7%
Promotion abuse

2022-2023
+33.5%

Video gaming

2023
7.6%
Gold farming

2022-2023
+32.6%

Gaming
(online gambling, poker, etc.)

2023
5.3%
Promotion abuse

2022-2023
+2.9%

Communities
(online dating, forums, etc.)

2023
4.6%
Profile misrepresentation

2022-2023
+9.3%

Telecommunications

2023
4.5%
Credit card fraud

2022-2023
-7.6%

Financial services

2023
4.3%
True identity fraud

2022-2023
+5.8%

Travel & leisure

2023
2.3%
Credit card fraud

2022-2023
+25.0%

Insurance

2023
1.5%
Policy violation

2022-2023
+18.8%

Government

2023
1.4%
Account takeover

2022-2023
+144.9%

Logistics

2023
0.9%
Shipping fraud

2022-2023
-43.9%

Source: TransUnion TruValidate

New Account Creation Digital Fraud Risk

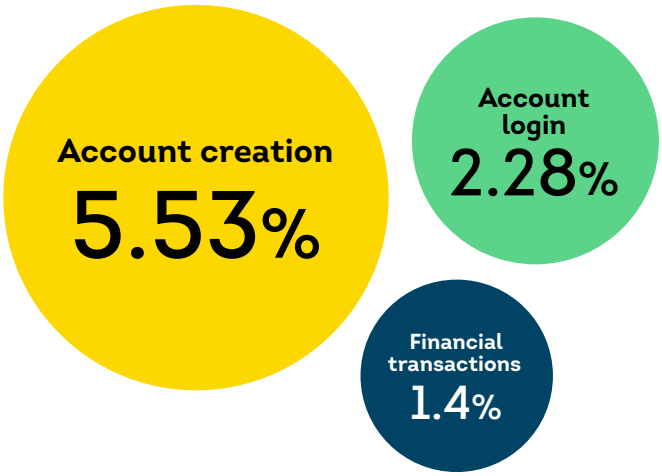
New account openings present highest risk stage in customer journey

Organisations and consumers face risk across the omnichannel experience. Looking at risk by customer journey stage, of particular concern is risk to new account creation. Primarily driven by bad actors using fabricated or stolen identities to open accounts, this account creation stage of the consumer journey is fraught with challenges for organisations, with first-party fraud, bonus abuse and ghost broking posing key issues for fraud prevention leaders. Of all UK account creation transactions in 2023, 5.53% were suspected to be fraudulent. The high percentage of account opening fraud contrasted with transactions more typically associated with fraudulent behaviour. In fact, it was over 50% higher than account logins leading to ATO, and nearly four times more than financial transactions in which money actually changed hands.

Interestingly, the UK isn't alone in this trend, and a similar pattern was detected in each of the global markets TransUnion operates in.

Customer Journey Transaction Type Digital Fraud Risk

Percentage of each transaction type suspected to be Digital Fraud globally in 2023



Money mule rings are on the rise

Echoing this sentiment, instances of money muling continued to rise across the UK with over 37,000 bank accounts demonstrating behaviour associated with muling in 2023.[4] While businesses broadly agree the younger generation is most vulnerable to this type of crime — the majority of mules recruited are aged between 17 and 24[5] — older groups are also susceptible. Lloyds Banking Group reported a 29% increase in people aged over 40 involving themselves in muling,[6] showcasing how cost of living pressures continue to squeeze household funds and drive crime in new demographics.

These trends may accelerate as muling moves onto social media platforms and becomes more visible. Well-intended legislation like the Online Safety Bill may create a new or expanded industry of social media accounts being created and sold by willing mules. As legitimate users allow fraudsters to use accounts with permission, credentials and accounts will hold value for fraudsters.

As the Payment Systems Regulator's (PSR) 50-50 shared liability regulation is set to come into force in late 2024, whereby there will be a shared liability split between sending and receiving institutions, it's vital lenders tackle this growing issue. Those that fail to do so could risk losing significant sums to this type of fraud.

