TransUnion

H2 2024 UPDATE

STATE OF OMNICHANNEL FRAUD

Trends and strategies for protecting organisations and consumers

Introduction

Business leaders recognise they potentially face substantial revenue losses and increased operational cost due to fraud every year. Cybercriminals are stealing more identity information from organisations and individuals to open new accounts in consumers' names; creating fraudulent accounts, including a record number of synthetic accounts; or tricking consumers into sharing access to their accounts. Shifting to a threat posture that assumes consumer information is compromised, organisations that build consumer trust by enhancing their omnichannel experiences with friction-right fraud detection and prevention capabilities stand to win. That means employing enhanced identity and risk signal data, centralised fraud rules and integrated technology to ensure confidence in the authenticity of the people they're dealing with regardless of the channel.

In this State of Omnichannel Fraud Report, TransUnion brings together trends, benchmarks, and identity and fraud expertise from across our organisation. The report provides insight to those responsible for preventing fraud and securing 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, a specially commissioned TransUnion business survey in Canada, India, the UK and US, and a specially commissioned TransUnion consumer survey in 18 countries and regions globally. Throughout this report, H1 (the first half of the year) is Jan. 1 to June 30 and H2 (the second half of the year) is July 1 to Dec. 31.

KEY TAKEAWAYS

Cost of fraud posed significant financial risk to organisations

6.5%
of equivalent revenue on average lost due to fraud – representing USD$359 billion of fraud loss in the past year among 801 businesses leaders surveyed in Canada, India, and the US and UK

75%
of business leaders indicated fraud increased or stayed the same in the past year

Fraud concern remains high for businesses and consumers

5.2%
of all attempted global digital transactions were suspected Digital Fraud in H1 2024 according to TransUnion's global intelligence network

49%
of adults in 18 countries and regions said they were targeted by email, online, phone call and text messaging scams in Q2 2024 according to a TransUnion consumer survey

New account creation posed highest fraud risk

6.5%
of all attempted digital account openings globally were suspected Digital Fraud according to TransUnion's global intelligence network; this was the highest risk stage in the customer journey

USD$3.2 billion
in lender exposure to suspected synthetic identities for US auto loans, bank credit cards, retail credit cards and unsecured personal loans at the end of June 2024 (highest level ever); the percentage of synthetic identities among accounts opened in H1 2024 also highest ever according to TransUnion's global intelligence network

Contents

TransUnion

Business Leaders' Fraud Experiences

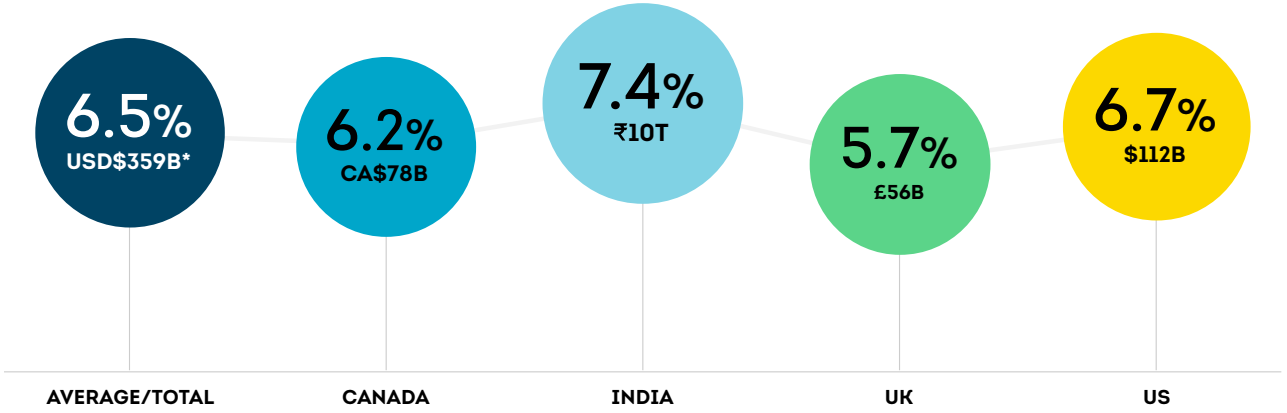
The cost of fraud

Protecting customers and their businesses from fraud is essential for the health and success of organisations. Business leaders surveyed in Canada, India, and the US and UK said on average their companies lost the equivalent of 6.5% of revenue due to fraud in the past year. That represents a total of USD$359 billion of fraud losses among the 801 businesses leaders surveyed.

Nearly a third (31%) of business leaders cited scam/authorised fraud as the most prominent cause of reported fraud losses followed by third-party fraud (17%). While 75% reported every type of fraud measured stayed the same or increased in the past year, nearly half (49%) said scam/authorised fraud increased the most; 10 percentage points higher than any other type of fraud.

Total Cost of Fraud

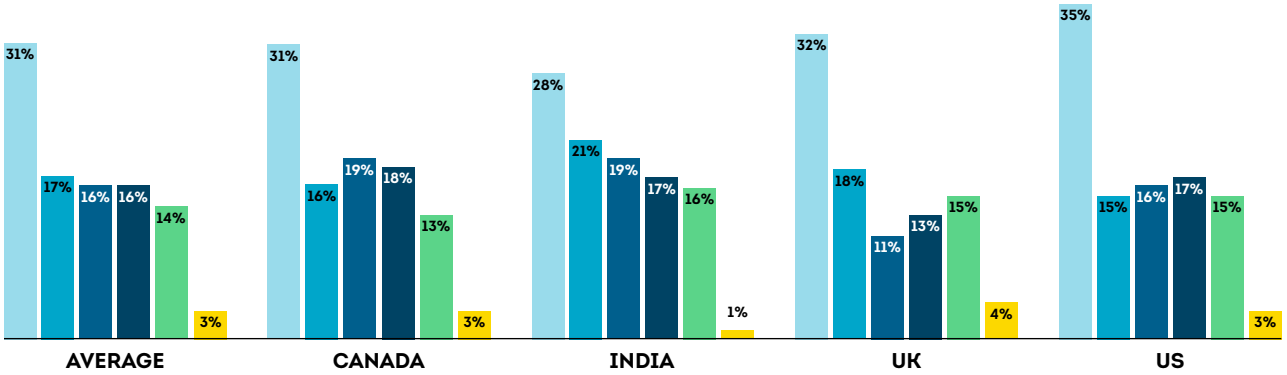
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding monetary amount



*USD conversion based on currency exchange value on Aug. 5, 2024

Most Prominent Cause of Fraud Losses

- **Scam/Authorised fraud** — Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Third-party fraud** — The use of stolen identity to open an account
- **Account takeover** — Unauthorised individuals taking over someone's online account (e.g., bank, social media, email) without their permission
- **Synthetic identity fraud** — Use of a combination of personally identifiable information to fabricate a person or entity to commit a dishonest act for financial or personal gain
- **First-party fraud** — Identity misrepresentation or falsifying information for the purpose of financial gain
- **Other**



