TransUnion

TransUnion 2024 State of Omnichannel Fraud Report

Trends and insights for enabling trusted commerce

Introduction

Now more than ever, knowing the identity of the person you're dealing with is central to every organisation's fraud prevention strategies. Capitalising on continued growth in digital transactions globally following the pandemic, fraud reached new heights in 2023. Cybercriminals are stealing more identity information from organisations and individuals to commit account takeover (ATO), instigating third-party fraud or creating fraudulent accounts — including a record number of synthetic accounts — to perpetrate first-party fraud. Consumers reacting to a very real threat are relying on companies to protect their personal data, selecting brands based on perceived security. Organisations demonstrating safety and convenience in their omnichannel experiences through friction-right fraud detection and prevention capabilities to build consumer trust stand to win.

In the 2024 State of Omnichannel Fraud Report, TransUnion brings together trends, benchmarks, and identity and fraud expertise from across our organisation. It provides insight to those responsible for preventing fraud and streamlining customer experiences to deliver better business outcomes. Use this report to evaluate current fraud prevention programs in the context of the broader market. Share this information across your organisation with the goal of increasing customer satisfaction, reducing fraud and improving business performance.

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

KEY TAKEAWAYS

Identity takeover fuelled fraud risk

15%
increase in US data breaches from 2022 to 2023 and +157% from 2020 to 2023; breach severity increased 11% from 2022 to 2023

54%
of consumers in 18 select countries and regions reported being targeted with online, email, phone call or text messaging fraud attempts from Sept. to Dec. 2023

Digital Fraud outpaced transaction growth

5%
of all global digital transactions were suspected Digital Fraud in 2023, with volume of suspected Digital Fraud increasing 14% over 2022

105%
growth in the volume of suspected Digital Fraud from 2019 to 2023, outpacing the 90% increase in digital transactions overall

Account creation posed high risk across channels

13.5%
of all global digital account creation transactions in 2023 were suspected Digital Fraud

$3.1 billion
in lender exposure to suspected synthetic identities for US auto loans, bank credit cards, retail credit cards and unsecured personal loans originated at the end of 2023 (highest level ever; percentage of synthetic identities among accounts opened also highest ever)

Contents

TransUnion

Consumer Mindset

Honouring expectations for security and convenience is a winning strategy

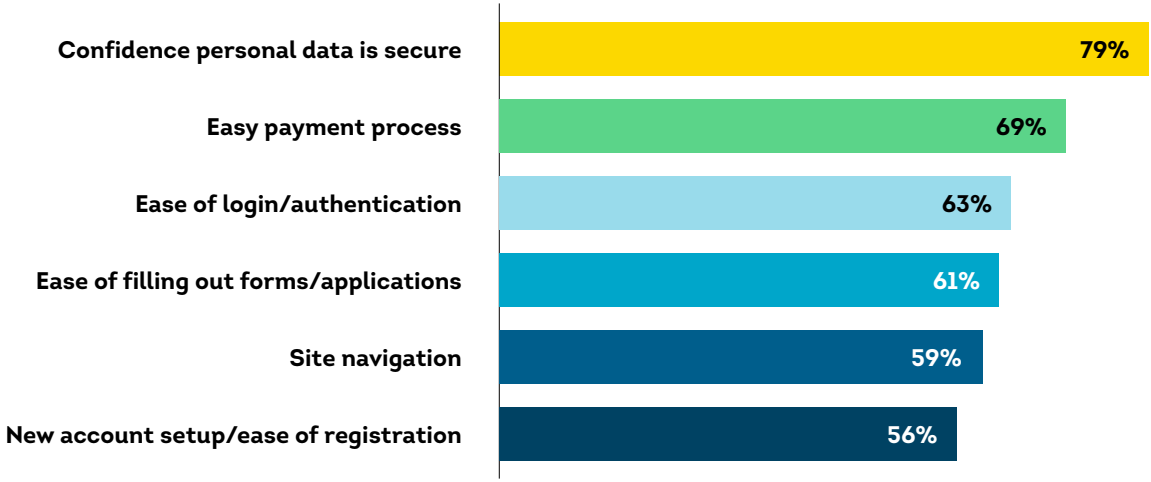
Consumers have high expectations for organisations to protect their identities while delivering convenient experiences. In fact, 59% of consumers reported they're likely to switch companies to get a better digital experience. Yet, consumers ranked personal data security (50%) as the top reason to do business with an online company. Furthermore, 93% said confidence their personal data will not be compromised is most important when choosing who to transact with online with 79% saying it's very important.

Ranked Expectations or Qualities in Preferred Online Companies

Top answer chosen

Stated Important Features When Choosing Whom to Transact With Online

Very important



Source: TransUnion consumer fraud survey

TransUnion

Trust and safety critical to online conversion rates

Organisations need to ensure omnichannel experiences are perceived as safe and secure or risk losing customers. Fewer (34%) consumers reported conducting more than 50% of their transactions online in 2023, down from 36% in 2022 and 45% in 2021. While the drop may be due to more physical locations being open following the global pandemic, it may also be in response to increased fraud risk awareness.

Two-thirds (65%) of consumers reported fraud concerns were the top reason they wouldn't use a site again, up from 63% in 2022. Half of consumers reported abandoning an online shopping cart due to concerns about fraud and/or security. While most (52%) people have abandoned financial and insurance online applications, their reasons spanned safety and ease: Too much information requested (48%); didn't trust their personal data would be secure (41%); and too much time to complete (37%) were the top reasons for abandonment.

Top Reason Consumers Said They Abandoned Online Application or Form for a Financial or Insurance Product

Source: TransUnion consumer fraud survey

Identity Data Exposure Trends

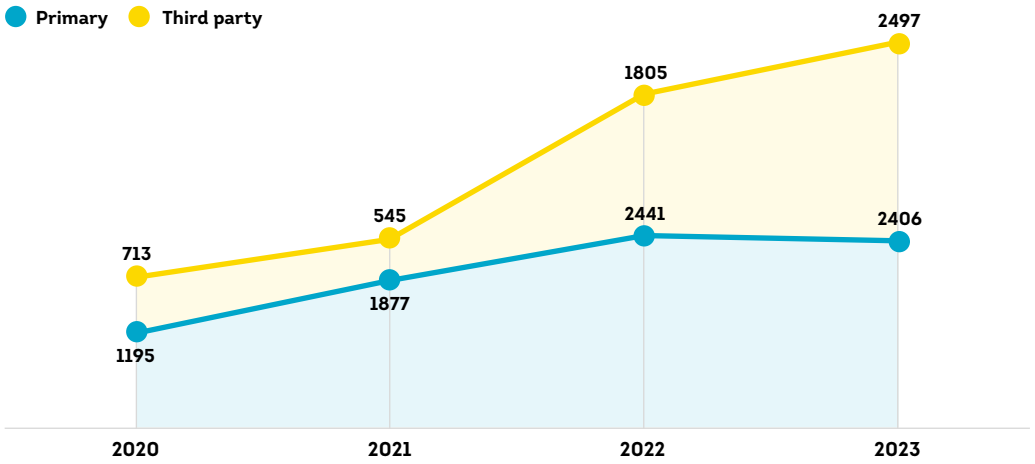
Identity data or personally identifiable information (PII) is a core target of cybercriminals. They're using all means possible, targeting organisations and consumers alike, to harvest identity credentials to fuel fraud schemes. More than half (54%) of all consumers said they were targeted by fraudulent email, online, phone call or text messaging scams in the last three months. In addition, reported data breaches and their severity reached historic highs in the US.

US data breaches reached record volume and severity

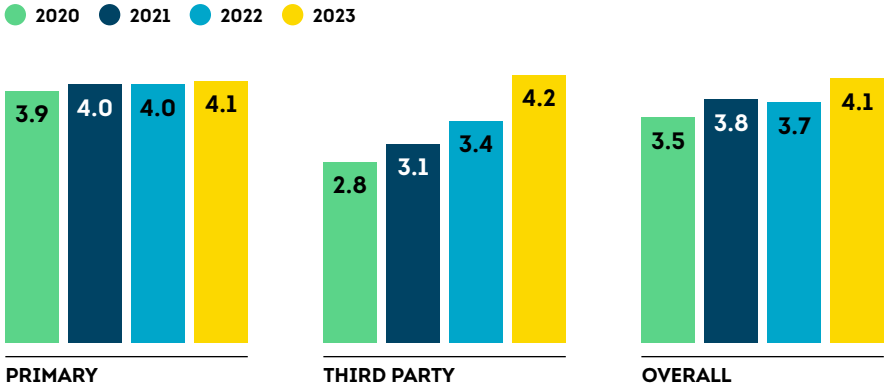
Data breaches are a leading indicator of future fraud as cybercriminals steal credentials in unprecedented numbers. US data breaches increased 15% year over year (YoY) in 2023 to a volume never seen before — driven by a 38% YoY increase in third-party breaches. In addition, the average breach risk severity (the ability of a breach to enable identity fraud) as measured by TransUnion TruEmpower™ Breach Risk Score (BRS) increased 11% YoY to 4.1 in 2023, also the highest ever measured.