Source: TransUnion TruValidate

4 Biggest ever crackdown on money mules in the UK - GOV.UK
5 https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime/money-muling#:~:text=Most%20mules%20are%20recruited%20between,adequately%20explain%20the%20origin%20of.
6 Money mules are getting older – with serious penalties for those caught moving scam cash - Lloyds Banking Group plc

Consumers readily modify identity when originating accounts

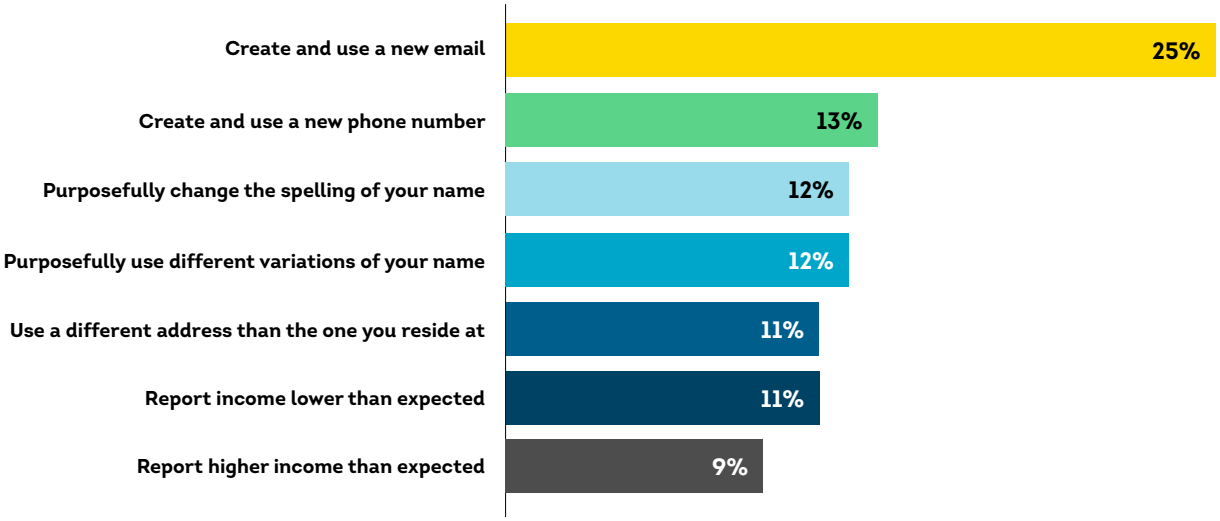
Sixty three percent of UK consumers admitted to modifying their identity attributes when signing up for a product or service in 2023. When asked in what ways they modified their identities, consumers cited creating and using a new email address (25%) as the most common way followed by modification of their names (24%) and using a different phone number (13%).

While some consumers may opt to change these details to avoid SPAM emails — a growing concern that led to the creation of Apple's *Hide My Email* feature — there could be more concerning reasons as to why they readily amend their personal data when originating accounts. As the cost of living crisis leaves many household incomes under strain, it's unsurprising some consumers may feel under pressure to commit these acts in order to secure access to better deals, repay debts or save funds.

However, economic pressures may not be the only driver of this behaviour as consumer attitudes toward first-party fraud also seem to be changing. When asked what types of fraud consumers thought were 'reasonable,' 24% cited asset conversion (for example, the act of selling a vehicle privately that was subject to a finance agreement) and money muling (20%) as the most acceptable forms of fraud. These types of fraud were also considered least likely to be illegal at 34% and 22%, respectively — followed by mobile insurance fraud (20%).[7]

These statistics hint at high levels of tolerance among the UK population toward certain types of first-party fraud, which could lead to some consumers feeling justified in their actions and others unaware they're committing an act of fraud in the first place.

Top Ways Consumers Said They'd Modify Their Identity Attributes When Signing Up for a Product or Service



Source: TransUnion consumer fraud survey

7 1 in 8 UK adults admit to committing fraud in the last 12 months

Consumer Focus: Fraud Risk is Baked into Financial Vulnerability

One of the economic challenges stemming from the cost of living crisis is the growing concern around consumer vulnerability. The socioeconomic turbulence of the 2020s has created unpredictable consumer behaviours and a spike in digital crime. This has made vulnerability a complex, wide-ranging concept for organisations to grapple with.

Fraud is the most experienced crime in the UK, affecting society economically and socially. It accounts for over 40% of crime in England and Wales.[8] We've seen the publication of the first National Fraud Initiative in over a decade and the Financial Conduct Authority's Consumer Duty which demands better outcomes for customers, and there's a clear motivation across the digital economy to better detect and prevent fraud.