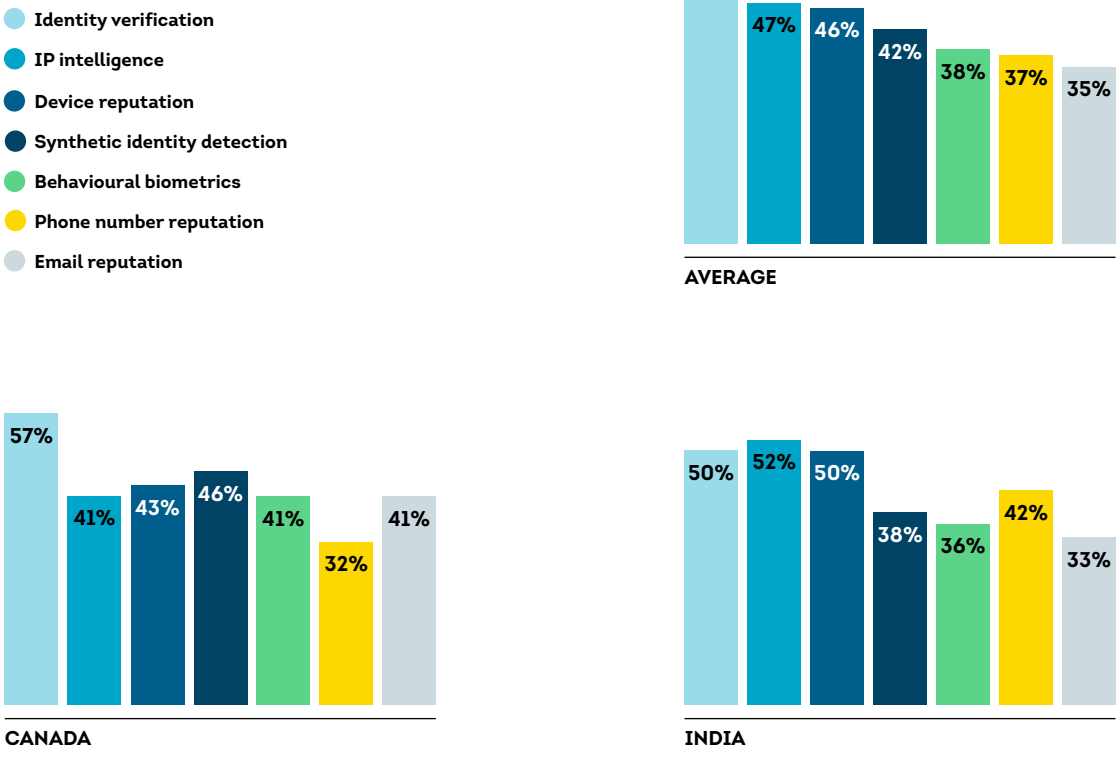
Source: TransUnion business survey

TransUnion

Most effective fraud prevention technology

Given the complexity of fraud and risk from compromised consumer identities, organisations use a variety of data, risk signals, technology and tools to prevent fraud. More than half (56%) of business leaders surveyed overall ranked identity verification as the most effective technology for preventing fraud, and nearly two-thirds (64%) of US business leaders said the same (both the highest stated percentage).

Technology Ranked as Most Effective for Preventing Fraud

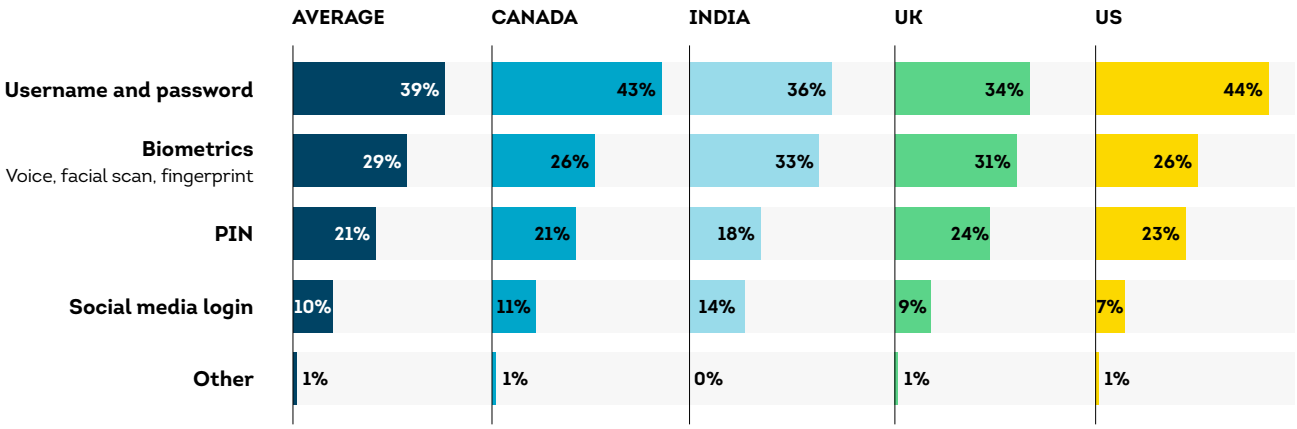


Source: TransUnion business survey

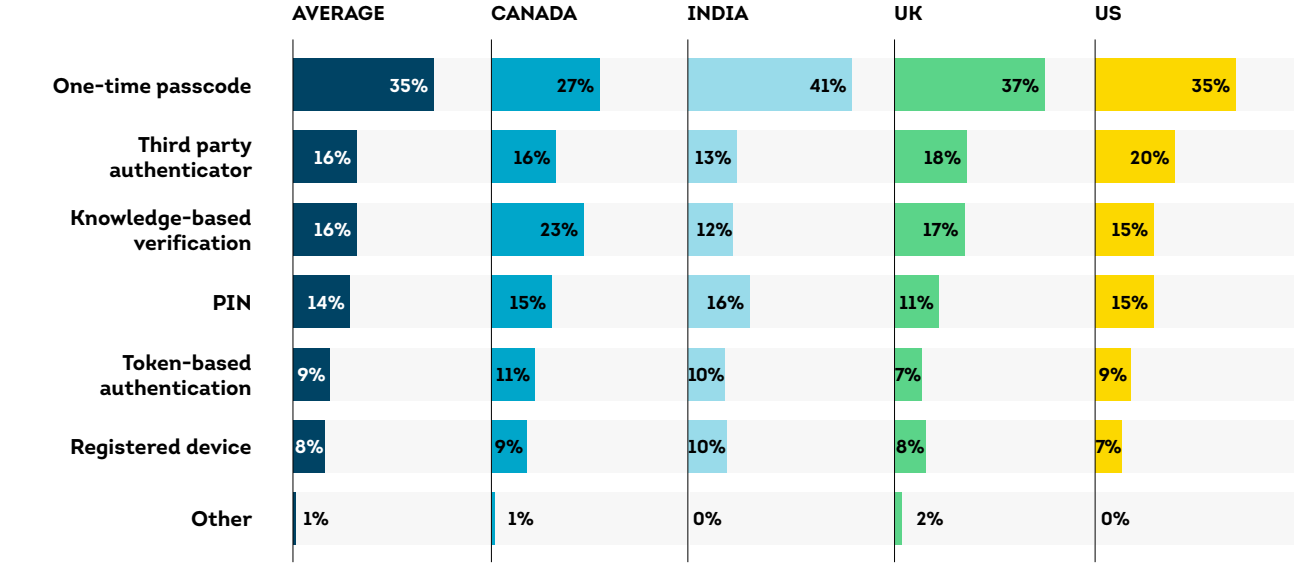
Identity authentication method utilisation

While user credentials were under threat from data breaches and consumers scams, 39% of business leaders indicated they utilise usernames and passwords as their primary methods of customer authentication — the highest percentage. Another 29% indicated biometrics as the primary method of authentication. One-time passcodes were the most popular second factor for customer authentication with 35% of business leaders indicating they utilise them.

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey

TransUnion

Identity Data Exposure Trends

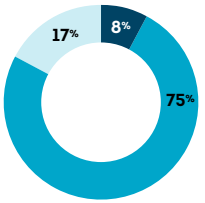
Consumers reported being regularly targeted by fraud scams

Nearly half (49%) of consumers reported being targeted by an email, online, phone call or text messaging fraud scheme, and 9% said they fell victim from Jan. to May 2024 in TransUnion's Q2 2024 Consumer Pulse Survey. However, a significant portion of the population didn't recognise potential fraud; 51% said they were unaware of being targeted by fraud schemes. Among those who said they were targeted, smishing at 37%, phishing at 34%, and vishing at 33% were the leading types of fraud consumers reported experiencing globally.

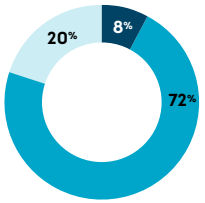
Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from Jan. to May 2024, and the most frequent scheme by which they reported being attacked.

