TransUnion

H1 2025 UPDATE

STATE OF OMNICHANNEL FRAUD

Trends and strategies for protecting organizations and consumers

Introduction

Successful organizations have strategies designed to shift when market conditions change or new opportunities present themselves. Professional criminals are no different, employing similarly flexible strategies and deliberately changing tactics to improve results when they see a new opportunity emerge. Recent fraud trends point toward an apparent shift in strategy as fraudsters use exposed personal information to focus more on high-success, short-term payoffs in 2025. Countering these trends, fraud prevention leaders need to enhance fraud detection that won't impede customer growth. Consumers expect safety, security and convenience from the brands they choose. If they perceive an organization isn't protecting them, they'll find another that will.

In the State of Omnichannel Fraud Report, TransUnion® brings together trends, benchmarks, and identity and fraud expertise from across our organization. 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 organization with the goals 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 business survey in Canada, India, and the UK and US; and a consumer survey in 18 countries and regions globally. See methodology on page 21 for definitions of digital fraud and other fraud types.

KEY TAKEAWAYS

Quality over quantity – Stolen personal information supply chain shifts focus

34%
rise in US data breach severity from 2023 to 2024 (the highest going back to when TransUnion started measuring for this study in 2020), but a 45% decrease in breach volume year over year

53%
of adults in 18 countries and regions said they were targeted by email, online, phone call and text messaging fraud schemes from August to December 2024

Short-term payoff – Cybercriminals shift digital fraud strategies

11%
increase in financial transactions suspected to be digital fraud attempts last year over 2023, representing the transaction type with the biggest growth in digital fraud in 2024

20%
rise in volume of suspected digital account takeover (ATO) attempts globally from 2023 to 2024, representing one of the fastest-growing types of digital fraud reported to TransUnion by its customers last year

Follow the money – Consumers and lenders report significant fraud losses

29%
of consumers said they lost money from email, online, phone or text messaging fraud in the last year, costing a median amount of USD$1,747 among those surveyed in 18 countries and regions

USD$3.3 billion
in lender exposure to synthetic identities in the US for auto loans, bank credit cards, retail credit cards and unsecured personal loans at the end of 2024, an all-time high

Contents

TransUnion

Consumer Mindset Driven by Fraud Experience

Business growth tied to consumer perception of data security and safety

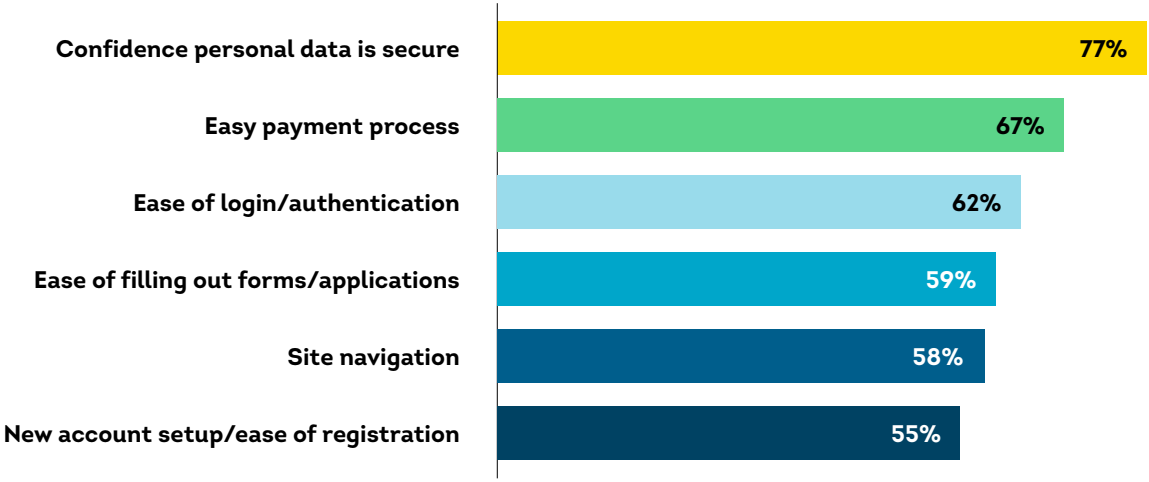
Consumers prefer organizations they feel protect their identities while delivering convenient experiences. Expectations for the brands they choose to spend money with have been consistent. In Q4 2024, 59% (unchanged over last year) of consumers we surveyed reported they're likely to switch companies to get a better digital experience. Over three-quarters (77%) said confidence their personal data will not be compromised is very important when choosing who to transact with online.

Ranked Expectations/Qualities in Preferred Online Companies

Top answer chosen

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered very important



Source: TransUnion consumer survey conducted Nov. 21–Dec. 11, 2024

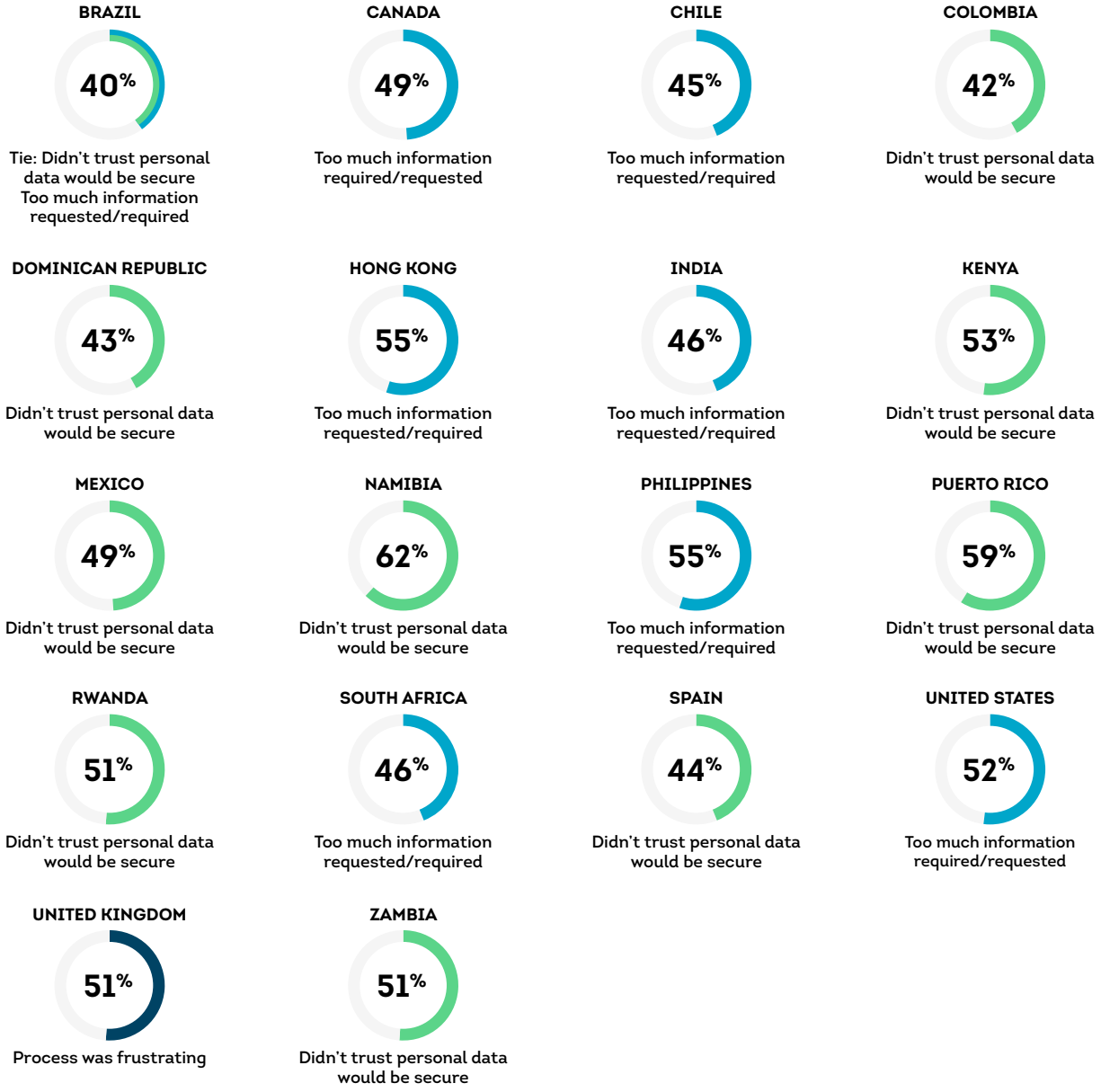
TransUnion

Honouring expectations for security and convenience is a winning strategy

Worldwide retail ecommerce sales (excluding other online activities like banking, gaming and travel) were expected to surpass USD$6 trillion in 2024, according to market research company EMARKETER, Inc. (2024). To capture some of that market opportunity, organizations must ensure omnichannel experiences are perceived as safe and secure — or they risk losing business. Consumer-reported online behaviour remained consistent in 2024: 34% said they conducted more than half of their transactions online — the same as 2023.

About two-thirds (62%) of consumers reported fraud concerns were the top reason they wouldn't use a website again. Nearly half (48%) of consumers reported abandoning an online shopping cart due to fraud and/or security concerns. While the majority (51%) said they've abandoned online financial or insurance applications, their reasons spanned safety and ease: Too much information requested (46%), didn't trust their personal data would be secure (41%), and the process was frustrating (38%) were the top abandonment explanations.