Cybercriminals zeroed in on third-party service providers as the largest data breach vector — surpassing primary breaches for the first time in 2023. Not only were there more third-party breaches, they were also more severe with an average BRS 24% higher than 2022.

US Data Breach Volume



Average Breach Risk Score for US Data Breaches



A primary data breach represents a direct attack on an organisation. A third-party data breach, also known as a supply-chain attack, value-chain attack or backdoor breach, is when an attacker accesses an entity's network via third-party vendors or suppliers — payroll processing or medical billing, for instance.

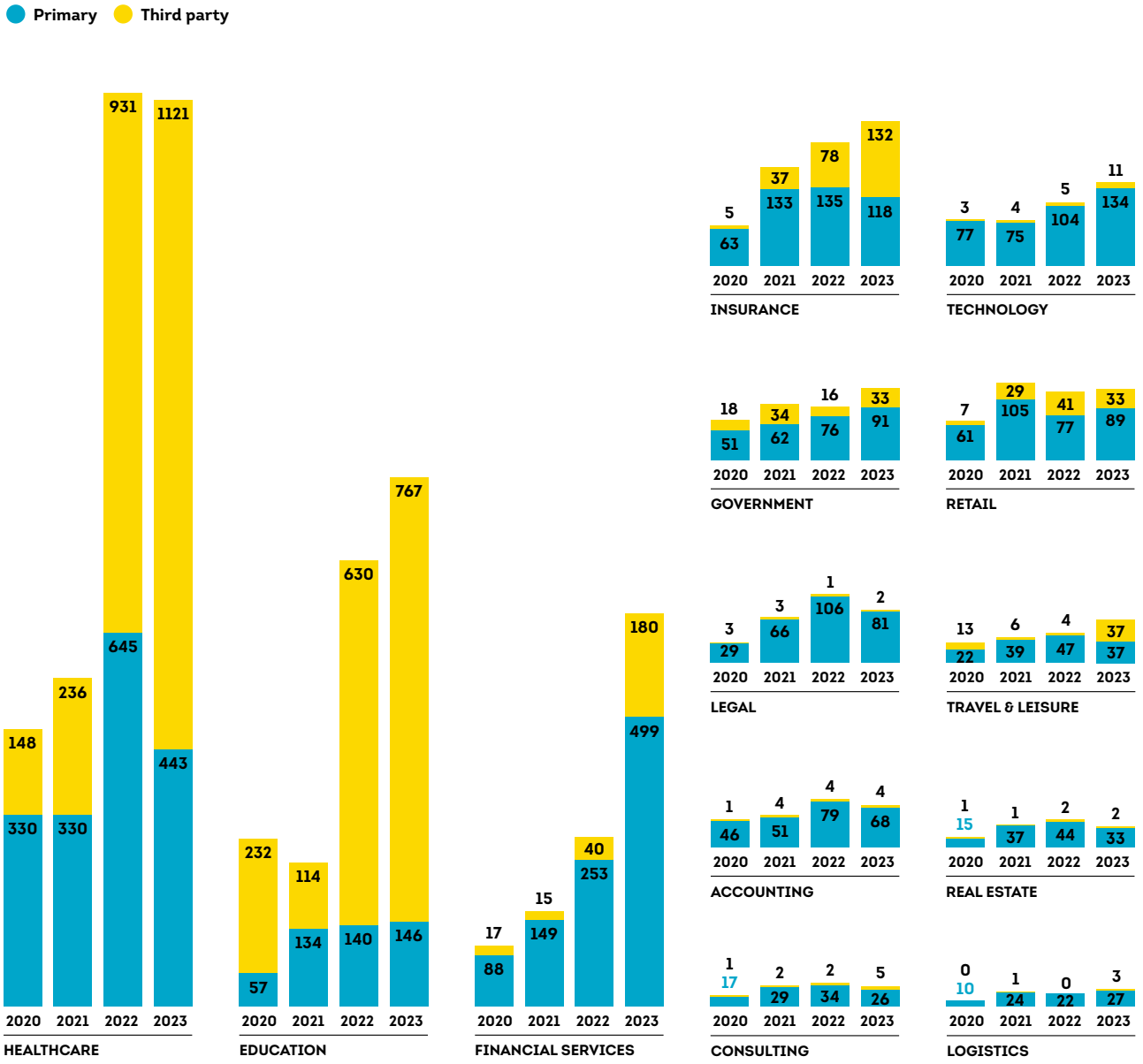
Source: TransUnion TruEmpower

TransUnion

Healthcare and education experienced the most data breaches

For the second year in a row, healthcare experienced the highest number of breaches followed by education. Despite the highest volume occurring in healthcare, the most severe breaches occurred in education (5.6 BRS) and insurance (4.9 BRS).

US Data Breach Volume by Industry 2023



Note: Reporting changes at the New York State Attorney General Office increased the number of breaches reported in financial services in 2023.

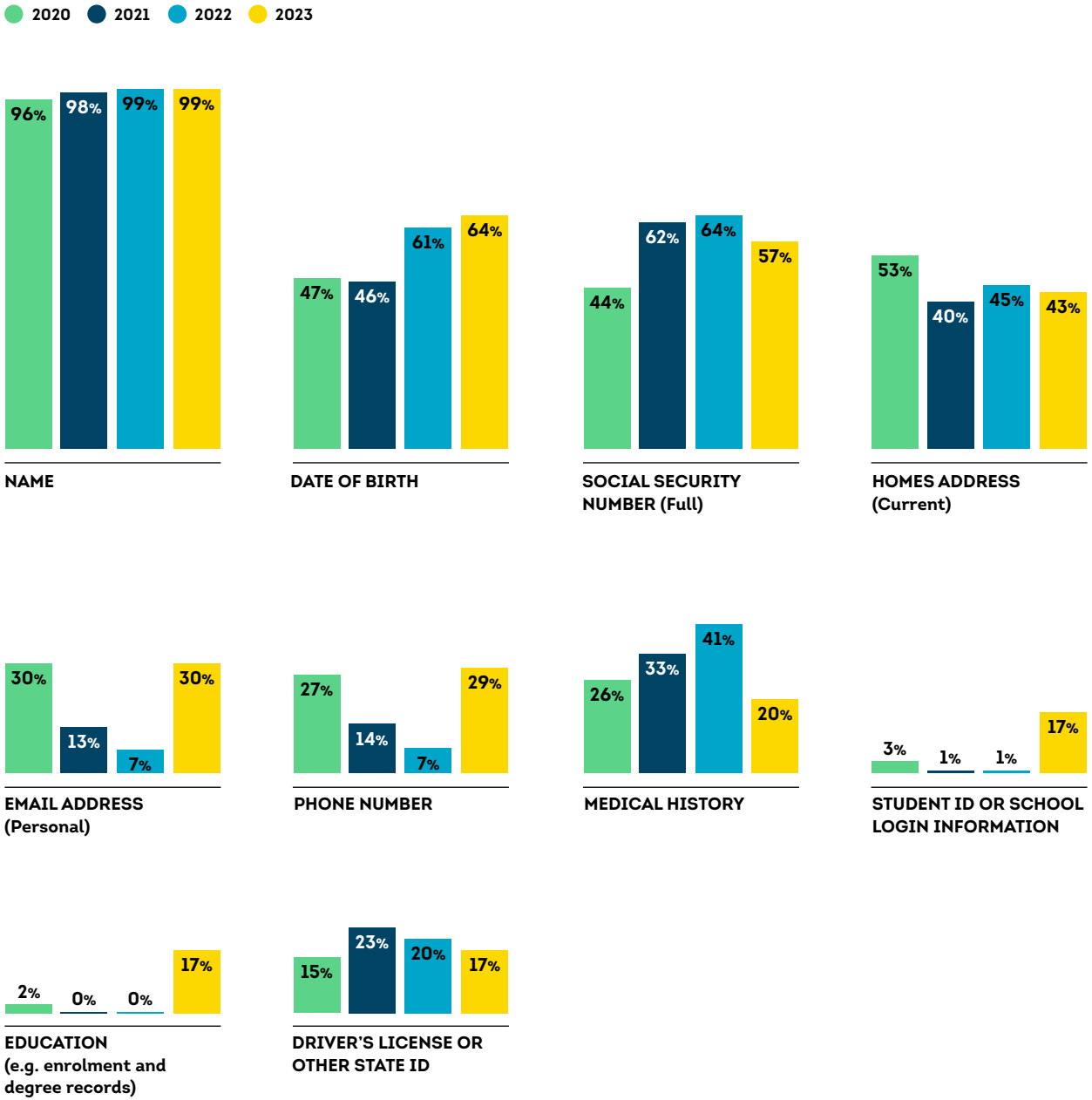
Source: TransUnion TruEmpower

TransUnion

Core identity credentials are the target of data breaches

Cybercriminals continued to breach organisations' systems to steal consumer identity credentials, including date of birth, full Social Security number and home address, required to open fraudulent accounts and create synthetic identities. They also sought credentials like email address, phone number and student ID or school login information to possibly enable account takeover and consumer scams.