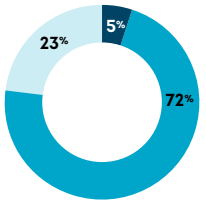
- **Targeted and fell victim**
- **Targeted but didn't fall victim**
- **Not targeted**
- **Most reported fraud scheme**



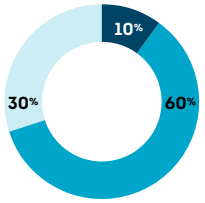
ZAMBIA
Money/Gift card scam



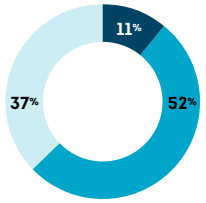
KENYA
Vishing



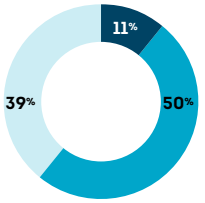
BOTSWANA
Vishing



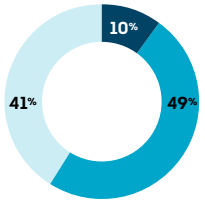
PHILIPPINES
Phishing



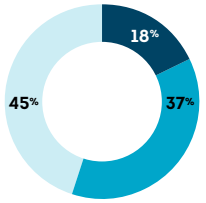
NAMIBIA
Money/Gift card scam



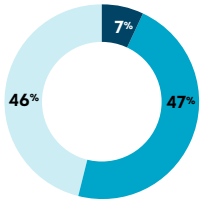
RWANDA
Money/Gift card scam



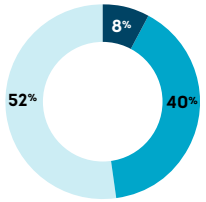
SOUTH AFRICA
Money/Gift card scam



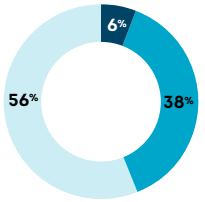
INDIA
Phishing



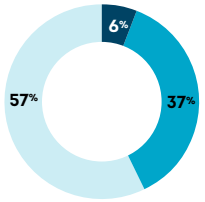
CANADA
Phishing



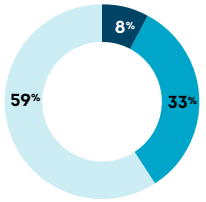
UNITED STATES
Phishing



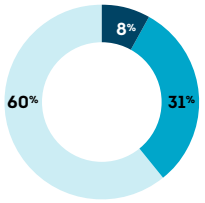
HONG KONG
Smishing



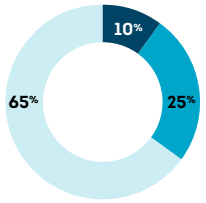
UNITED KINGDOM
Phishing



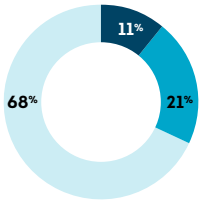
COLOMBIA
Smishing



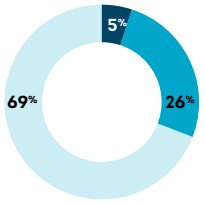
CHILE
Smishing



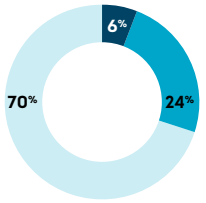
GUATEMALA
Third-party seller scam/ Smishing



DOMINICAN REPUBLIC
Stolen Credit Card



SPAIN
Smishing



BRAZIL
Stolen PIX Scam

Source: TransUnion Q2 2024 Consumer Pulse Survey

TransUnion

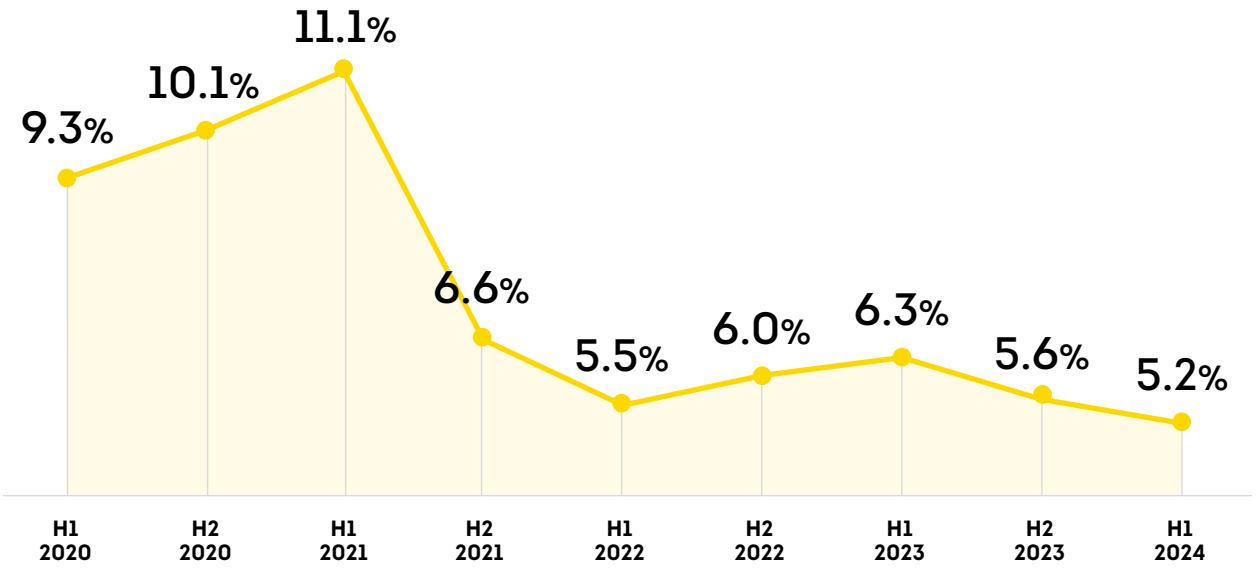
Global Digital Fraud Trends

Suspected Digital Fraud risk remained elevated

Digital Fraud continued its historic, wave-like pattern but remained stubbornly high. The rate of suspected Digital Fraud globally among TransUnion TruValidate® customers fell to 5.2% in H1 2024 from 5.6% in H2 2023 and 6.3% in H1 2023. As seen in previous reports, the risk of Digital Fraud varied by country where the consumer was located when attempting to transact, industry and transaction type.

Of the 19 markets where we provided country and regional breakdowns, seven (Brazil, Canada, Chile, Colombia, India, Mexico, and the Philippines) saw an increased rate of suspected Digital Fraud YoY in H1 2024. In addition, seven markets (Brazil, Canada, Colombia, the Dominican Republic, Hong Kong, India and the Philippines) had suspected Digital Fraud rates above the global average of 5.2% in H1 2024.