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



Source: TransUnion consumer survey conducted Nov. 21–Dec. 11, 2024

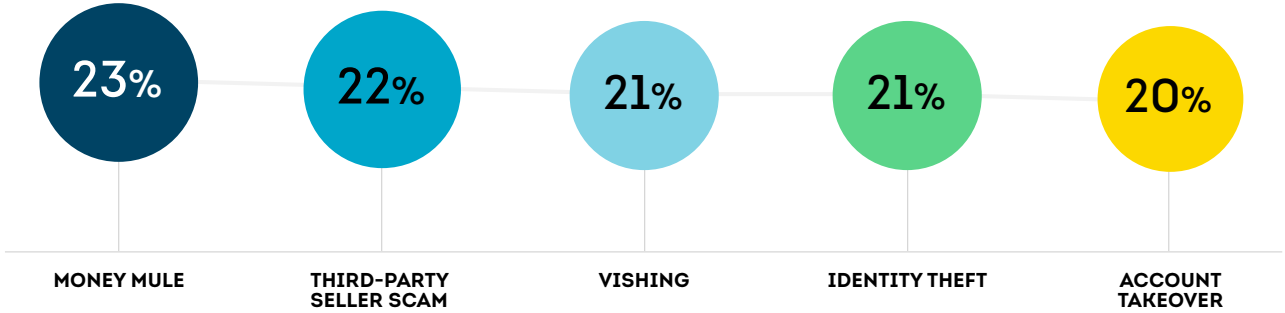
TransUnion

The cost of fraud for consumers

Among consumers surveyed in 18 countries and regions, 29% said they lost money due to email, online, phone call or text messaging fraud in the last year. Gen Z was the highest (38%) among surveyed generations and Baby Boomers the lowest (11%). The median amount (averaged across 18 countries and regions surveyed) consumers said they lost due to fraud in the past year was USD$1,747. Across countries or regions, the highest median was in India (USD$5,740) and the lowest in Zambia (USD$232). In the US, 20% of adult consumers said they lost money, with a median loss reported of USD$4,967. Extrapolated to the US adult population (266.3 million on July 1, 2024, according to the US Census Bureau), that reflects an estimated USD$265 billion lost by US consumers to email, online, phone call or text messaging fraud in the past year.

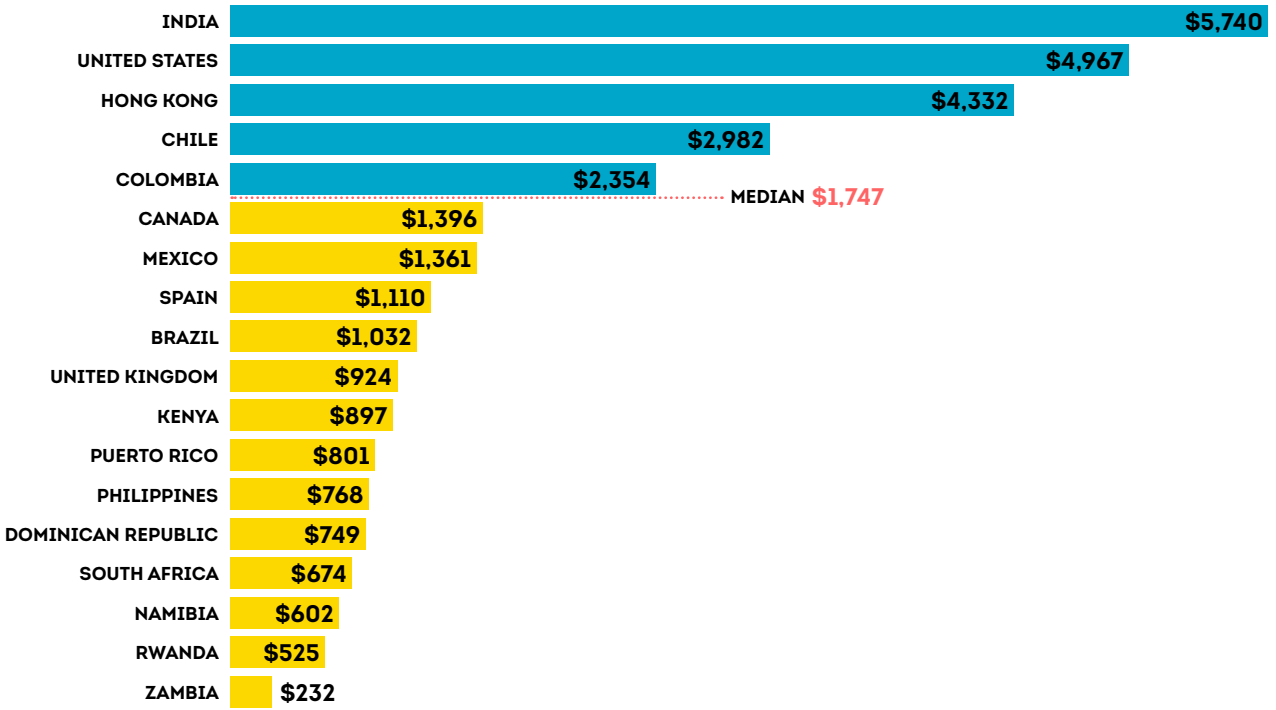
Top Schemes Resulting in Consumer Monetary Fraud Loss in Last Year

Percentage reporting losing money to these schemes among consumers who said they lost funds from email, online, phone call or text messaging fraud



Consumer Reported Fraud Loss

Median reported fraud loss in the last year, among those who said they lost money from email, online, phone call or text messaging fraud, in USD for each country or region



*USD conversion based on currency exchange value on Jan. 6, 2025

Source: TransUnion consumer survey conducted Nov. 21–Dec. 11, 2024

TransUnion

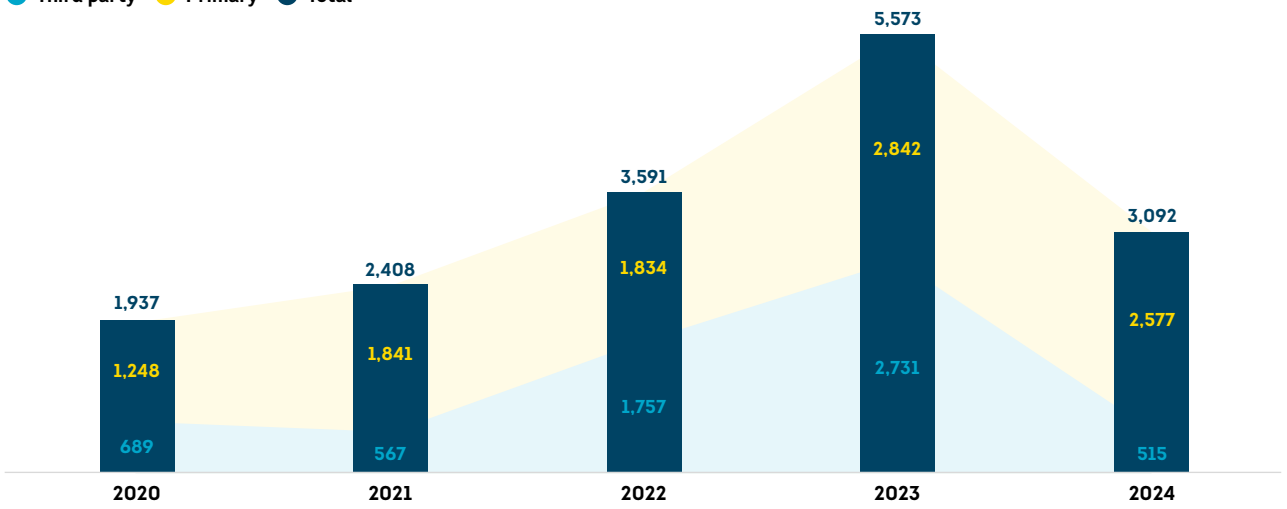
Personal Information Exposure Trends

Criminals remained determined to acquire consumer personal information — targeting organizations and consumers alike — to fuel fraud schemes. However, they appeared to shift focus to data quality over quantity. Data breaches targeted more high-quality credentials, and consumers reported being targeted by data harvesting scams in every channel, including email, online, phone and text. Exposed personal information enables criminals to more readily power automated, identity-based attacks on organizations and individuals.