Three types of fraud that are linked to consumer vulnerability are:

- Authorised payment fraud, particularly on vulnerable consumers — and the resultant mental health impact this can have on victims.
- Scams, mules and account takeovers are increasingly evident — while there are best efforts being deployed by government, industry, and company-direct awareness campaigns and the introduction of controls like confirmation of payee for payments, there remains a long way to go.
- Dormant accounts and the ability to spot no intent to pay characteristics — In recent years, TransUnion has pioneered client portfolio analysis looking for signals within dormant accounts and launched new models to help businesses identify risk of consumers with no intent to pay facilities they are taking on.

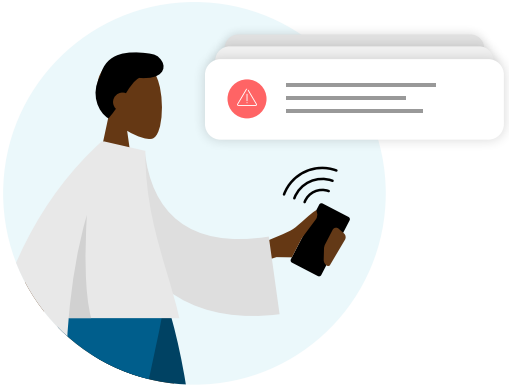
Consumer vulnerability and fraud: How data solutions and customer education can help

Consumer vulnerability is likely to be a consideration for professionals charged with addressing fraud and crime within their organisation. It requires a strategic mindset and the agility to orchestrate a friction-right experience that addresses this specific challenge whilst countering the numerous fraud types and threats. Data solutions that offer deeper customer insights and advanced identity verification can play a valuable role in developing appropriate approaches.

Additionally, adhering to evolving compliance requirements will require a renewed commitment to customer care — which can quickly become a key part of an organisation's value proposition. This can be split into:

- An emphasis on programmes for vulnerable consumers that provide the layers of checks that allow them to use services in a secure, accessible way and raises alerts to suspicious behaviour.
- Appropriate and timely support for victims of financial crime — this experience will likely make or break the customer and business relationship.
- Continued work in the education space that includes making customers aware of the risk posed by participating in online crime and advice if they are being coerced to do so, and providing useful content on how to protect their accounts and personal data.

Over 40% of crime in England and Wales is attributed to fraud [8]



8 https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

Response Strategies for Fraud Prevention and Digital Leaders

In 2024, there is a renewed pressure on business leaders to balance consumer demand for streamlined, convenient transactions with robust fraud prevention strategies that will protect both consumers and organisations from financial crime. However, as the fraud and identity landscape continues to shift, this ever-moving goal can feel increasingly difficult to execute in practice.

To help businesses achieve this intricate balance, organisations can leverage a range of response strategies to mitigate fraud risks in 2024:

Frictionless digital insight at onboarding

As the volume of attempted fraud at the onboarding stage continues to soar, there is an urgent need for organisations to enhance their digital insights without adding fiction for genuine customers.

Solutions such as Device Risk can identify devices with evasive behaviours, risky attributes or a history of fraud from the moment they connect with an online platform. Coupled with the granular fraud evidence uploaded by cross-industry organisations within the consortia, this powerful solution enables businesses to make faster, better-informed onboarding decisions without sacrificing on the customer experience.

However, as all fraud leaders know, there is no one silver bullet when it comes to fraud prevention. Layering signals such as mobile and email verification adds an additional level of invisible security. By effectively validating email address and mobile phone information, these solutions can help identify credentials linked to suspicious behaviour and produce a risk score that enables your teams to make faster, better-informed decisions on when to increase fraud and Know Your Customer (KYC) checks for certain users.

Step-up authentication to address and reduce the "grey"

Utilising step-up authentication within your fraud prevention strategy can help to strike the balance between security and friction. The goal of this authentication is to adapt identity requests to the importance of the resource and the risk level if it were to be exposed. Asking for too little gives your users (or whoever might be posing as them) a dangerous amount of freedom, whereas asking too much, especially up front, creates obtrusive friction that could cause you to lose good customers.