Rate of Suspected Digital Fraud

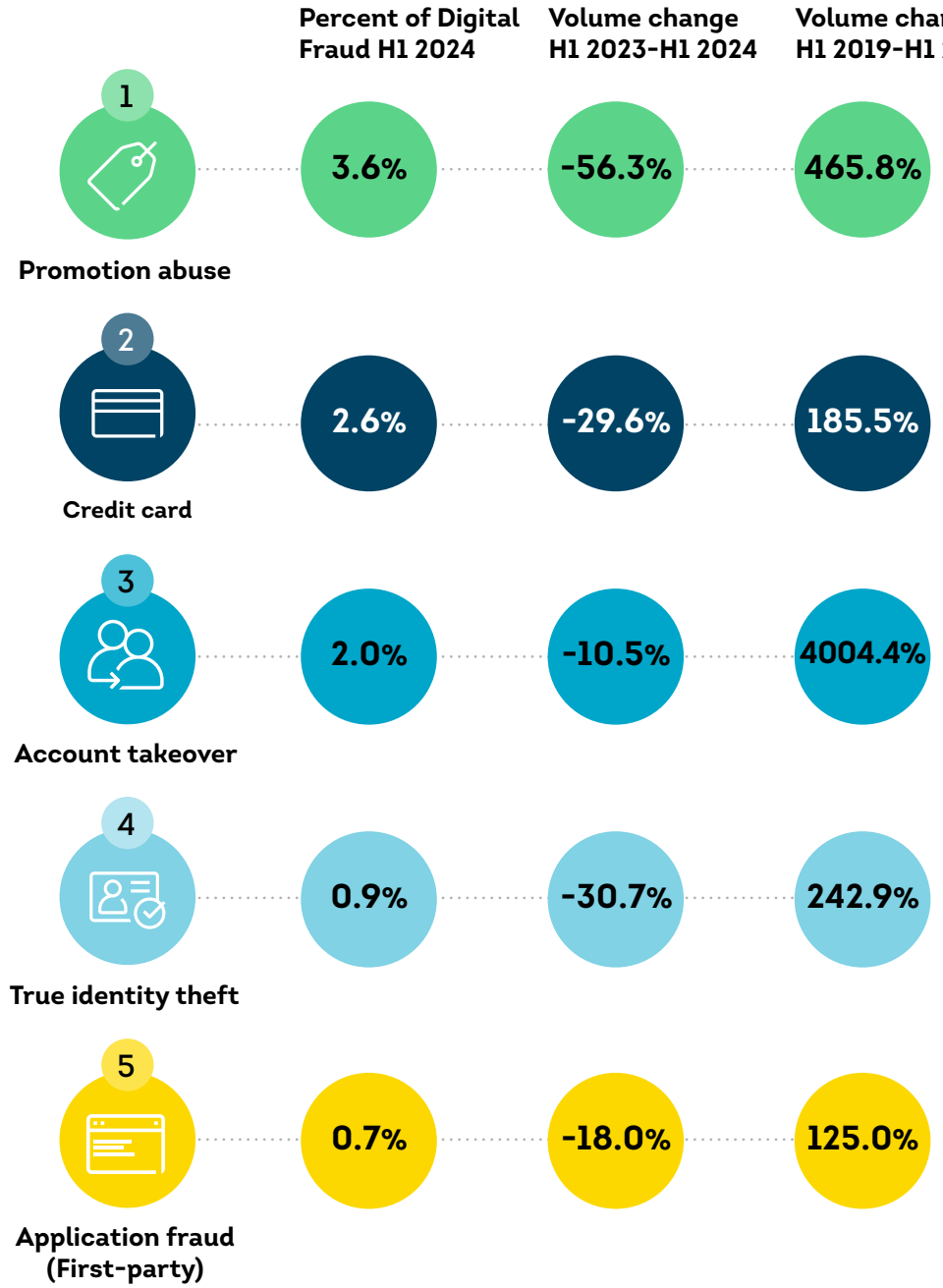


Source: TransUnion TruValidate

Promotion abuse topped list of most common fraud types

At 3.6%, promotion abuse (consumers or fraudsters taking advantage of marketing offers to receive unintended financial incentives) was the top type of Digital Fraud reported to TransUnion by its customers globally in H1 2024, about a third more than credit card fraud (2.6%). However, synthetic identity fraud (153% increase) was the fastest growing type of Digital Fraud volume-wise from H2 2023 to H1 2024, and ACH/debit payments fraud (113% increase) was the fastest growing YoY in H1 2024, according to TransUnion customers.

Top Fraud Types and Their Growth



Source: TransUnion TruValidate

TransUnion

Communities industry experienced the highest Digital Fraud rates

The communities industry, which includes web properties like online forums and dating sites, experienced the largest percentage (11.5%) of suspected Digital Fraud globally in H1 2024, according to data in TransUnion TruValidate, representing a 23% rate and 22% volume increase in suspected Digital Fraud over H1 2023. Online community users rely on organisations to provide trust and safety while using their platforms. However, communities customers of TransUnion reported profile misrepresentation as the most frequent type of Digital Fraud they witnessed in H1 2024. Not surprisingly, communities was the industry with the highest suspected Digital Fraud rate in 7 of the 19 countries and regions for which we provided breakdowns in H1 2024.

Global Digital Fraud Attempts by Industry

- **Suspected fraud attempt rate H1 2024**
- **Top fraud type H1 2024**
- **Percent change in suspected Digital Fraud volume H1 2023-H1 2024**

Communities
(online dating, forums, etc.)

H1 2024
11.5%
Profile misrepresentation

H1 2023-H1 2024
+22.3%

Video gaming

H1 2024
11.4%
Scammer/Solicitation

H1 2023-H1 2024
-6.3%

Retail

H1 2024
7.3%
Promotion abuse

H1 2023-H1 2024
-61.1%

Gaming
(online gambling, poker, etc.)

H1 2024
7.2%
Promotion abuse

H1 2023-H1 2024
-9.2%

Financial services

H1 2024
4.6%
Account takeover

H1 2023-H1 2024
-3.6%

Logistics

H1 2024
2.9%
Shipping fraud

H1 2023-H1 2024
+120.7%

Telecommunications

H1 2024
2.4%
True identity theft

H1 2023-H1 2024
-89.2%

Insurance

H1 2024
1.8%
Ghost broker

H1 2023-H1 2024
-32.4%

Government

H1 2024
1.6%
n/a*

H1 2023-H1 2024
+13.3%

*N/A - the number of customers reporting types of Digital Fraud wasn't statistically significant enough to be reported