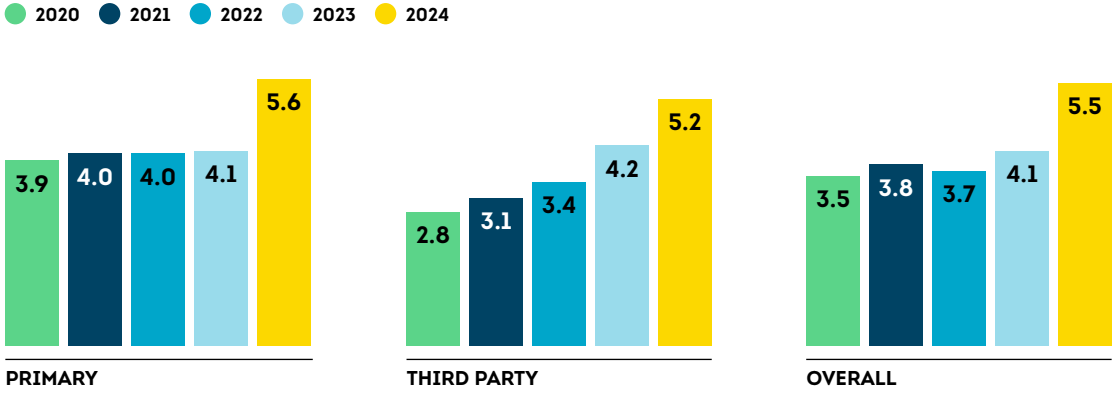
US data breaches reached record severity

The pace of US data breach growth reversed in 2024. However, breach severity — a leading indicator of future fraud — reached record levels. While the volume of US data breaches decreased 45% year over year in 2024, the average breach risk severity (the ability of a breach to enable identity fraud), as measured by TransUnion TruEmpower™ Breach Risk Score (BRS), increased 34%, its highest point ever since TransUnion initiated studies in 2020.

US Data Breach Volume



Average Breach Risk Score for US Data Breaches



A primary data breach represents a direct attack on an organization. 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

*TruEmpower is US specific

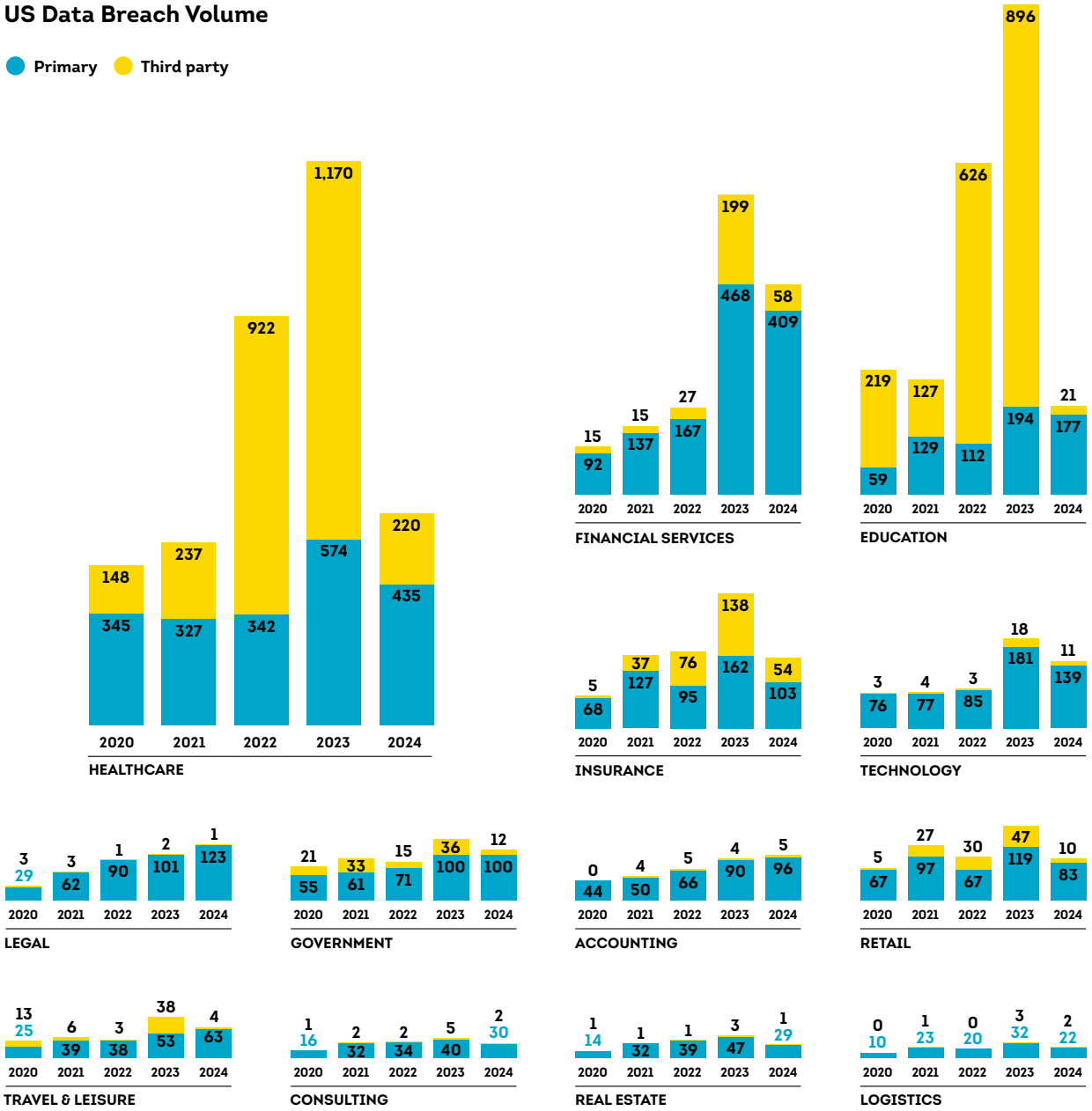
TransUnion

Healthcare and financial services most breached industries

For the fifth year running, the healthcare industry experienced the highest number of breaches. This was followed by financial services in 2024. Not only did healthcare have the highest volume of breaches, TransUnion found healthcare also experienced breaches that posed the highest risk during that period (with a BRS of 6.3 followed by government at 6.0). Both direct and indirect attacks focused on high-value identity credentials, including full Social Security number (SSN), medical history, payment numbers and contact information — all important in perpetrating consumer scams, as well as verifying already compromised data.

Criminals often seek the easiest targets to breach. For example, more than 60% of government data breaches were focused on local government agencies in 2024 — organizations least likely to be able to fund significant protections.

US Data Breach Volume



Source: TransUnion TruEmpower

*TruEmpower is US specific

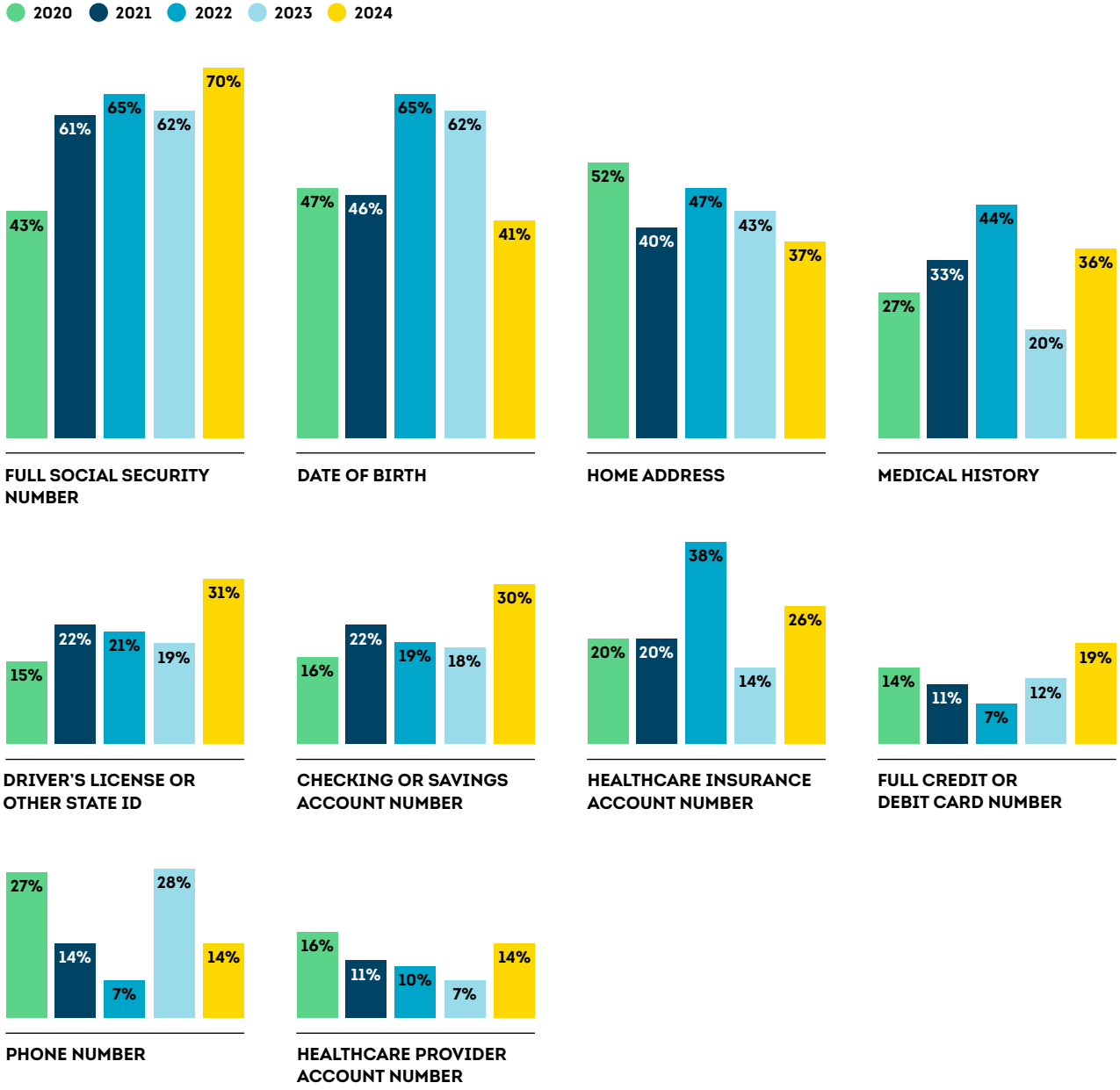
TransUnion

High-value identity credentials prioritized by criminals

In 2024, criminals appeared to focus on high-value credentials to enable future fraud and consumer scams across the customer lifecycle. In 2024, TransUnion found full SSNs were exposed in 70% of data breaches (a 13% increase over 2023), which could support new account, synthetic, tax refund and government benefits identity fraud. Healthcare data exposure showed significant growth in 2024 — with the possible intent of powering targeted consumer scams to further insurance account takeover or medical claim fraud. Medical histories (including diagnoses and physicians) were included in 36% of breaches overall, an 80% year-over-year increase, and 60% of third-party breaches, a 346% increase.