Solutions such as Document Verification and Facial Biometrics can form an important component of this strategy. By automatically recognising and verifying multiple datapoints in real-time, this form of step-up authentication can create an additional layer of evidence to support decisioning – maintaining high first-time pass rates and low false-positive rates, with minimal verification speeds. Ensuring these solutions leverage the latest in technological capability – such as liveness checks and AI-detection – is critical.

Improved identity views

Utilising previous search and consortia data is a powerful tool often under-utilised by some businesses. This additional layer of insight can be invaluable to fraud leaders, as it allows them to spot patterns in behaviour – this can help build a 'identity graph of trust', based on a longitudinal view of multiple genuine interactions of an individual with businesses. Widening the usage of consortia data can also equip fraud teams with the insights needed to spot anomalies which may have otherwise gone unnoticed, helping capture more instances of fraud without impacting on the customer experience.

Enhanced internal capabilities

According to a study by IBM, human error is the main cause of 95% of breaches.[9] To help reduce this statistic, it is vital for organisations to enhance their internal capabilities through initiatives such as staff training. By investing in the ongoing development of your teams, and keeping them informed of your authentication policies and the tactics employed by bad actors, organisations can heavily reduce the risks posed by fraudsters looking to commit financial crimes.

However, it would be remiss to assume that staff training alone will resolve this far-reaching issue. Mistakes do happen, which is why it is important all companies and government bodies have a plan in place in the event that a fraudster is able to penetrate your organisation's perimeter. Investing in a Data Breach Support Service can help minimise both the reach and risk of a breach, whilst building trust with consumers through advanced remediation strategies.

9 The Role of Human Error in Successful Cyber Security Breaches (usecure.io)

Conclusion

Moving forward, organisations face more sophisticated techniques used by cybercriminals targeting identity data with the means of performing first- and third-party fraud schemes at scale. Not only will organisations have to deal with persistent account hacking, fraudsters will continue building fake but reputable identities enabled by technology to operate with unprecedented scale and speed.

As for consumers, they want secure digital experiences that foster confidence when transacting. And they want those experiences to be convenient at every stage of the customer journey. That said, consumers do want strong authentication controls to ensure they're safe — but not so much as to become a hassle. Fraud leaders should take an enterprise-wide approach to fraud prevention and building customer trust. Employ a strategy of continuous innovation through better data, analytics and technology to detect possible fraud more accurately while reducing friction for genuine customers.

For more information on how to enhance your existing fraud prevention strategy, contact a member of our team today.

linkedin.com/company/transunion

transunion.co.uk/truvalidate

TransUnion

Data Sourcing Methodology

This report blends proprietary data from TransUnion's global intelligence network and specially commissioned consumer research. The TransUnion TruValidate™ suite comprises identity and fraud products that help secure trust across channels and deliver seamless consumer experiences.

Consumer credit report disputes

TransUnion's consumer credit report dispute findings were based on UK consumer credit data.

Consumer survey

This online survey of 13,923 adults was conducted Dec. 5–23, 2023 by TransUnion in partnership with third-party research provider, Dynata. Adults 18 years of age and older residing in 18 global markets (Brazil, Canada, Chile, Colombia, the Dominican Republic, Hong Kong, India, Kenya, Mexico, Namibia, the Philippines, Puerto Rico, Rwanda, South Africa, Spain, the UK, the US and Zambia) were surveyed using an online research panel method across a combination of desktop, mobile and tablet devices. Survey questions were administered in Chinese (Hong Kong), English, French (Canada), Portuguese (Brazil) and Spanish (Colombia, the Dominican Republic, Mexico, Puerto Rico and Spain). To ensure representation across resident demographics, the survey included quotas to balance responses across key demographics like age, gender and income. Please note some chart percentages may not add up to 100% due to rounding or multiple answers being accepted.

Digital fraud

TransUnion uses intelligence from billions of transactions originating from over 40,000 websites and apps to protect digital transactions. The rate or percentage of suspected digital fraud attempts reflects those which TransUnion customers either denied in real time due to fraudulent indicators or determined were fraudulent after reviewing — compared to all transactions it assessed for fraud. The country and regional analyses examined transactions in which the consumer and suspected fraudster was located in a select country and region when conducting a transaction. The global statistic represents every country worldwide and not just the select countries and regions.

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/truvalidate

TransUnion