Travel & leisure

H1 2024
1.0%
Credit card fraud

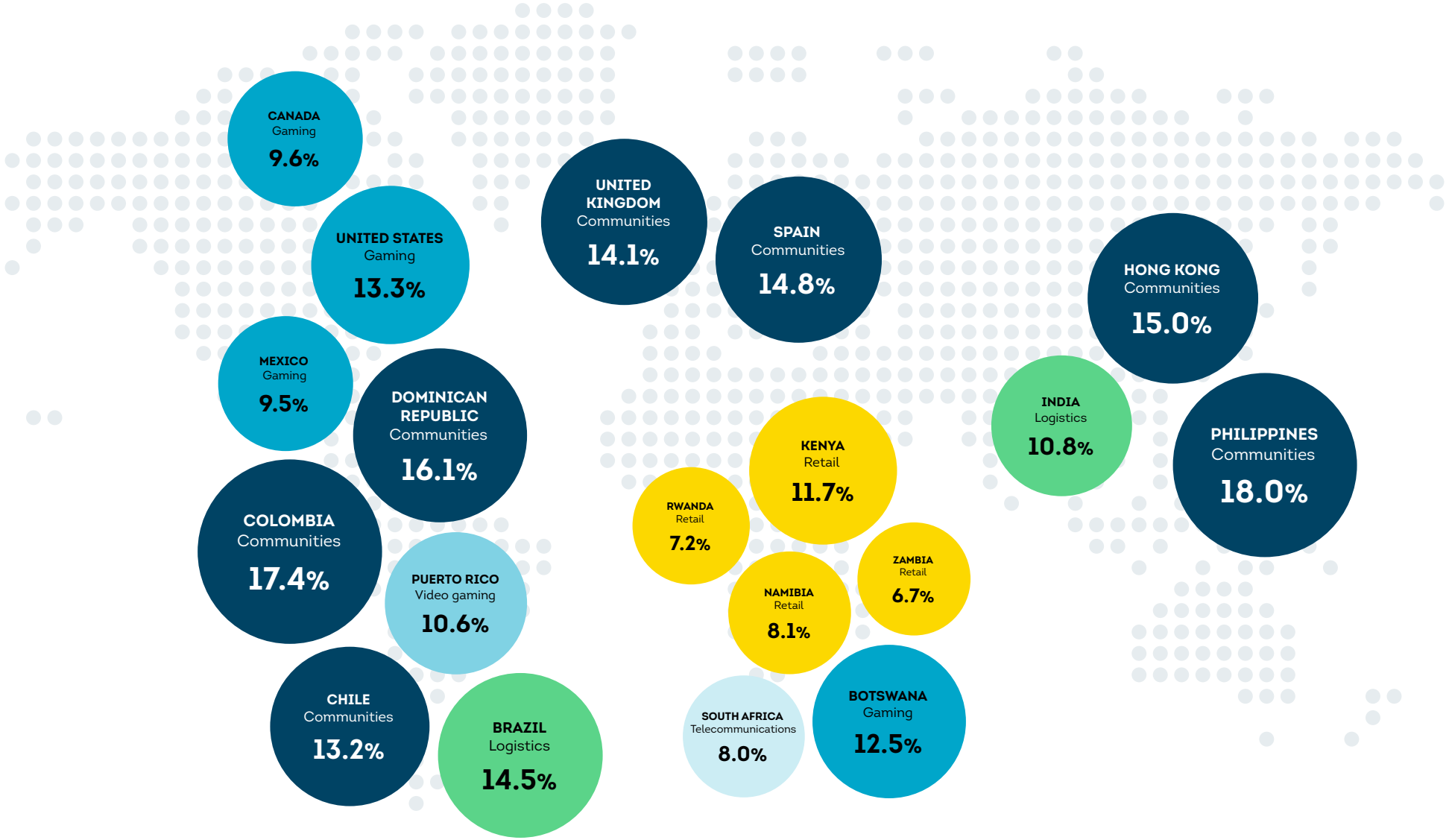
H1 2023-H1 2024
-33.2%

Source: TransUnion TruValidate

TransUnion

Digital Fraud Attempts by Region and Industry H1 2024

The industry with the highest rate of suspected Digital Fraud where the consumer is located in that region during the attempted 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 may be exploited in multiple ways. Among business leaders in the TransUnion-sponsored business survey who said they're very or extremely knowledgeable about fraud-related activity in their call centres, 43% indicated fraudsters increased their attacks on call centres in the past year. Also among those business leaders, more than half indicated stolen personal information to pass knowledge-based authentication (59%), the use of spoofing to impersonate a customer (54%) and virtual call services to be anonymous or untraceable (53%) have increased in the past year.

High-risk calls into call centres rose rapidly

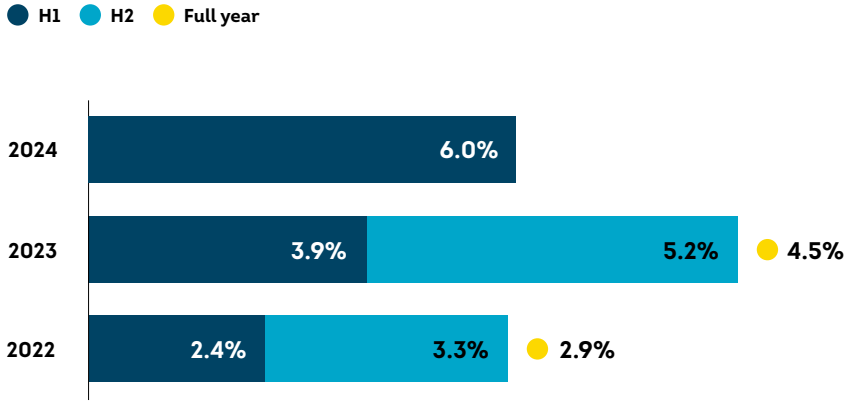
TransUnion documented a 54% increase in the percentage of high-risk calls into US call centres from H1 2023 to H1 2024 from 3.9% to 6.0%.

Increased Frequency of Call Centre Fraud Attacks

The change in frequency of fraud attacks in call centres over the past year cited by business leaders who said they're very or extremely knowledgeable about fraud-related activity in their call centres.

Source: Transunion business survey

High-Risk Calls Into Call Centres



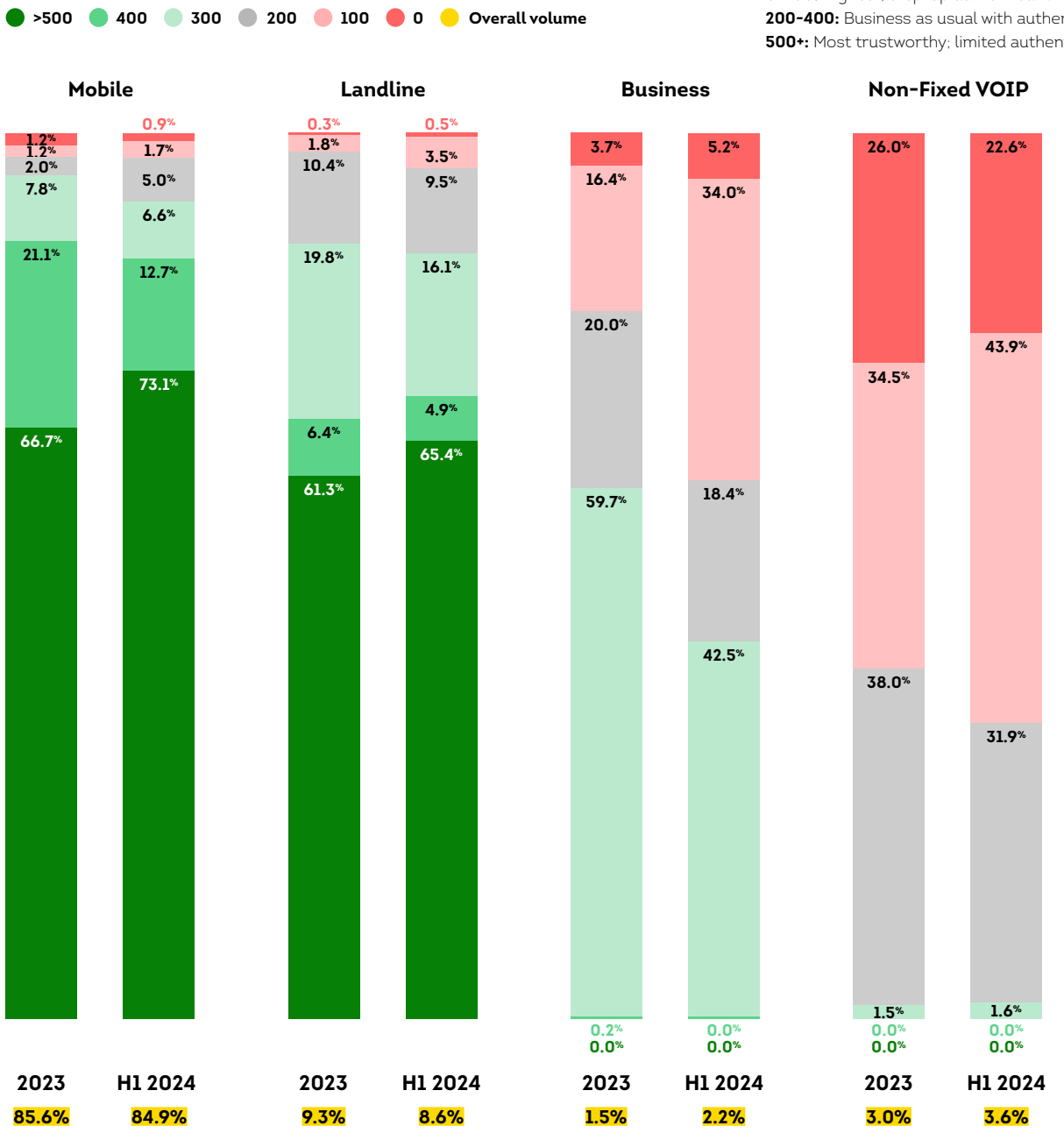
Source: TransUnion TruValidate

TransUnion

Virtual calls pose highest risk to call centres

While TransUnion documented the vast majority (85%) of calls received by its US call centre customers in H1 2024 were from mobile phones, only 2.6% of those calls were identified as being the highest risk for fraud. The percentage of risky mobile calls rose from 2.4% for all of 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 3.6% of total call volume, 67% of those calls were identified as high risk for fraud, an increase over all of 2023.