Top 10 Exposed Identity Credentials in US Data Breaches 2023



Source: TransUnion TruEmpower

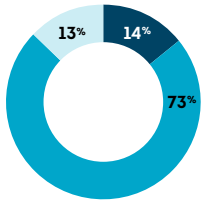
Consumers regularly targeted with scams to gain access to accounts or deception to steal funds

More than half (54%) of consumers reported being targeted by an email, online, phone call or text messaging fraud scheme, and 11% said they fell victim from Sept. to Dec. 2023. Among those who said they were targeted, phishing (fraudulent emails, websites, social posts, QR codes, etc. meant to steal data) at 33%; smishing (fraudulent text messages meant to trick you into revealing data) at 29%; and vishing (fraudulent phone calls meant to trick you into revealing data) at 27% were the leading types of fraud consumers reported experiencing.

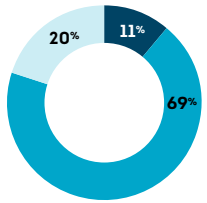
Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from Sept. to Dec. 2023, and the most frequent scheme by which they reported being attacked

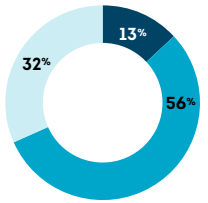
- **Targeted and fell victim**
- **Targeted but didn't fall victim**
- **Not targeted**
- **Most reported fraud scheme**