Top 10 Exposed Identity Credentials in US Data Breaches 2024

Frequency of credentials exposed in data breaches



Source: TransUnion TruEmpower

*TruEmpower is US specific

TransUnion

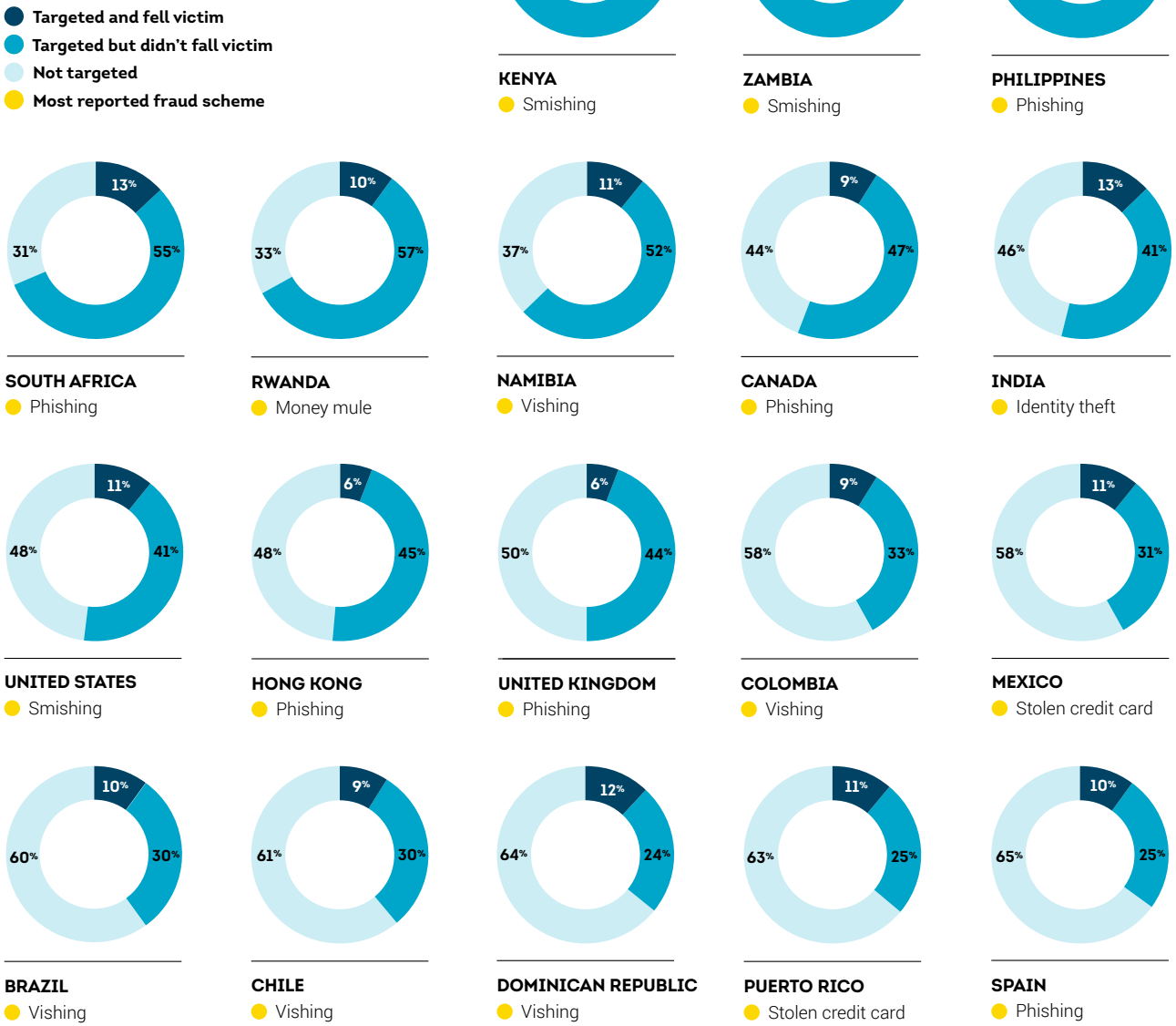
Nearly half of consumers reported being unaware of fraud schemes targeting them

While more than half (53%) of consumers surveyed in 18 countries and regions reported being targeted by an email, online, phone call or text messaging fraud scheme in the last three months, a significant portion of the population may not recognize potential fraud: 47% said they were unaware of being targeted. Among those who said they were targeted, phishing at 31%, smishing at 28% and vishing at 27% were the leading types of fraud consumers reported experiencing.

While criminals will attack at any time using any channel, they appear to focus on popular channels. In regions where mobile phones are the most common route to the internet, such as parts of Africa and Central and South America, the most common attack vector reported by many consumers was vishing.

Consumers Targeted With Fraud

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



Source: TransUnion consumer survey conducted Nov. 21–Dec. 11, 2024

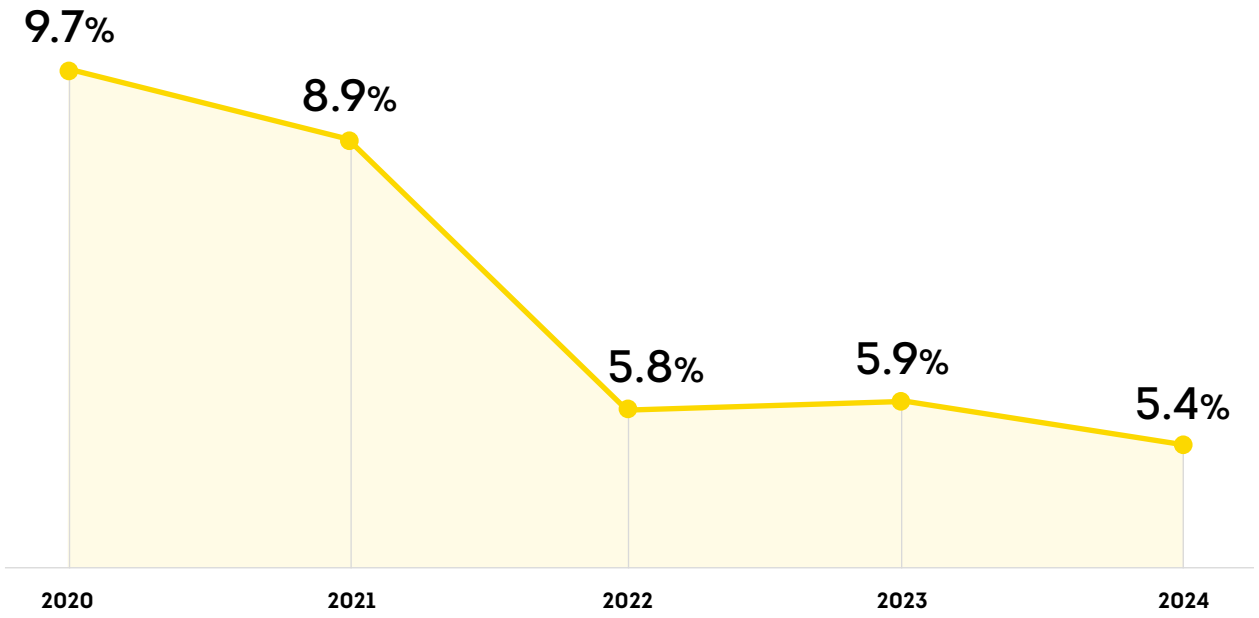
TransUnion

Global Digital Fraud Trends

Suspected digital fraud risk stabilized over past three years

The rate of suspected digital fraud attempts globally among TransUnion TruValidate® customers fell 8% to 5.4% in 2024 from 5.9% in 2023. Of the 20 markets included in this year's analysis, 7 (Canada, Colombia, India, Mexico, Namibia, the Philippines and Puerto Rico) saw an increased rate of suspected digital fraud year over year in 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 5.4% in 2024.