US Call Centre Risk by Channel and Overall Volume



Source: TransUnion TruValidate

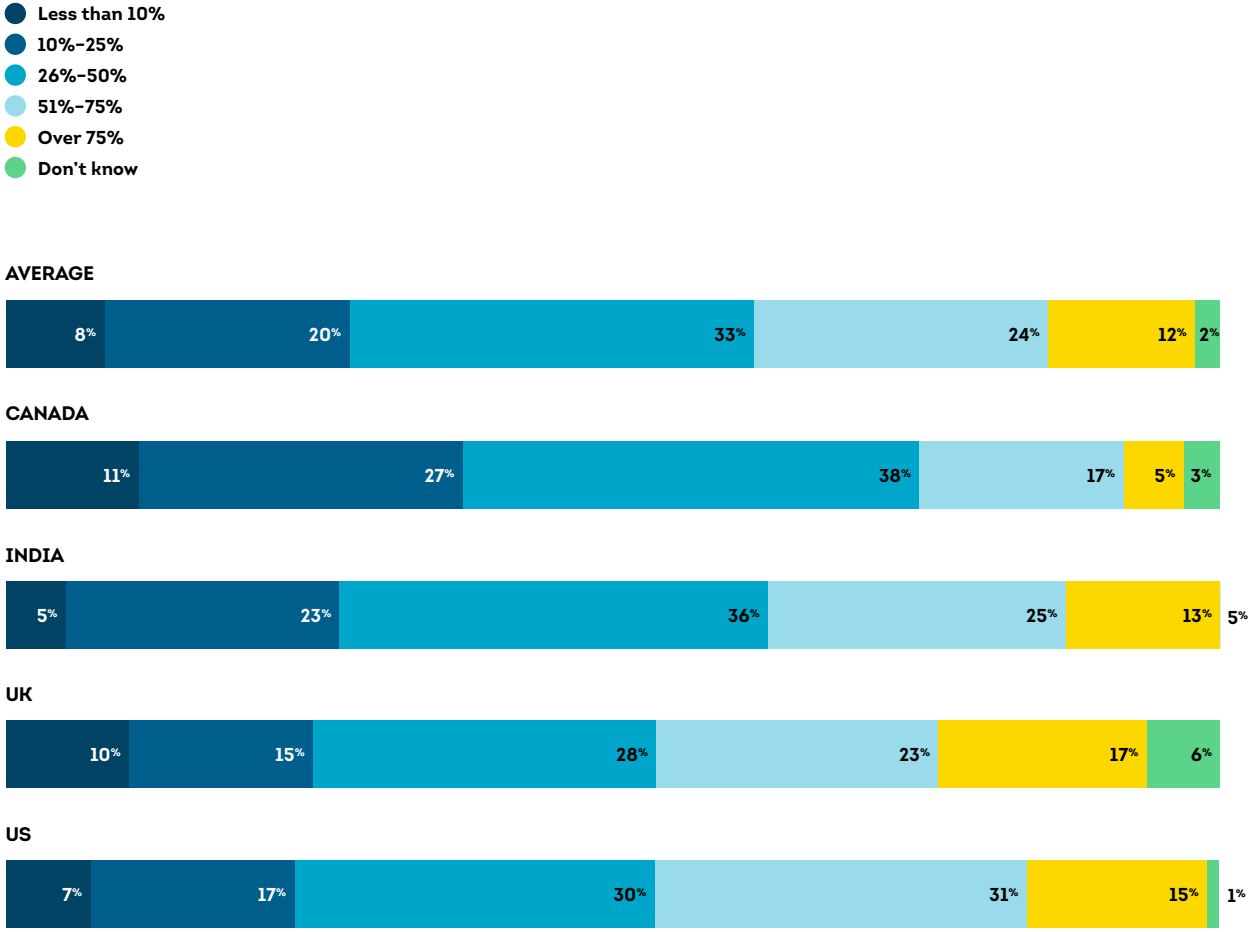
TransUnion

New Account Fraud Risk Threatens Digital Experiences

As organisations rely more on digital and mobile channels to deliver fast and convenient customer experiences, online new account creation poses increasing risk. More than two-thirds of business leaders surveyed by TransUnion indicated at least 25% of their organisations' new account openings are done online — over a third indicated it was 51% or more. While nearly three-quarters (72%) of business leaders indicated a high detection rate was extremely or very important for their fraud solutions, with so much compromised identity information in the market, they often struggle to protect their businesses while ensuring fast, seamless customer experiences — especially at new account opening.

New Accounts Opened Online

Percentage of new customer accounts opened online



Source: Transunion business survey

New account openings present highest risk stage in customer journey

Looking at risk by customer journey stage, of particular concern is risk to new account creation — driven by bad actors using synthetic or stolen identities to open accounts. Of all TransUnion TruValidate global digital account creation transactions attempted in H1 2024 (representing 7% of all traffic volume), TransUnion found 6.5% were suspected to be Digital Fraud — the highest risk rate of any customer journey stage.

Customer Journey Stage Examples

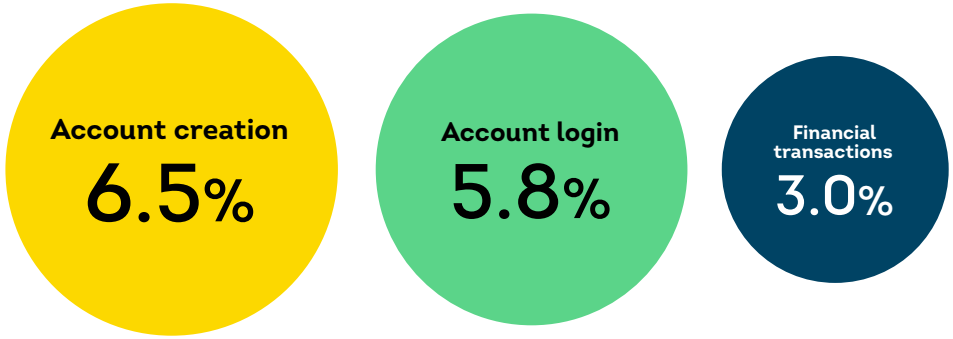
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Customer Journey Transaction Type Digital Fraud Risk

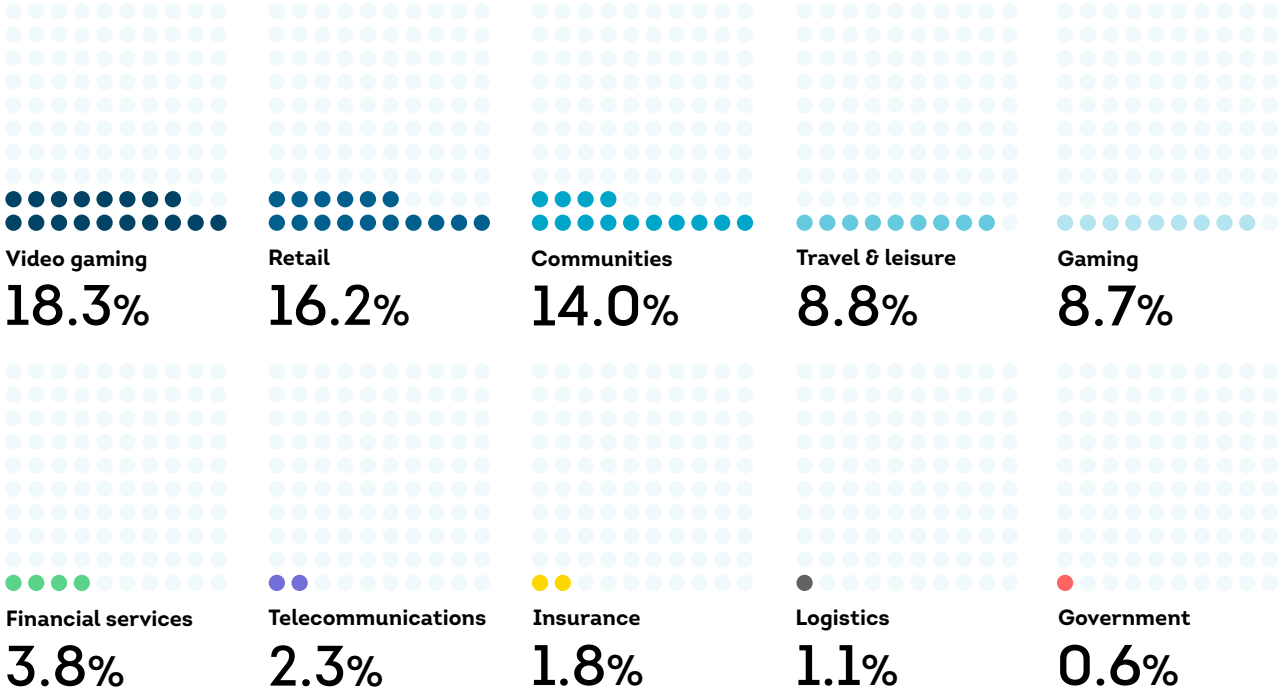
Percentage of each attempted transaction type suspected to be Digital Fraud globally in H1 2024