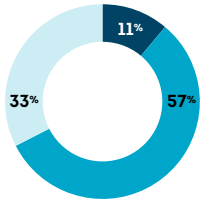
KENYA
Smishing



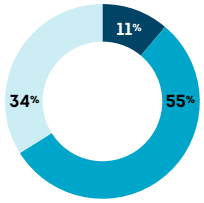
ZAMBIA
Smishing



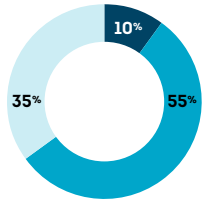
SOUTH AFRICA
Money Mule



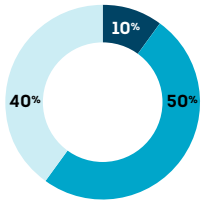
PHILIPPINES
Phishing



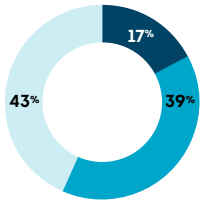
RWANDA
Money Mule



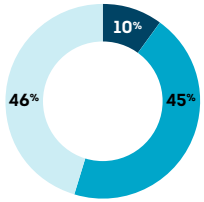
NAMIBIA
Phishing



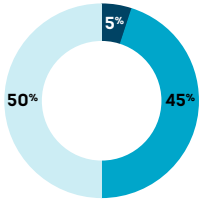
CANADA
Phishing



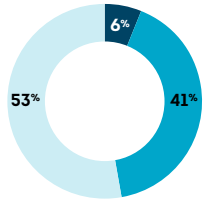
INDIA
Phishing



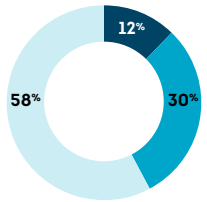
UNITED STATES
Phishing



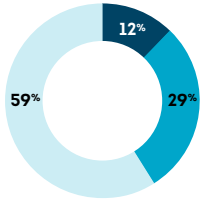
HONG KONG
Phishing



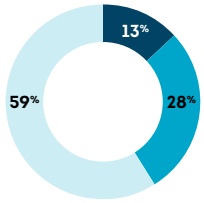
UNITED KINGDOM
Phishing



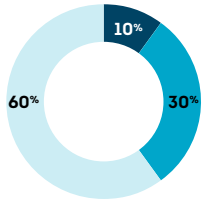
MEXICO
Stolen Credit Card



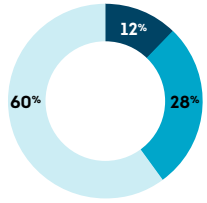
CHILE
Vishing



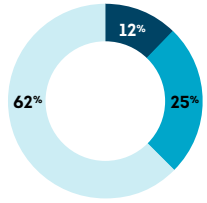
PUERTO RICO
Stolen Credit Card



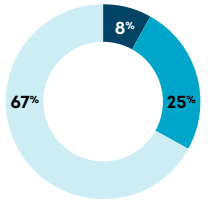
BRAZIL
Stolen Credit Card



COLOMBIA
Vishing



DOMINICAN REPUBLIC
Stolen Credit Card



SPAIN
Stolen Credit Card

Source: TransUnion consumer fraud survey

TransUnion

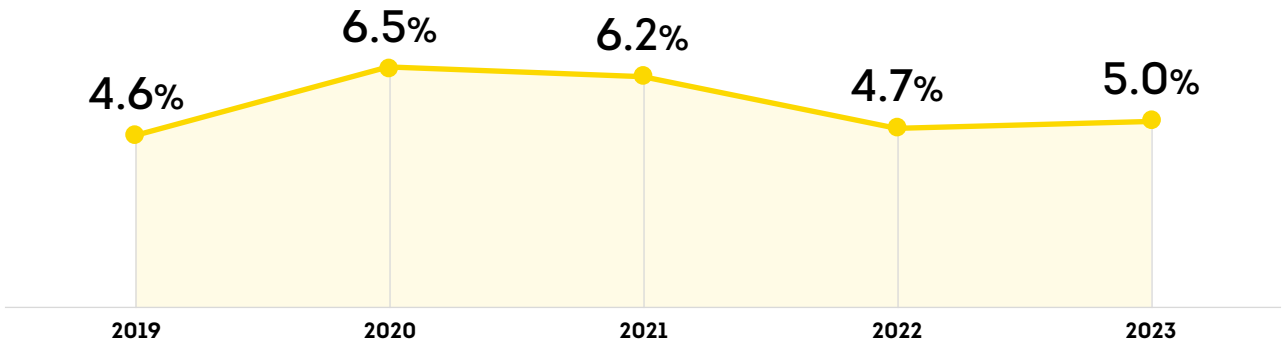
Global Digital Fraud Trends

Suspected Digital Fraud rates rose along with digital transaction volume

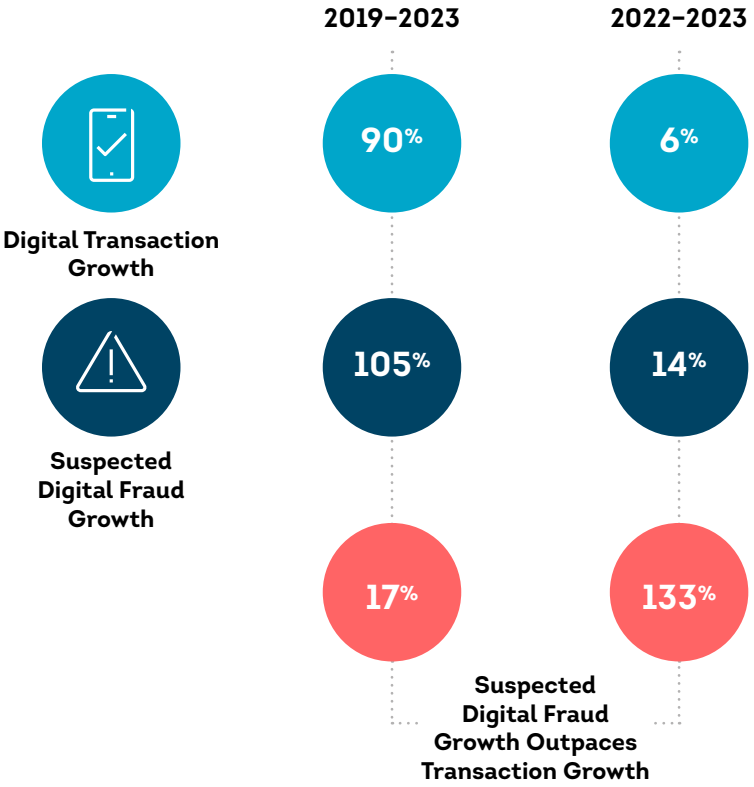
Digital Fraud continued to grow while the rate of fraud was slightly higher than pre-pandemic levels globally. The rate of suspected fraudulent digital transactions globally rose to 5% in 2023, 6% higher than 2022. The volume of suspected Digital Fraud globally grew faster than the actual number of transactions worldwide as well. In 2023, the volume of suspected Digital Fraud increased 14% compared to 2022 (+6% for all transactions) and 105% compared to 2019 (+90% for all transactions). Suspected Digital Fraud growth outpaced digital transaction growth by 133% from 2022 to 2023 and 17% from 2019 to 2023.

For transactions where the consumer or fraudster was in the US, the rate and volume of risky digital transactions was relatively unchanged from 2022 to 2023 (-1% and +1%, respectively) but increased significantly from pre-pandemic levels from 2019 to 2023 (+16% and +124%, respectively). Of the 19 markets included in this year's analysis, about half (Brazil, Botswana, Canada, Colombia, the Dominican Republic, India, Namibia, Rwanda, Spain and Zambia) saw an increased rate of suspected Digital Fraud YoY in 2023. However, only five markets (Brazil, Canada, Hong Kong, India and the Philippines) had suspected Digital Fraud rates above the global average of 5% in 2023.

Rate of Suspected Digital Fraud



Growth in Volume of Suspected Digital Fraud Compared to Digital Transactions Globally



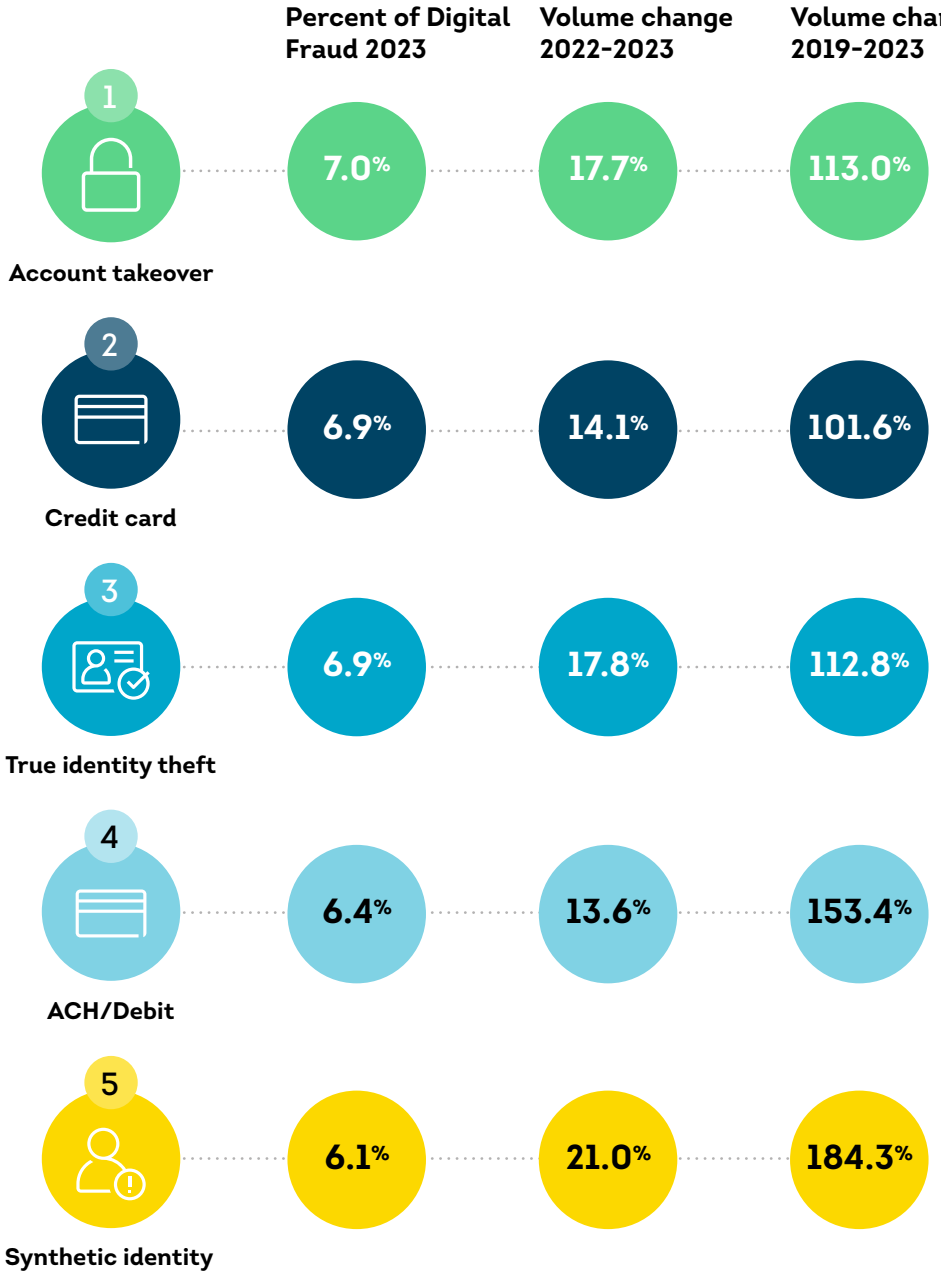
Source: TransUnion TruValidate™

TransUnion

Account takeover topped list of most common fraud types

ATO accounted for 7% of Digital Fraud globally in 2023, slightly surpassing credit card fraud which was the top type of Digital Fraud reported to TransUnion by its customers in 2022. However, synthetic identity fraud was the fastest growing Digital Fraud type in 2023, rising to 6.1% globally from 5.3% in 2022, and 21% volume-wise year over year and 184% from 2019 to 2023.

Top Fraud Types and Their Growth



Source: TransUnion TruValidate

TransUnion

Retail experienced the highest Digital Fraud rates

The retail industry experienced the largest percentage (8.7%) of suspected fraudulent digital transactions globally in 2023, a 21% increase over 2022, and 34% growth in suspected Digital Fraud volume year-over-year. Promotion abuse was the most reported type of Digital Fraud for retail transactions. Despite retail's overall exposure to fraud, gaming (online gambling) experienced the highest rate of suspected fraudulent transactions in 2023 in the most (six) markets analysed: Colombia, the Dominican Republic, Kenya, Puerto Rico, Spain and the US.