Rate of Suspected Digital Fraud

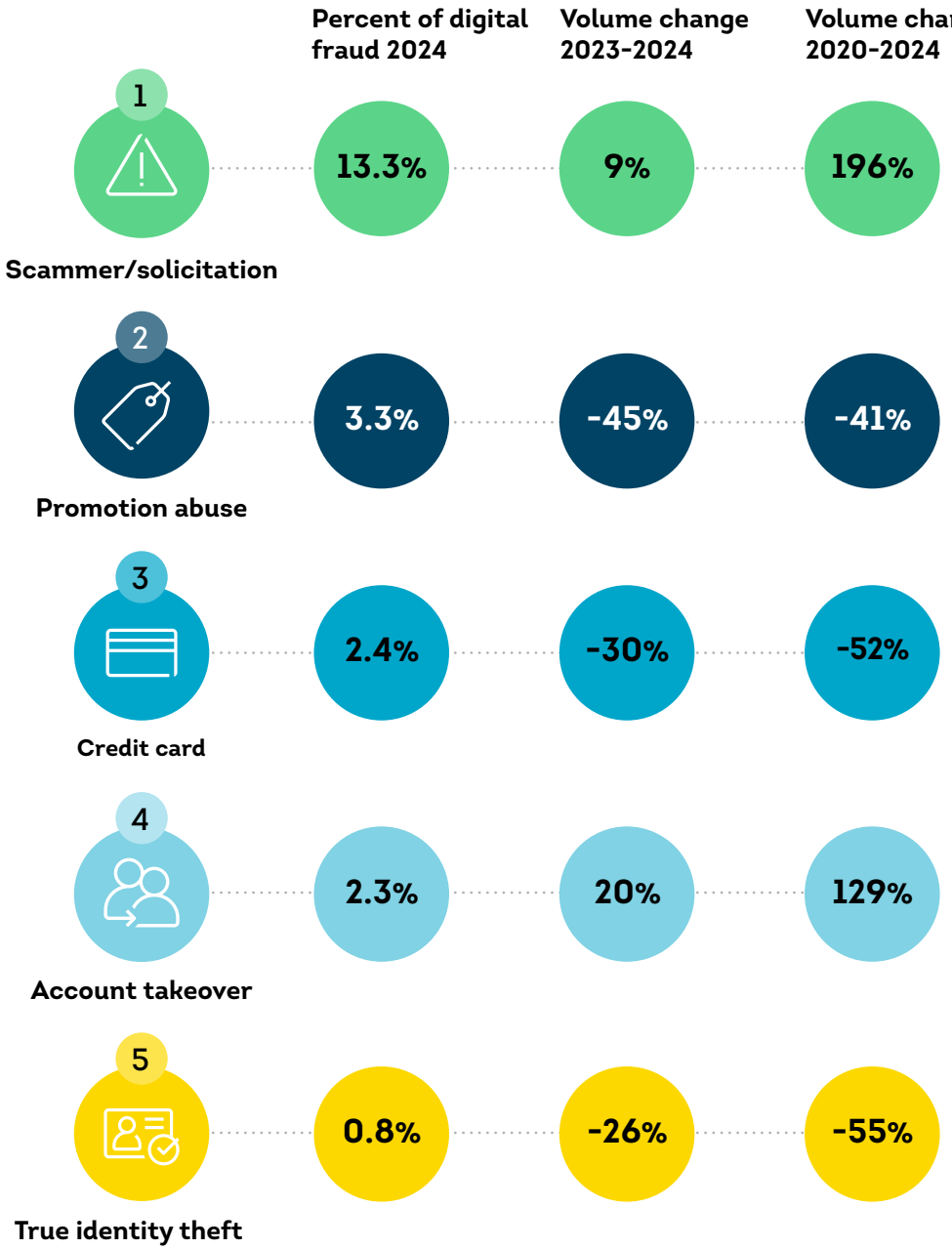


Source: TransUnion TruValidate

Account takeover growth a concerning trend

ATO, while just 2.3% of digital fraud attempts reported to TransUnion by its customers globally last year, saw volume grow 20% over 2023 and 129% since 2020, the first year TransUnion analyzed for this study. At 13.3%, scammer/solicitation fraud (promoting unauthorized services and products, often to steal account credentials) was by far the top type of digital fraud reported to TransUnion by its customers in 2024. These two types of fraud schemes are closely linked as scammer/solicitation scams often lead directly or indirectly to account takeover attempts.

Top Digital Fraud Types and Their Growth



Source: TransUnion TruValidate

TransUnion

Communities industry experienced the highest suspected digital fraud rate

Communities, which include web properties like online forums and dating sites, experienced the highest percentage (11.6%) of suspected digital fraud attempts globally in 2024 among industries analyzed, a 9% volume increase over 2023. Cybercriminals, taking advantage of the trust inherent on community-based platforms, targeted members with scammer/solicitation, the most reported type of digital fraud in communities and video gaming sites.

Other industries that experienced increased suspected digital fraud volume in 2024 included logistics (101% increase), gaming (20%), government (6%) and financial services (3%).

Global Digital Fraud Attempts by Industry

- **Suspected fraud attempt rate 2024**
- **Top fraud type 2024**
- **Percent change in suspected digital fraud volume 2023-2024**

Communities
(online dating, forums, etc.)

2024
11.6%
Scammer/solicitation

2023-2024
+9%

Video gaming

2024
10.8%
Scammer/solicitation

2023-2024
-23%

Gaming
(online gambling, poker, etc.)

2024
7.8%
Promotion abuse

2023-2024
+20%

Retail

2024
7.6%
Promotion abuse

2023-2024
-45%

Financial services

2024
4.9%
Account takeover

2023-2024
+3%

Telecommunications

2024
3.0%
True identity theft

2023-2024
-79%

Logistics

2024
2.6%
n/a*

2023-2024
+101%

Insurance

2024
2.0%
First-party application fraud

2023-2024
-29%

Government

2024
1.7%
Credit card fraud

2023-2024
+6%

Travel & leisure

2024
0.9%
Credit card fraud

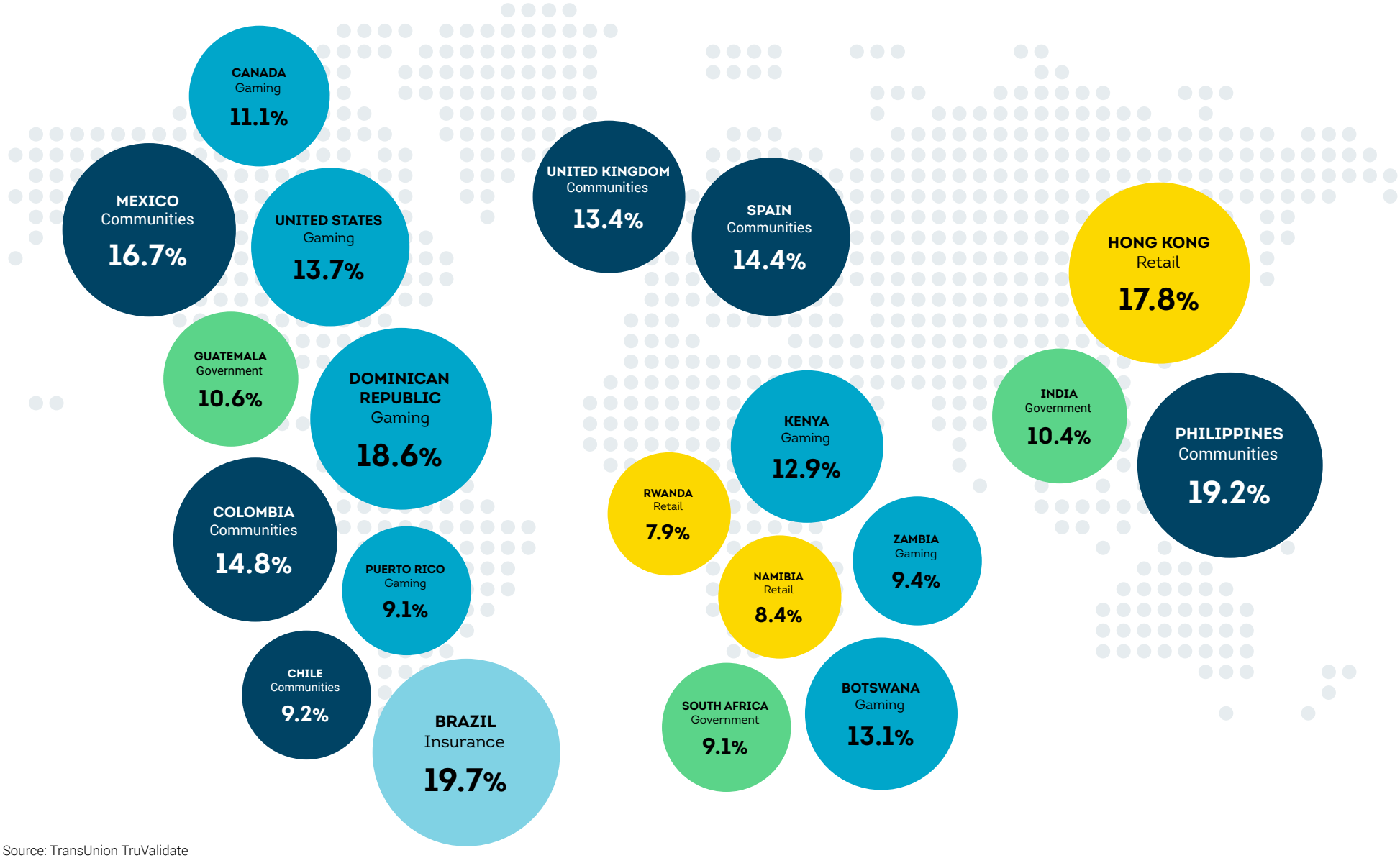
2023-2024
-38%

*N/A — The number of customers reporting types of digital fraud wasn't statistically significant enough to be reported