Source: TransUnion TruValidate

Account Creation Digital Fraud by Industry

Percentage of attempted digital account creation transactions in each industry globally that was suspected to be Digital Fraud in H1 2024



Source: TransUnion consumer fraud survey

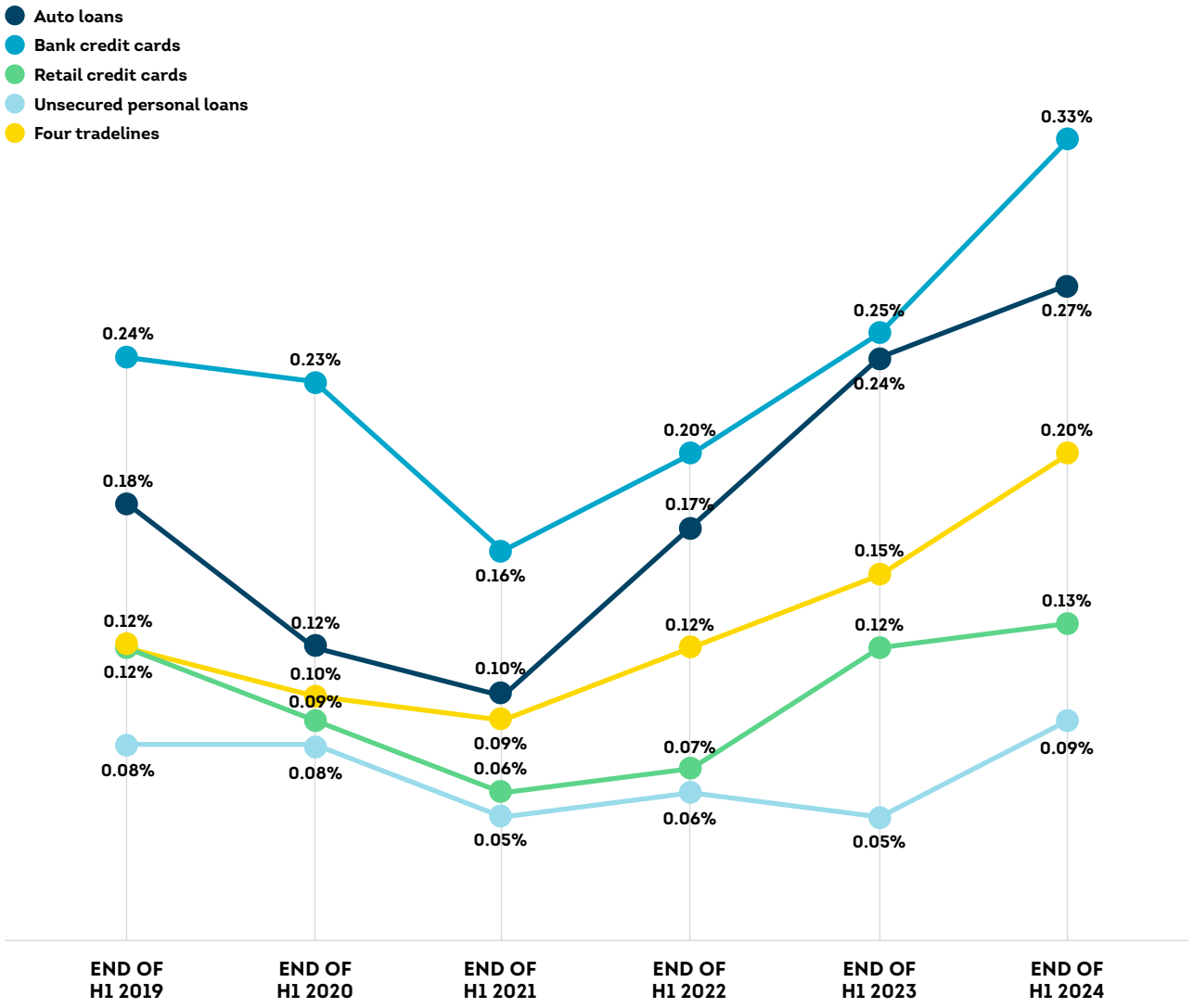
TransUnion

Synthetic identity lending exposure at all-time high

With a wealth of stolen identity credentials readily available, TransUnion found criminals are getting very good at fabricating identities. According to TransUnion's consumer credit data, 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 H1 2024, leaving lenders exposed to USD$3.2 billion in potential losses — also an all-time high and 7% more than the end of H1 2023. Synthetic identities among accounts opened rose 18% (reaching 0.20%) in H1 2024 compared to H1 2023. Based on the percentage of attempted account openings with synthetic identities, the market is facing a rising threat of charge-offs in the future. Applying synthetic identities to auto loans seemed to be particularly appealing for fraudsters to accumulate balances. The total lender exposure to synthetic identities for auto loans had balances roughly double those of the bankcard sector which ranked second among credit types analysed.