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%

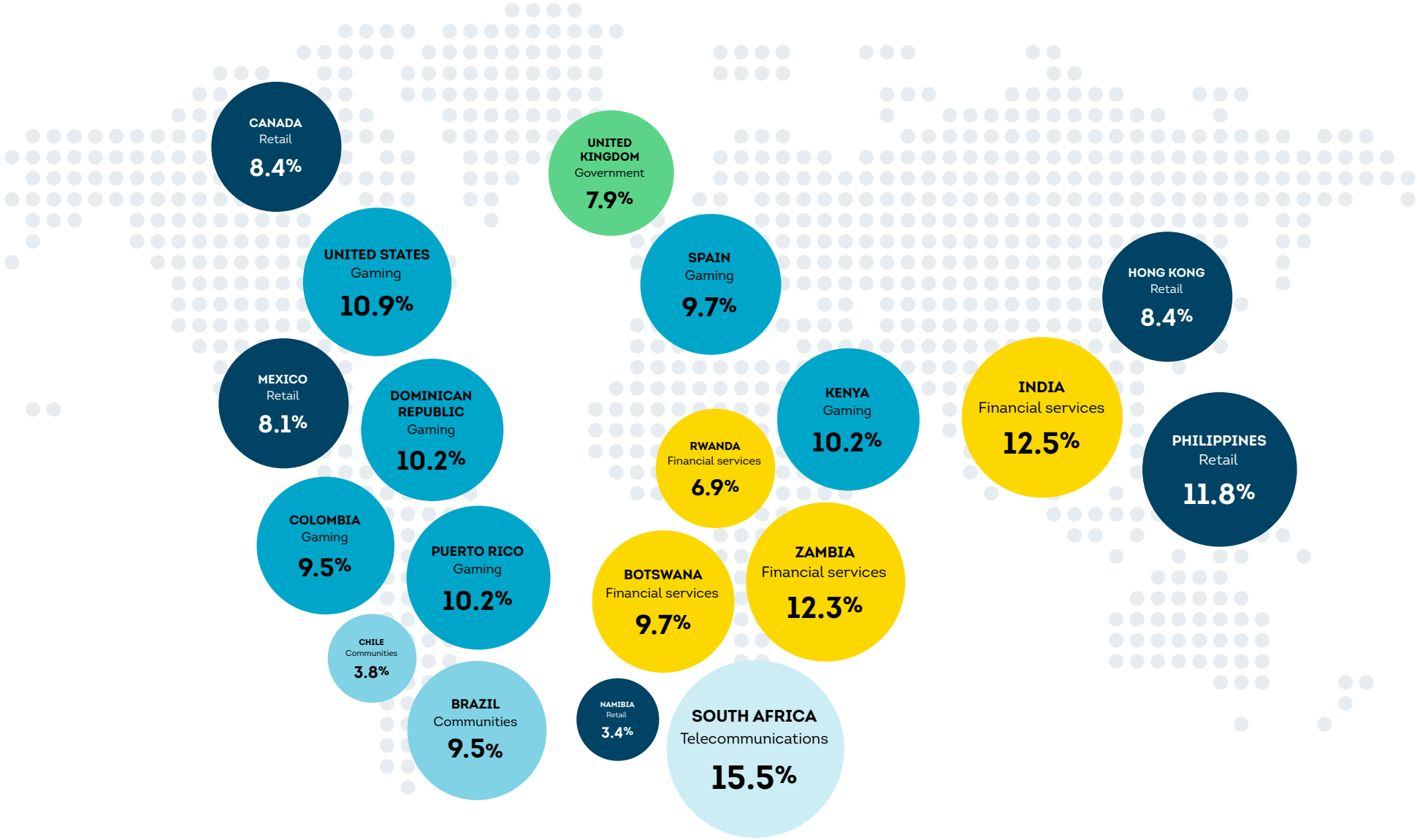
Logistics

2023
0.9%
Shipping fraud
2022-2023
-43.9%

Source: TransUnion TruValidate

Digital Fraud Attempts by Region and Industry 2023

The industry with the highest rate of suspected Digital Fraud where the consumer is located in that region during the transaction



Source: TransUnion TruValidate

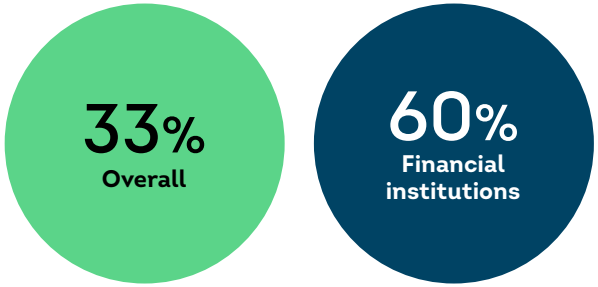
Call Centre Fraud Trends

Call centres play an important role in an omnichannel customer experience — representing a high-trust touchpoint for consumers who are being exploited in multiple ways. Fraudsters have increased their attacks on call centres to access credentials and take over customer accounts. Fraudsters are also facilitating ATO using outbound call spoofing to scam consumers into giving up their account credentials. Not surprisingly, a third (33%) of organisations TransUnion surveyed considered the call centre a top source of ATO, rising to 60% for financial institutions.

High-risk calls into call centres rose rapidly

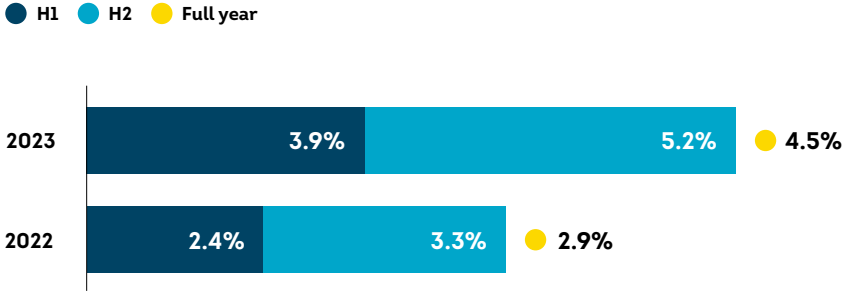
TransUnion documented a 55% increase in the percentage of high-risk calls into US call centres from 2022 to 2023 from 2.9% to 4.5%. In just a half year, TransUnion found high-risk calls into US call centres increased 33% from 3.9% in H1 to 5.2% in H2 2023.

Percent of US Organisations that Believed Account Takeover Starts in the Call Centre



Source: TransUnion 2023 State of Omnichannel Authentication Report

High-Risk Calls Into Call Centres



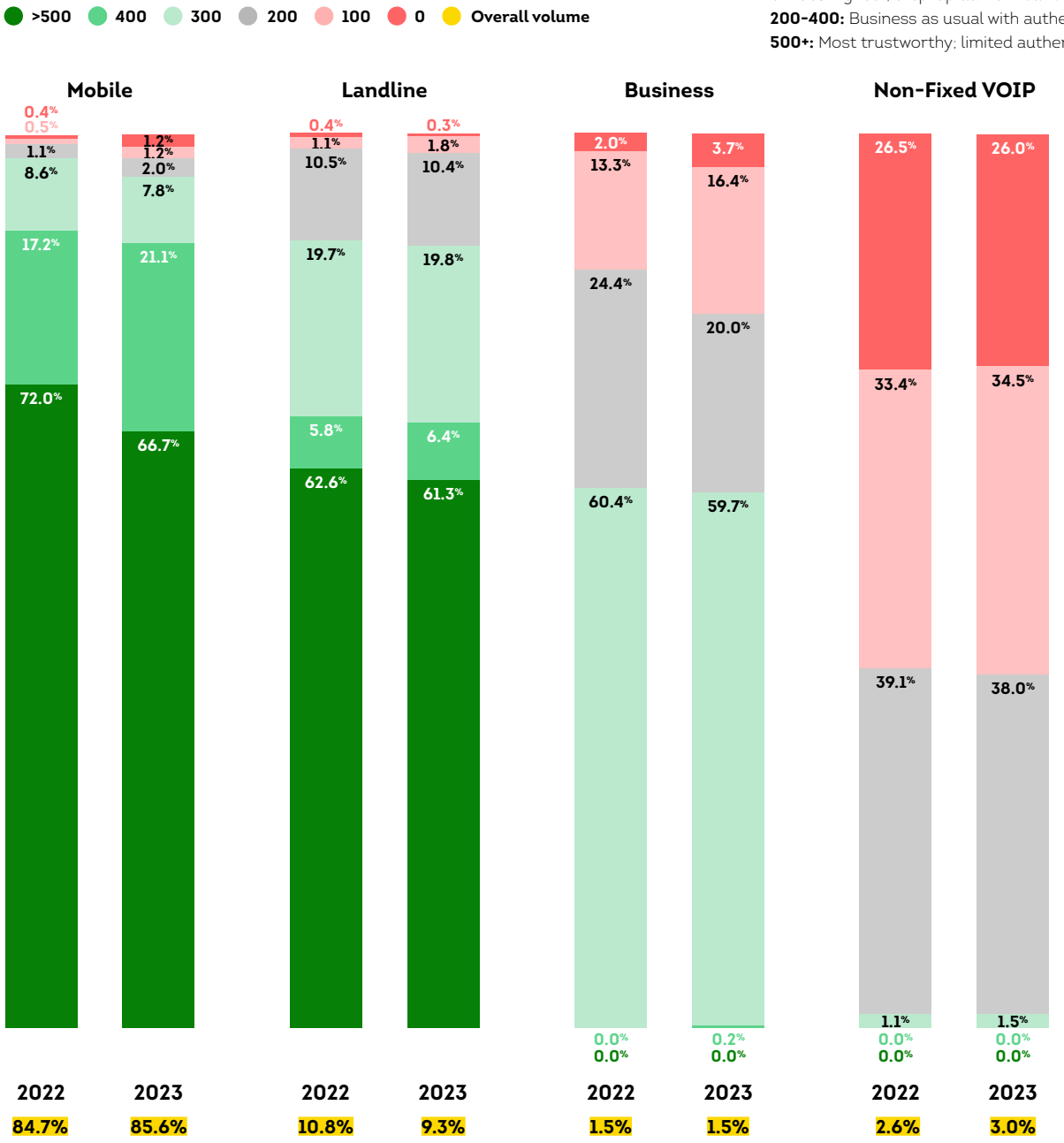
H1 is Jan. 1 to June 30 and H2 is July 1 to Dec. 31

Source: TransUnion TruValidate

Virtual calls pose highest risks to call centres

While TransUnion documented the vast majority (86%) of calls received by its US call centre customers were from mobile phones in 2023, only 2.4% of those calls were identified as being high risk for fraud. The percentage of risky calls made from mobile phones into US call centres rose from 2022 when it was 0.9% in 2023. The riskiest channel for the call centre was non-fixed Voice over Internet Protocol (VoIP), a phone number that isn't associated with a physical device. While that channel represented only 3% of total call volume in 2023, 61% of those calls were identified as high risk for fraud. Nearly the same percentage of non-fixed VoIP were considered high risk in 2022.