Source: TransUnion TruValidate

Digital Fraud Attempts by Region and Industry 2024

The industry with the highest rate of suspected digital fraud where the consumer was located in that region during the attempted transaction



Source: TransUnion TruValidate

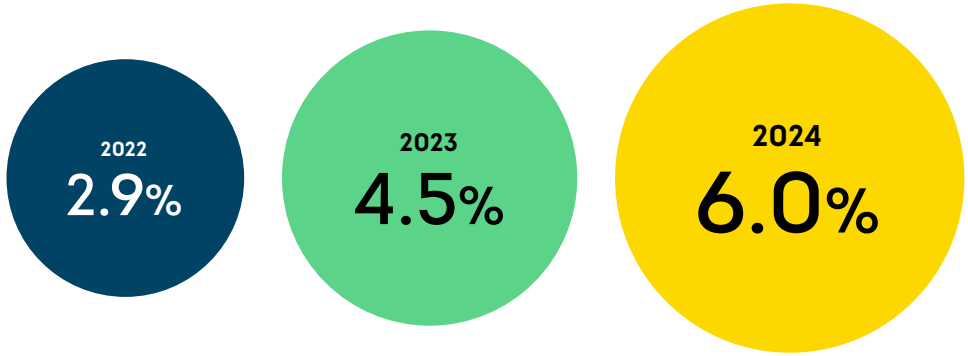
Call Centre Fraud Trends

Call centres play an important role in an omnichannel customer experience — representing a high-trust touchpoint for consumers — that may be exploited in many ways. Among business leaders (from Canada, India, and the UK and US) in a May 2024 TransUnion-sponsored survey who said they're very or extremely knowledgeable about fraud-related activities in their call centres, 43% indicated fraudsters increased their attacks on call centres in the past year. Although call centres are a vital customer service channel, they are also a key vector for criminal attacks — and the risk to this channel is rising.

High-risk calls into call centres rose rapidly

TransUnion documented a 33% increase (from 4.5% to 6.0%) in the percentage of high-risk calls into US call centres from 2023 to 2024. Risk increased across all phone channels measured. More than half of business leaders who said they're extremely or very knowledgeable about fraud in their call centre reported rising levels of criminal tactics targeting them including call spoofing to impersonate consumers, use of virtual call services and the use of stolen identity information to pass knowledge-based authentication questions.

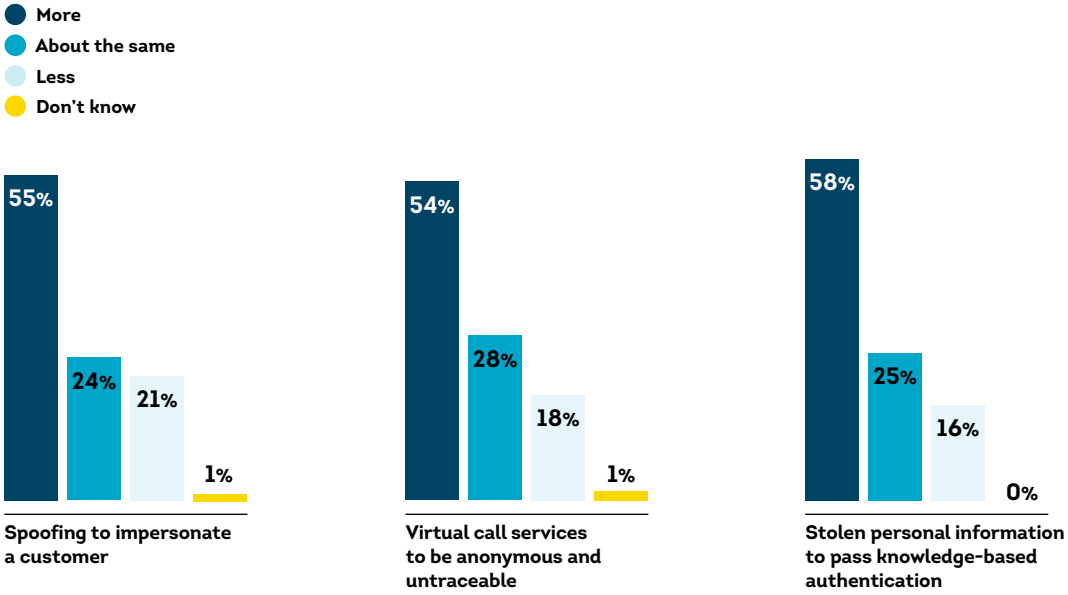
High-Risk Calls Into Call Centres



Source: TransUnion TruValidate

Criminal Call Centre Fraud Tactics

Percentage of business leaders who reported how certain criminal tactics associated with call centres changed in the past year among those who said they're extremely or very knowledgeable about fraud in their call centre



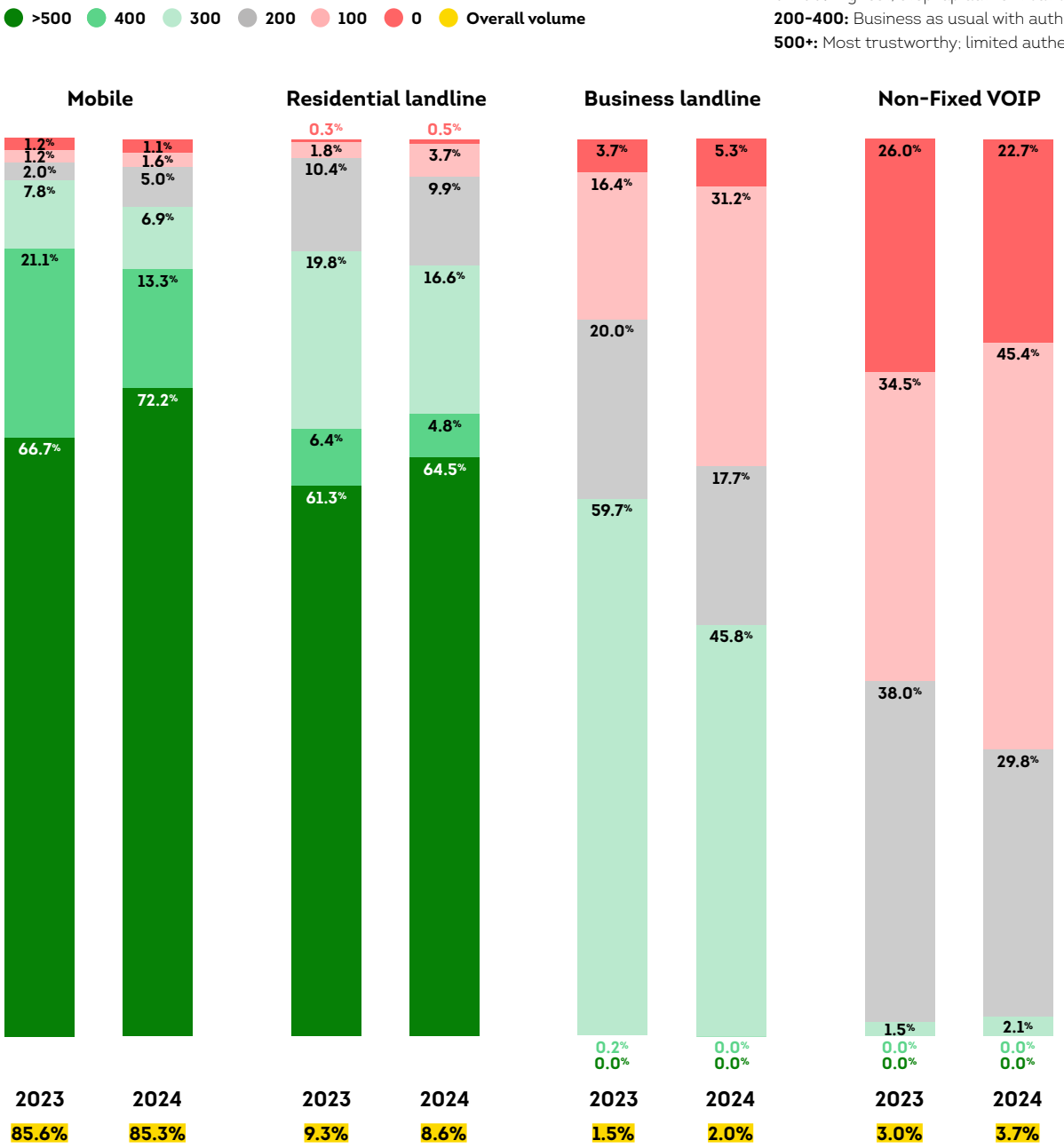
Source: TransUnion business survey conducted May 14–29, 2024

TransUnion

Mobile call risk increased; virtual calls continued to be most risky

TransUnion documented the vast majority (85.3%) of calls received by its US call centre customers in 2024 were from mobile phones. While just 2.7% of those calls were identified as being the highest risk for fraud, that's a 13% increase from 2.4% 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 3.7% of total call volume, it increased 23% over 2023. In addition, 68.1% of those calls were identified as high risk for fraud in 2024, a 13% increase over 2023.

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

Risky Identities Impact All Stages of the Customer Journey

Identity-based fraud, powered by massive amounts of exposed identities and increasingly sophisticated cybercriminals, continues to grow. Bad actors have the capability to attack everywhere, all at once.