Synthetic Identities at Account Opening

Percentage of newly opened US accounts associated with synthetic identities



Source: TransUnion TruValidate

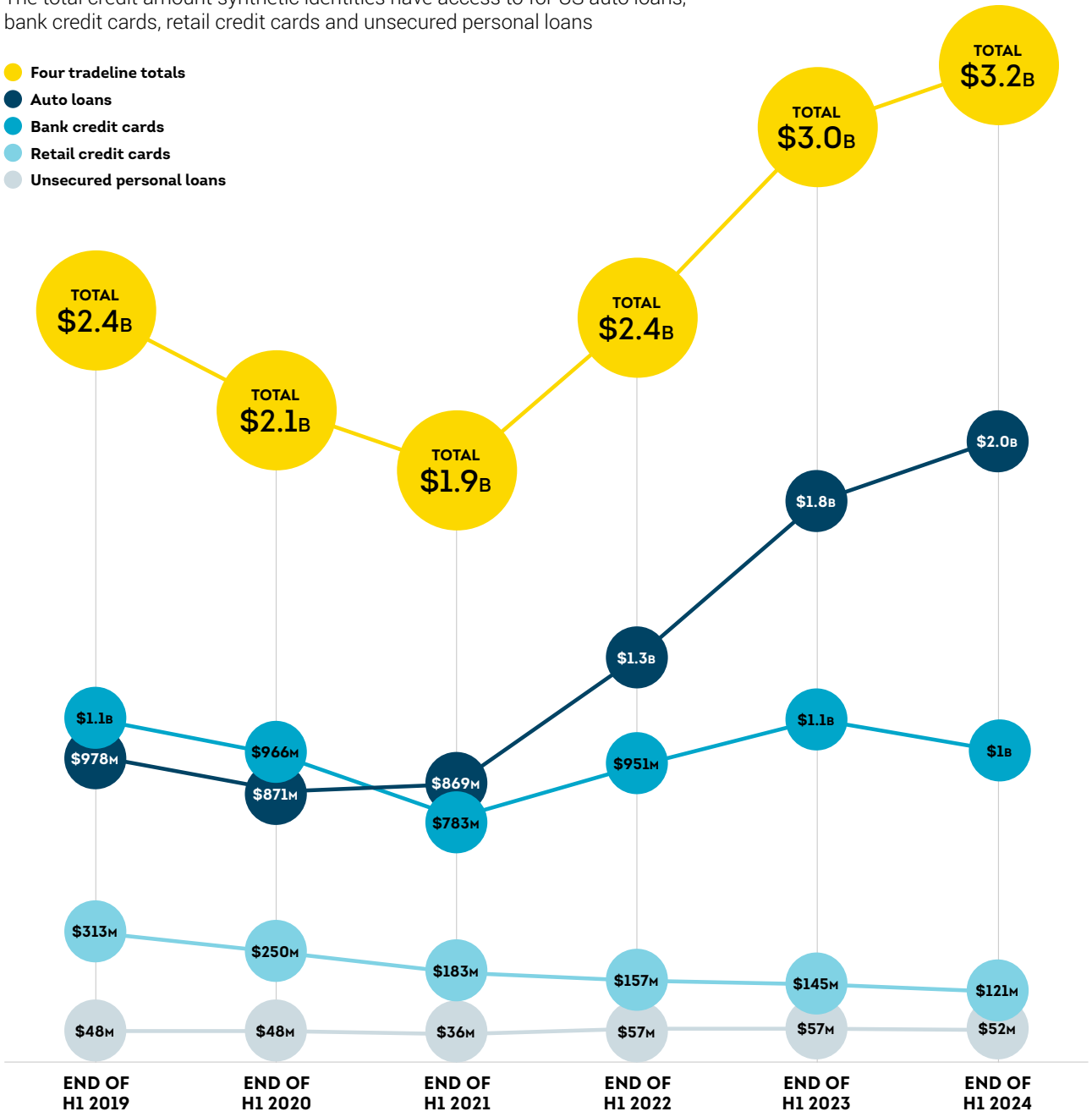
TransUnion

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 H1 2024, the total lender exposure to synthetic identities for auto loans had balances 100% higher than the bankcard sector.

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

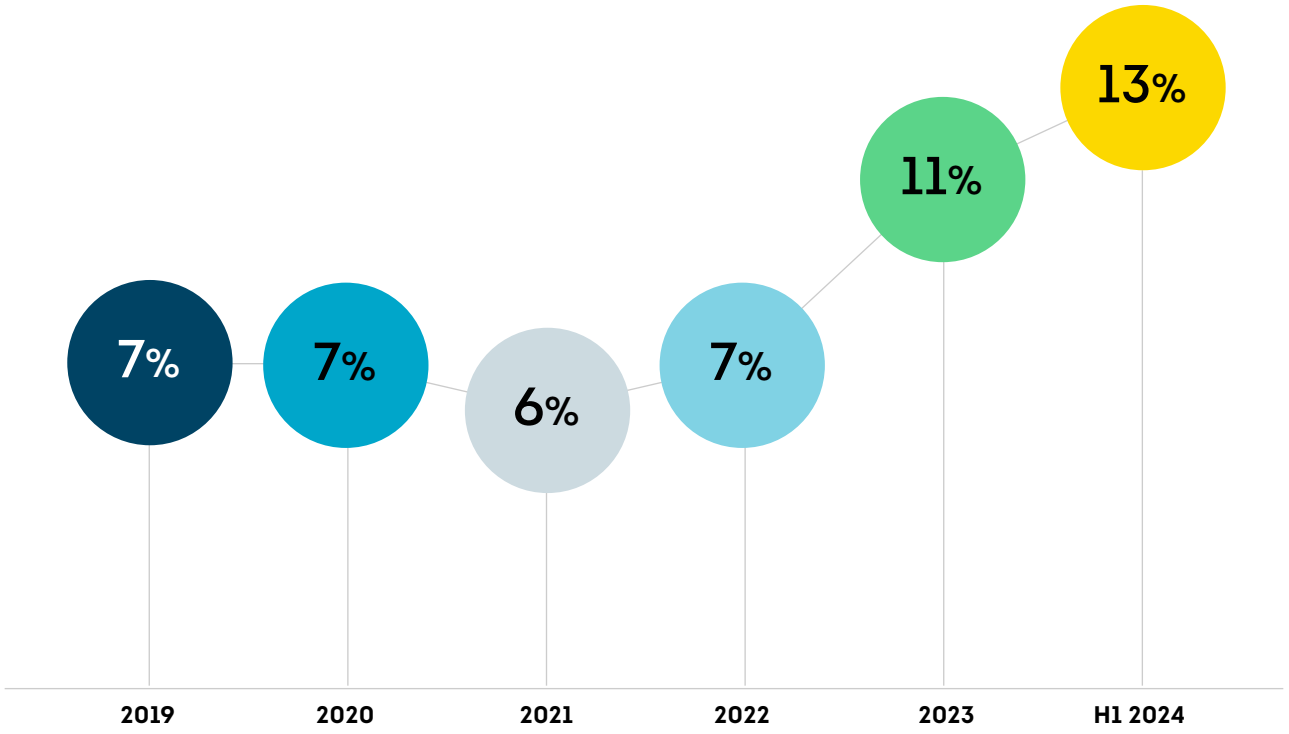
TransUnion

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 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 H1 2024, disputes in the US due to a fraud claim represented 13% of all disputes, the highest TransUnion analysed since 2019.

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



Source: TransUnion Consumer Credit

Conclusion

Digital Fraud waxes and wanes, but the trends in consumer scams are clear. Now and in the future, organisations face more sophisticated cybercriminals weaponising identity data at scale to perpetrate first- and third-party fraud schemes. Not only will organisations have to deal with persistent account hacking scams, fraudsters will continue building fake but reputable identities enabled by technology to operate with unprecedented scale and speed.

As for business leaders, they want to protect customers and their organisations alike. Fraud costs organisations significant revenue and profit loss every year. As leaders see fraud risk rising in every channel, fraud prevention is a necessary cost that needs to be as efficient as possible. Fraud leaders should take an enterprise-wide approach to fraud prevention and building customer trust. Employ a strategy of continuous innovation through better data and risk signals, advanced analytics and integrated technology to detect possible fraud more effectively — without increasing lost business and additional expense from false positives.

Data Sourcing Methodology

This report blends proprietary data from TransUnion's global intelligence network and specially commissioned business and consumer surveys.

Business survey

This online survey was conducted in Canada (200 respondents), India (200 respondents), and the UK (201 respondents) and US (200 respondents) from May 14–29, 2024 by TransUnion in partnership with third-party research provider, Dynata. The survey targeted managerial roles with responsibility for risk and/or fraud at businesses in which primary customer bases were consumers, and revenues were greater than CA$300M in Canada, ₹1B in India, £200M in the UK, and USD$200M in the US. Respondents were surveyed using an online research panel method across a combination of desktop, mobile and tablet devices. These research results are unweighted and statistically significant at the individual country level within ± 6.9 percentage points at a 95% confidence level based on calculated error margin. Please note some chart percentages may not add up to 100% due to rounding or multiple answers being accepted.

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 on approximately 400 million consumers.

Consumer Pulse Survey

This online survey of 15,372 adults was conducted April 29–May 20, 2024 by TransUnion in partnership with third-party research provider, Dynata. Adults 18 years of age and older residing in 18 global markets (Botswana, Brazil, Canada, Chile, Colombia, the Dominican Republic, Guatemala, Hong Kong, India, Kenya, Namibia, the Philippines, 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 (Chile, Colombia, the Dominican Republic, Guatemala 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. 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. Global statistics 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 on approximately 400 million consumers. The synthetic fraud analysis encompasses US credit activity recorded between Jan. 1, 2009 and June 30, 2024. 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 reputation and 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.

transunion.co.za/solution/truvalidate

TransUnion