US Call Centre Risk by Channel and Overall Volume



Call risk score tiers

0–100: Highest; step-up authentication
200–400: Business as usual with authentication
500+: Most trustworthy; limited authentication

Source: TransUnion TruValidate

TransUnion

New Account Creation Digital Fraud Risk

Account creation presents highest risk stage in customer journey

Organisations and consumers face risk, both fraud and policy driven, across the omnichannel experience. Looking at risk by customer journey stage, of particular concern is risk to new account creation. Of all digital global account creation transactions in 2023 (representing 6% of all traffic volume), 13.5% were found to be suspected Digital Fraud. The high percentage of account creation Digital Fraud contrasted with transactions more typically associated with digital fraudulent behaviour. In fact, it was more than four times higher than account login Digital Fraud which can lead to ATO, and more than five times higher than financial transactions in which money actually changed hands. This is indicative of fraudsters simply bypassing existing accounts to create new ones they control.

Customer Journey Stage Examples

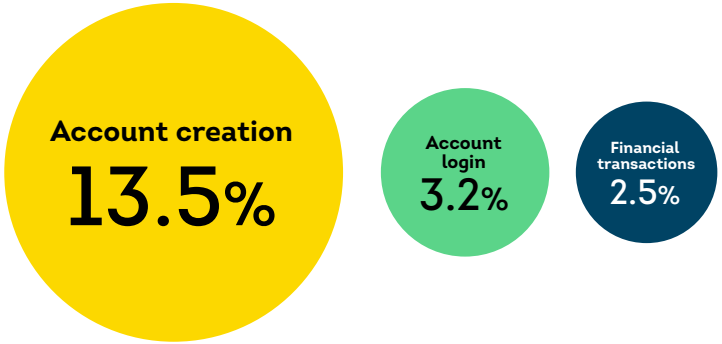
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

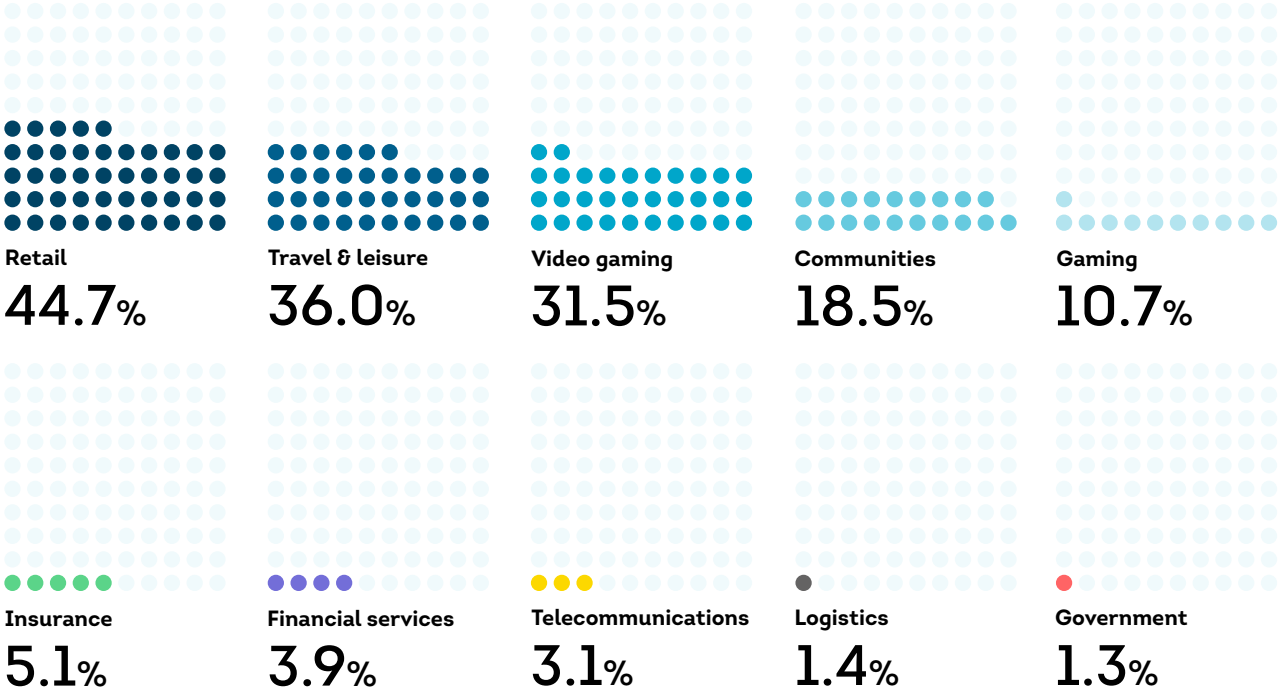
Customer Journey Transaction Type Digital Fraud Risk

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



Account Creation Digital Fraud by Industry

Percentage of digital account creation transactions in each industry globally that was suspected to be Digital Fraud in 2023



Source: TransUnion TruValidate

TransUnion

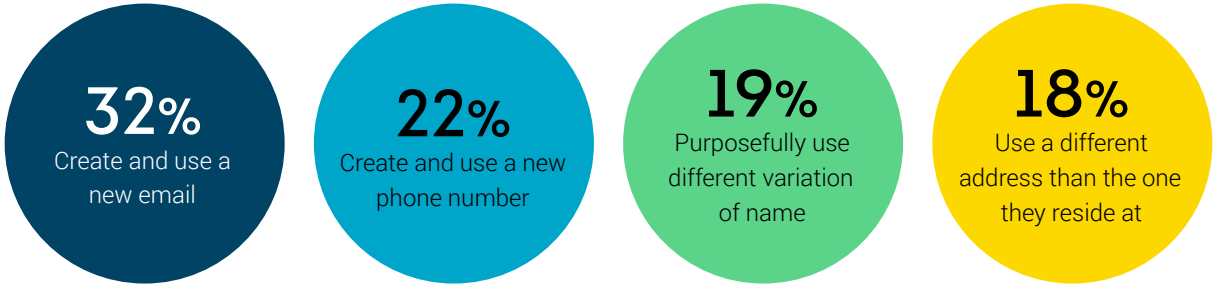
Consumers readily modify identity when creating accounts

Consumers around the world reported a willingness to modify their digital identities when establishing new accounts or applying for credit. Many retailers, online communities, media companies and services organisations require users to create an account, and consumers seeking anonymity may mask their identities when registering. This could be as simple as using a newly created email address, reporting living at an old address or altering one's name slightly.

Synthetic identity lending exposure at all-time high

With a wealth of stolen identity credentials readily available, criminals are getting very good at fabricating identities. The percentage of synthetic identities among accounts opened by US lenders for auto loans, bank credit cards, retail credit cards and unsecured personal loans reached an all-time high at the end of 2023, leaving lenders exposed to $3.1 billion in potential losses, also an all-time high and 11% more than the end of 2022. Synthetic identities among accounts opened for the four tradelines rose 17% in Q4 2023 compared to Q3 2023, reaching 0.19% at the end of 2023.