Financial transaction risk showed greatest growth in the digital customer journey

Digital account creation (6.9%) and account login (6.2%) experienced suspected digital fraud rates above those of suspected digital fraud overall (5.4%) in 2024. At the same time, fraudsters appeared to increase focus on immediate returns as the rate of suspected digital fraud attempts in financial transactions rose 11% over 2023.

Customer Journey Stage Examples

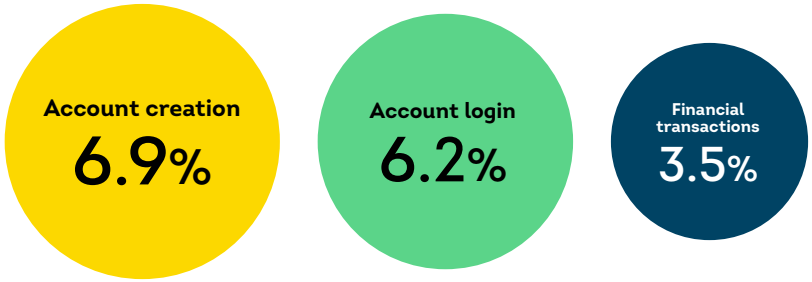
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Customer Journey

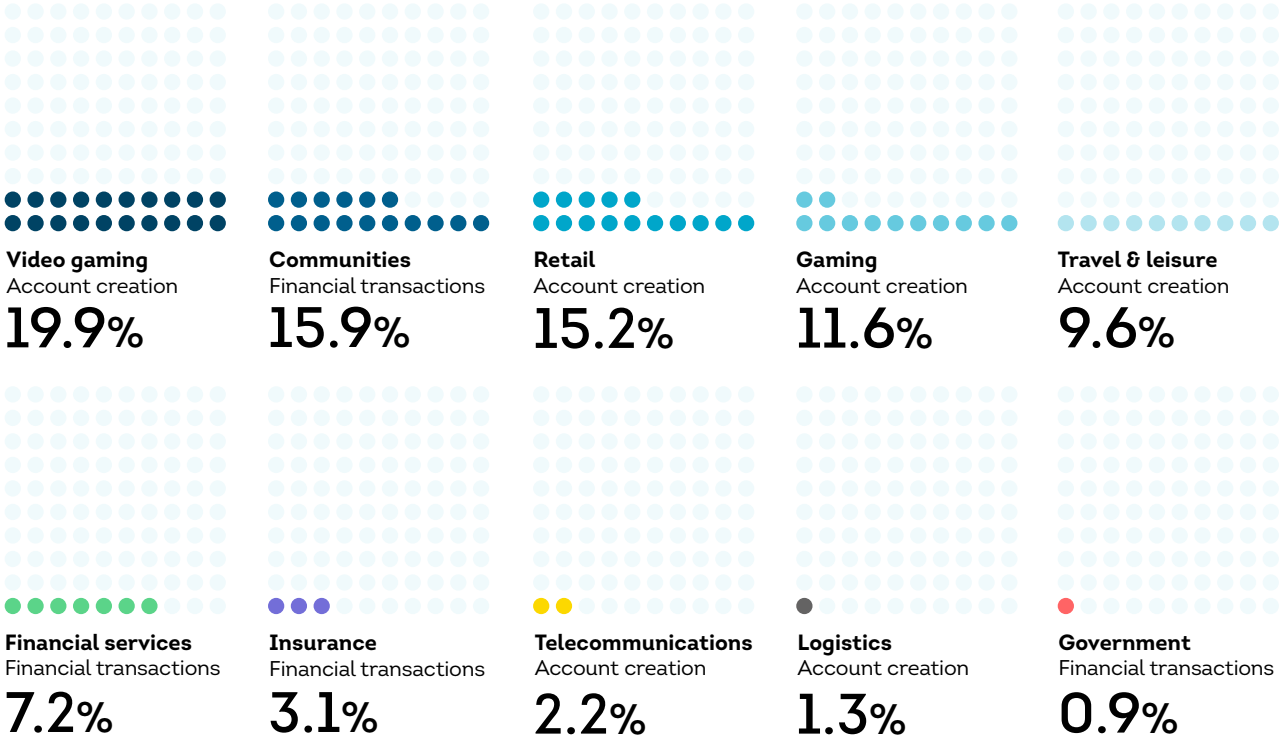
Percentage of each attempted transaction type suspected to be digital fraud globally in 2024



Source: TransUnion TruValidate

Fraud Risk in the Digital Customer Journey by Industry

The customer journey stage with the highest rate of suspected digital fraud by industry and the corresponding percentage in that stage globally in 2024



Source: TransUnion TruValidate

TransUnion

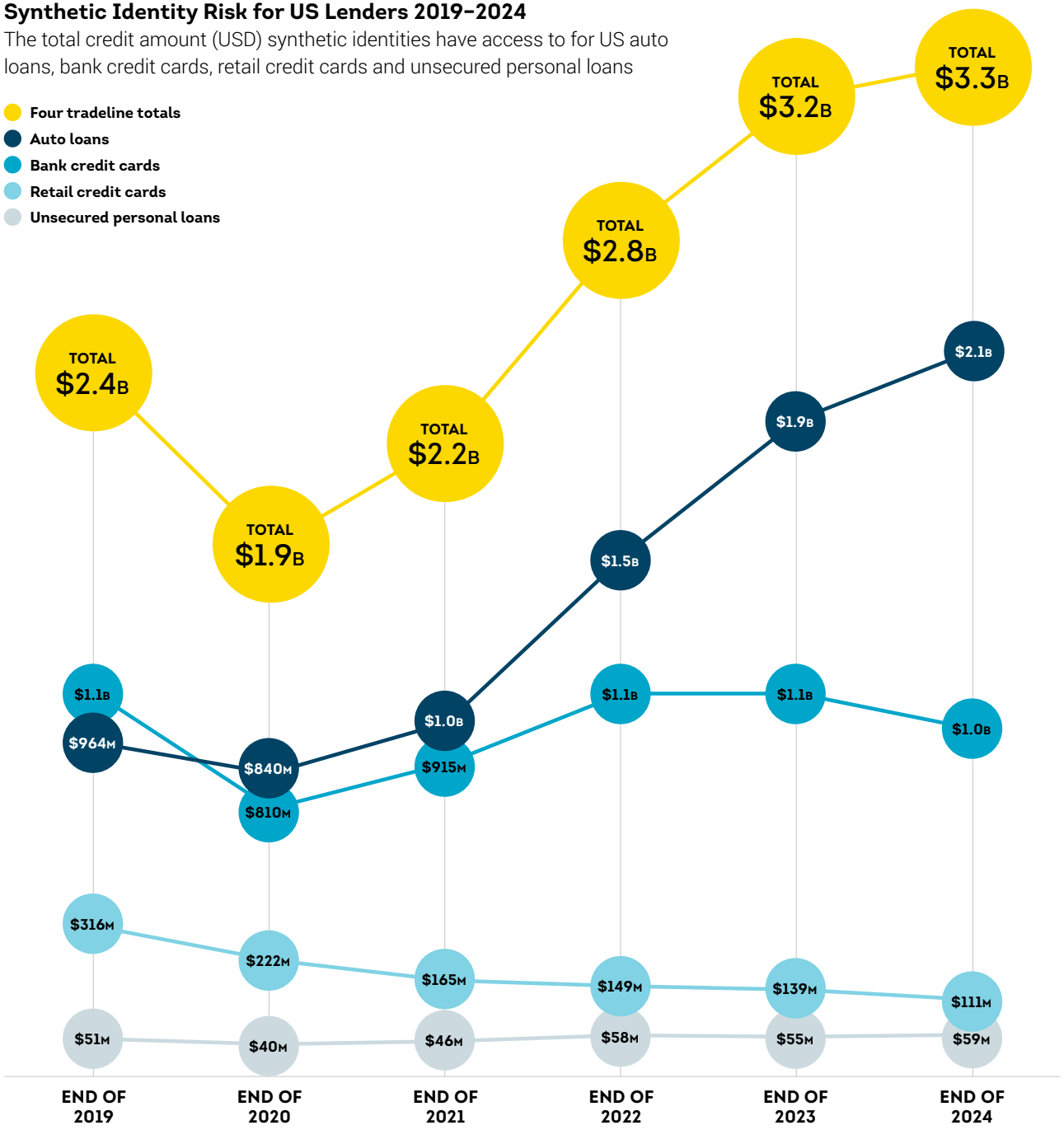
Synthetic identity lending exposure illustrated new account origination risk

With a wealth of stolen identity credentials readily available, TransUnion found criminals are pursuing more synthetic identity fraud. According to TransUnion's consumer credit data, the total exposure to synthetic identities among accounts opened by US lenders for auto loans, bank credit cards, retail credit cards and unsecured personal loans reached USD$3.3 billion in potential losses — an increase of 3% over the end of 2023 and an all-time high going back to TransUnion's first measurement in 2009.

Based on the percentage (0.32%) of attempted account openings with synthetic identities, the market is facing a continued threat of charge-offs in the future. While auto loans continued to represent the largest exposure by trade, incidences of synthetic identities for credit inquiries in bankcards was the highest among credit types analyzed, surpassing 1% at the end of 2024 — a first since TransUnion began reporting synthetic identity exposure.

Synthetic Identity Risk for US Lenders 2019–2024

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



Source: TransUnion TruValidate

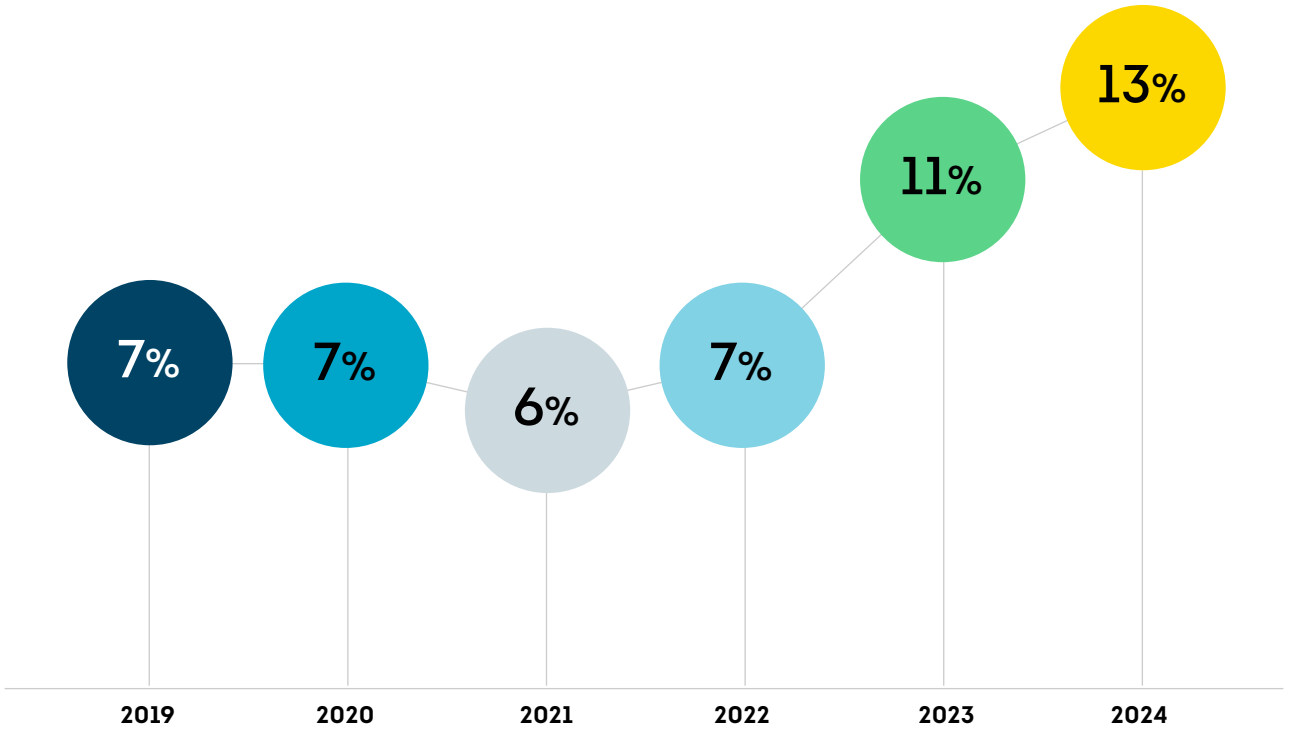
TransUnion

Credit washing extended new account opening fraud risk

As identity fraud increases, criminals who commit first-party fraud 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 unauthorized transactions on a consumer's legitimate credit account.

Consumers in the US (or their authorized representatives) have a legal right to dispute inaccurate items on their credit reports, and TransUnion follows a highly regulated dispute resolution process. In 2024, consumer credit report disputes in the US claiming fraud represented 13% of all disputes, the highest in the five-year period TransUnion analyzed.

US Consumer Credit Report Disputes Claiming Fraud as a Percentage of Total Disputes



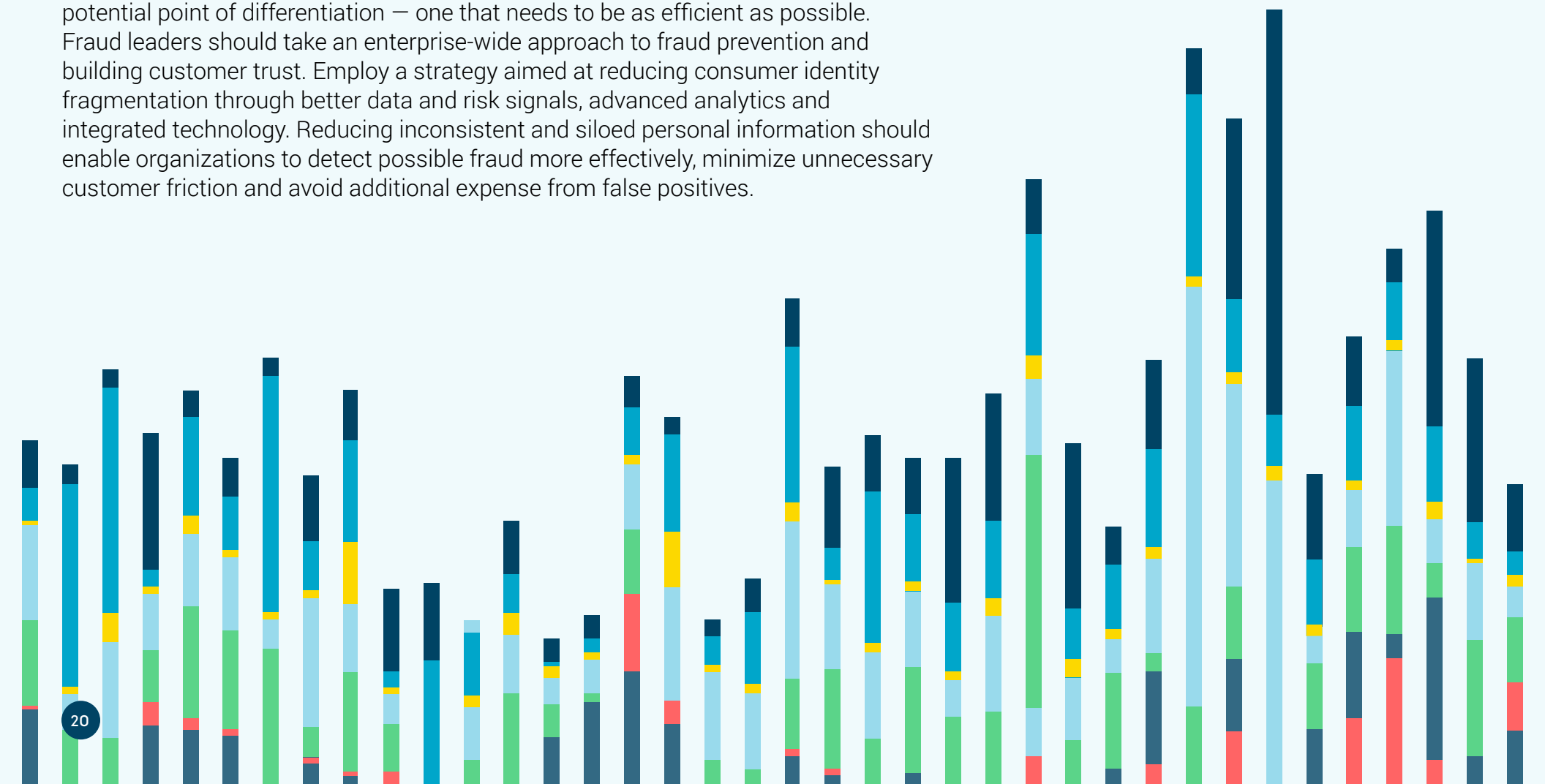
Source: TransUnion US Consumer Credit

TransUnion

Conclusion

Rising threats of fraud and monetary losses for consumers is substantial. Their fraud risk will continue as serious data breaches and scams lead to more personal information exposure. Cybercrime is an insidious business based on a supply chain of compromised personal information activated increasingly through sophisticated, AI-driven platforms.

For business leaders, protecting their organizations and customers is non-negotiable. As fraud risk rises in every channel, investment in fraud prevention represents a potential point of differentiation — one 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 aimed at reducing consumer identity fragmentation through better data and risk signals, advanced analytics and integrated technology. Reducing inconsistent and siloed personal information should enable organizations to detect possible fraud more effectively, minimize unnecessary customer friction and avoid 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), and the UK (201) and US (200) 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. 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 predominantly 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 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 survey

This online survey was conducted Nov. 21–Dec. 11, 2024 in Brazil (1000 respondents), Canada (1000), Chile (498), Colombia (995), the Dominican Republic (500), Hong Kong (998), India (1000), Kenya (500), Mexico (500), Namibia (308), the Philippines (990), Puerto Rico (326), Rwanda (361), South Africa (1000), Spain (1000), the UK (1000) and US (1000), and Zambia (411) by TransUnion in partnership with third-party research provider, Dynata. Adults 18 years of age and older 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 obtains its proprietary 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 attorneys general, 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 (BRS). 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 BRS 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. 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 or 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 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 Dec. 31, 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 organizations confidently and securely engage consumers across channels at each stage of the customer journey, helping improve conversion, reduce fraud losses and enhance the customer experience.

transunion.ca/solution/truvalidate

TransUnion