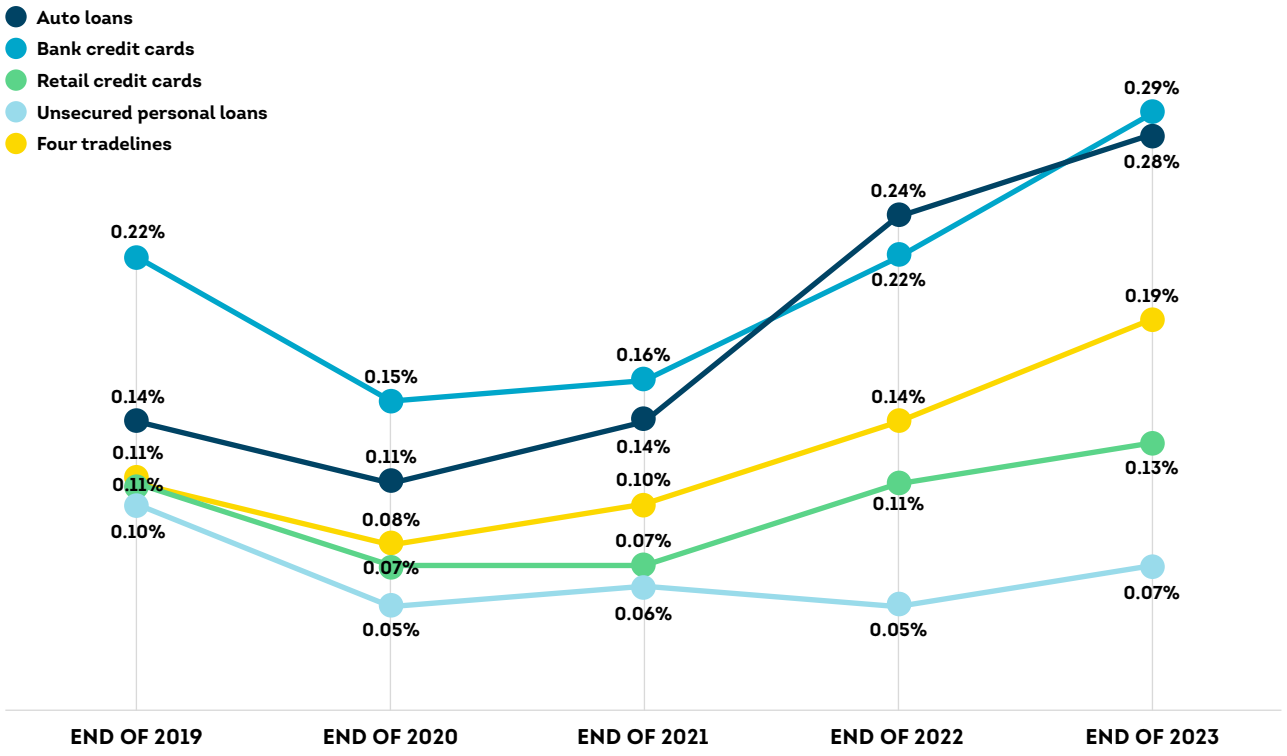
Top Ways Consumers Said They'd Modify Their Identity Attributes When Signing Up for a Product or Service



Source: TransUnion consumer fraud survey

Synthetic Identities at Account Opening

Percentage of newly opened US accounts associated with synthetic identities



Source: TransUnion TruValidate

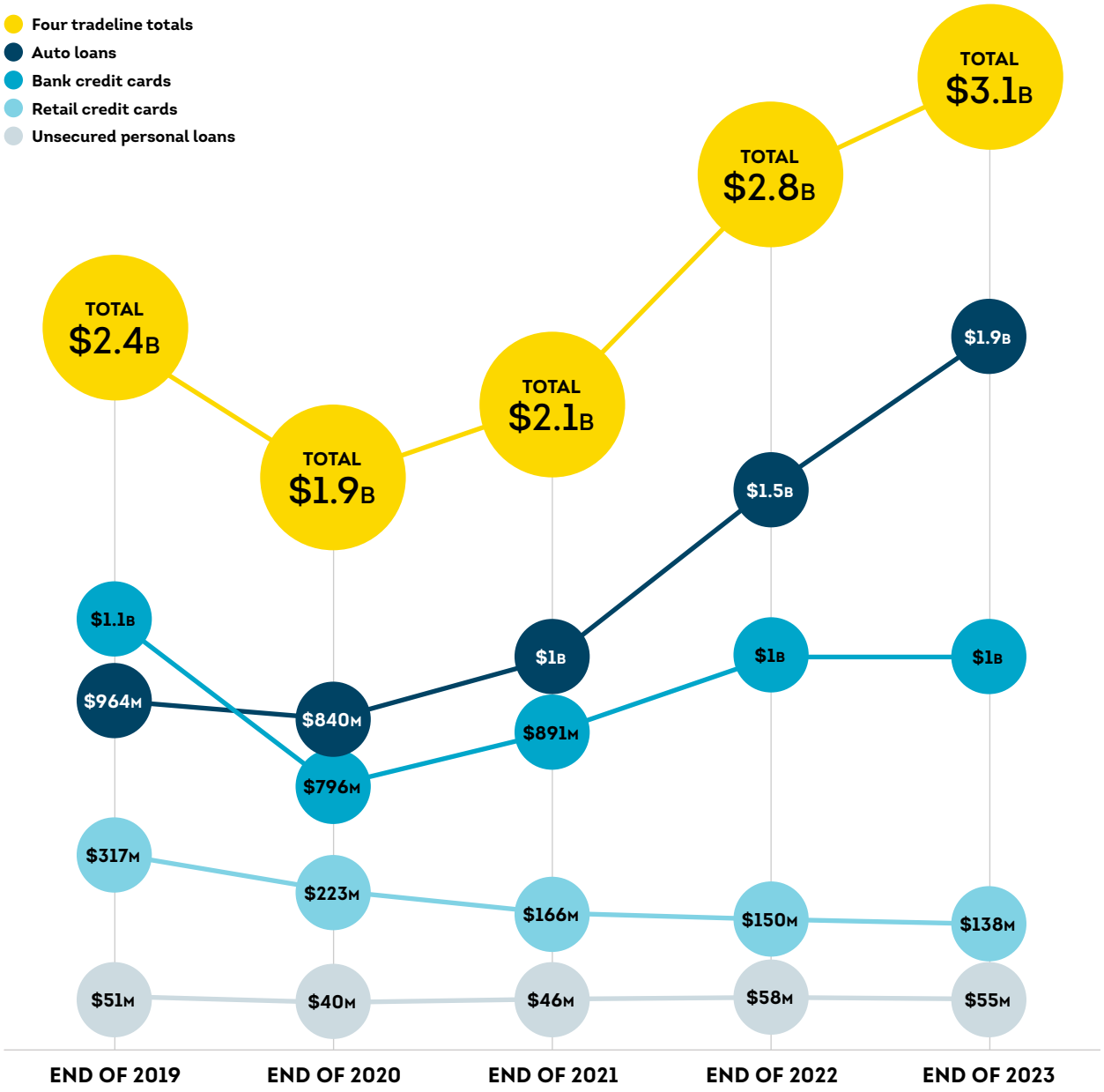
TransUnion

Auto loans high value attracting fraudsters

Based on the percentage of attempted account openings with synthetic identities, the market is facing a rising threat of charge-offs in the future. Among accounts opened using synthetic identities, auto loans appeared to be most attractive for fraudsters to stack up balances. At the end of 2023, the total lender exposure to synthetic identities for auto loans had balances of 90% more than the bankcard sector which is second among credit types analysed.

Synthetic Identities: Total Lender Exposure

The total credit amount synthetic identities have access to for US auto loans, bank credit cards, retail credit cards and unsecured personal loans



Source: TransUnion TruValidate

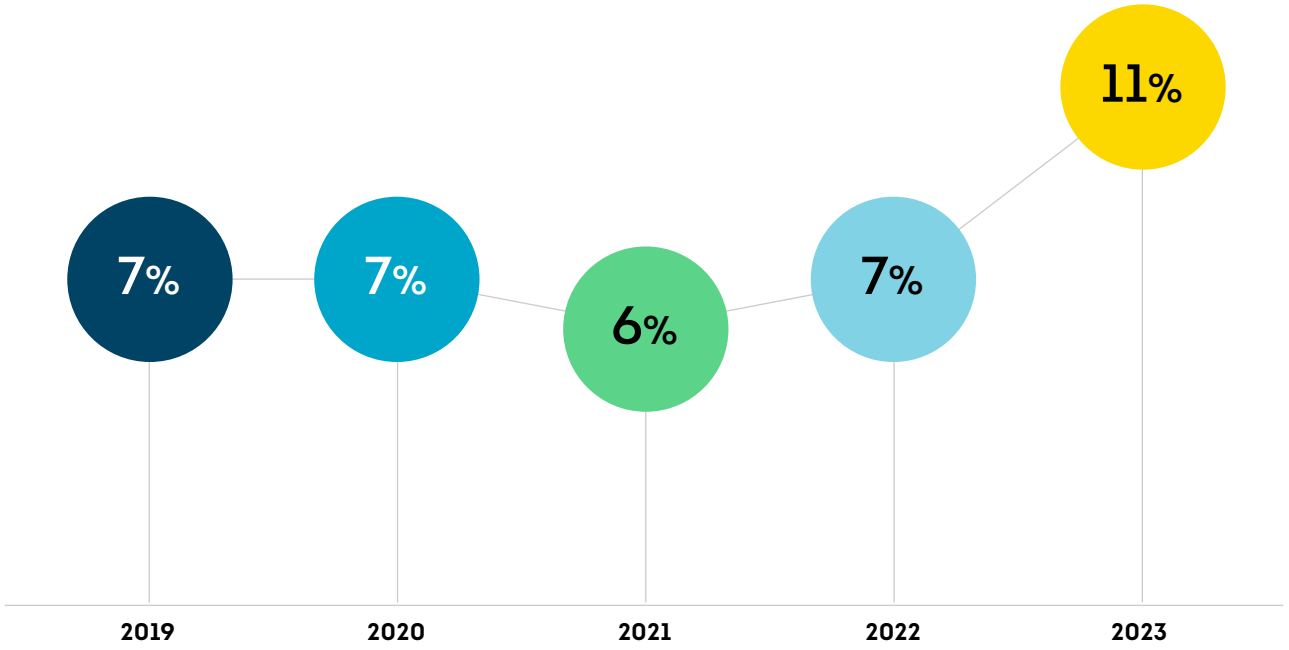
TransUnion

Credit washing extends new account opening fraud risk

As identity fraud increases, criminals who commit first-party fraud with stolen or synthetic identities may seek to recycle an identity using credit washing — a credit manipulation scam to wipe out negative information from an identity's credit history by making a false claim of identity fraud. These false credit report disputes could be made against accounts opened using a stolen consumer identity or a synthetic identity, or unauthorised transactions on a consumer's legitimate credit account.

Consumers in the US (or their authorised representatives) have a legal right to dispute records on their credit reports, and TransUnion follows a highly regulated dispute resolution process. In 2023, disputes in the US due to a fraud claim represented 11% of all disputes, the highest in five years.

US Consumer Credit Report Disputes Due to Fraud Claim as a Percentage of Total Disputes

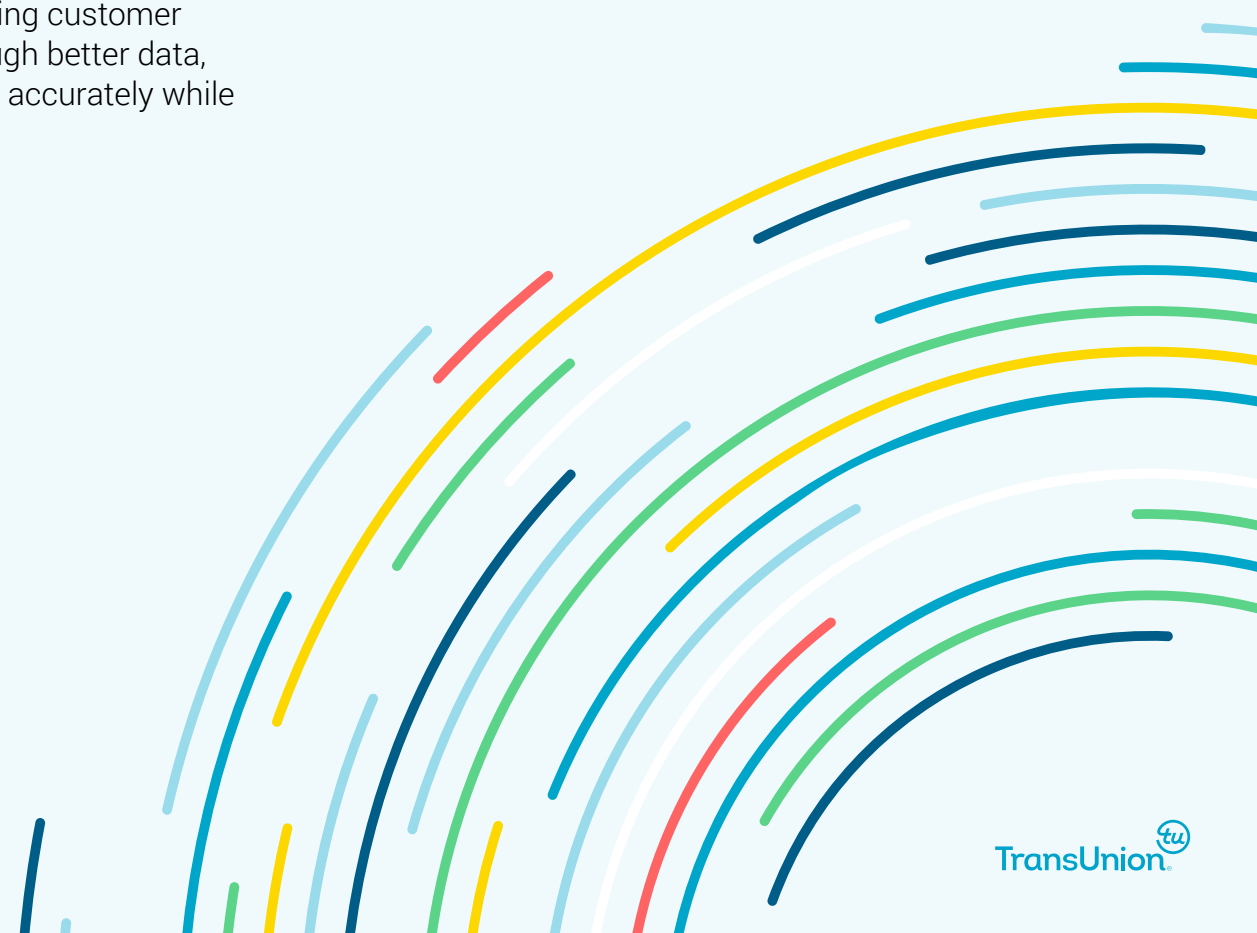


Source: TransUnion Consumer Credit

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 reach 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 good customers.



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 secure trust across channels and deliver seamless consumer experiences.

Call centre

TransUnion's call centre findings were based on data from both large and small financial institutions based in the US. The rate or percentage of high-risk calls was determined by the assessment of multiple risk factors.

Consumer credit report disputes

TransUnion's consumer credit report dispute findings were based on US consumer credit data from the US states, territories, protectorates, and US and overseas military bases. It's routinely sourced from more than 50 years of consumer credit data and contains credit information from approximately 400 million consumers.

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.

Data breaches

TransUnion TruEmpower obtains its proprietary cyber breach data in partnership with the Identity Theft Resource Center (ITRC). The ITRC staff tracks all US publicly reported data exposure events from sources that include state attorney generals breached entity press releases, law firms, cybersecurity experts and more. TransUnion expands the ITRC data with a process that computes each breach's top risks, appropriate actionable consumer steps and Breach Risk Score. The BRS is based on the quantity and severity of the particular identity credentials the affected entity determined to have been exposed. From among 60 possible identity credential choices, each breach is run through TruEmpower Identity Threat Profile to produce a risk score and pattern, and prescribed consumer actions. The Breach Risk Score uses a 1–10 scale where 1 represents least severe and 10 represents most severe.

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 determined met one of the following conditions: 1) denial in real time due to fraudulent indicators, 2) denial in real time for corporate policy violations, 3) fraudulent upon customer investigation, or 4) a corporate policy violation upon customer investigation — compared to all transactions assessed. The country and regional analyses examined transactions in which the consumer or 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.

Synthetic fraud

TransUnion's synthetic fraud findings were based on US consumer credit data from the US states, territories, protectorates, and US and overseas military bases. It's routinely sourced from more than 50 years of consumer credit data and contains credit information from approximately 400 million consumers. The synthetic fraud analysis encompasses US credit activity recorded between Jan. 1, 2009 and June 30, 2023. The lender exposure measures were based upon TransUnion's proprietary formula to capture potential total loss at risk for lenders.

About TransUnion TruValidate

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

transunionafrica.com/solution/truvalidate

TransUnion