TransUnion

H2 2025 UPDATE: TOP FRAUD TRENDS

DIGITAL IDENTITY RISK ACCELERATES FRAUD LOSSES

Business leaders claim their companies lost 18% more from fraud in the last year

Executive Summary

Fraud is evolving fast and fraud-fighting teams are struggling to keep pace. A never-ending supply of compromised identity data threatens to overwhelm fraud detection systems — enabling bad actors to attack every customer touchpoint with ease. This was the sobering backdrop for the first half of 2025 fraud trends. Increased risk at new account opening from synthetic, stolen and altered identities is exposing your organization to fraud. Consumer scams targeting authorized usage and account takeover fraud have increased, putting existing customers — and your brand — at risk. To get ahead, you need a clear picture of identity — enabling greater protection from risky users while improving experiences for real customers.

In the H2 2025 Update to the TransUnion® Top Fraud Trends Report, we bring together trends, benchmarks, and identity and fraud expertise from across our global network. The report provides insight into 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, Hong Kong, India and the Philippines, UK and US; and a consumer survey in 18 countries and regions globally. See methodology on page 39 for definitions of digital fraud and other fraud types. The first half or H1 is from Jan. 1 to June 30 and the second half or H2 is July 1 to Dec. 31.

KEY TAKEAWAYS

Cost of fraud for businesses balloons

7.7%
of equivalent annual revenue on average lost due to fraud in the last year, representing USD$534 billion among 1,200 business leaders surveyed in 2025

24%
of business leaders said scam/authorized fraud was the greatest source of fraud loss, followed by 20% who reported account takeover or synthetic identity fraud

Account takeover rises in the short and long term

21%
increase in the volume of digital account takeover from H1 2024 to H1 2025

141%
uptick in the volume of digital account takeover from H1 2021 to H1 2025

Account creation was riskiest stage in the consumer lifecycle

8.3%
of all digital account creation attempts in H1 2025 were suspected of fraud, making it the highest risk stage in the consumer lifecycle

26%
increase in the rate of suspected digital fraud for account creation attempts from H1 2024 (when it was 6.6%) to H1 2025

Contents

TransUnion

Anatomy of Digital Identity Risk

Consumers' digital identities — the things you use to make countless business decisions every day — are very risky, some might even say untrustworthy. Why? There's an entire stolen consumer identity industry operating in the dark corners of the web feeding fraud schemes. The fraud trends in H1 2025 bore this out: data breaches, high-pressure phone scams, consumer cons to acquire identity data — the list goes on. Criminals use stolen or harvested data to assemble identities for exploitation. That includes creating synthetic profiles, using deepfakes and acquiring credentials for account takeovers — targeting vulnerabilities throughout the consumer lifecycle. Depending on the initial attack's success, fraudsters may employ additional strikes to get by multi-factor authentication — or use tactics like synthetic account nurturing or credit washing to resurrect creditworthy identity profiles.

Over the past year, we've seen this supply chain become very specialized. Bad actors focused their hacking and scams on accessing high-value credentials to enable specific fraud schemes. Add to this GenAI; the perfect technology for super-charging compromised data to perpetrate fraud by enabling more credible synthetic identities, deepfakes and spoofing (your organization or your customer's identity).

Digital Identity Risk Fuelled by Compromised Consumer Data

Acquisition

- Data breaches
- Phishing attacks
- Smishing attacks
- Vishing attacks
- Malware infections
- Call centre social engineering

Distribution

- Underground forums
- Dark web marketplaces

Preparation

- Synthetic ID creation
- Credential testing
- Credential validation
- Deepfake creation

Exploitation

- New account creation
- Account takeover
- Financial transactions
- SIM swap/OTP takeover

Refinement

- Credit washing
- Synthetic ID account nurturing
- Profile manipulation

GLOBAL FRAUD TRENDS

Business and Consumer Fraud Experiences

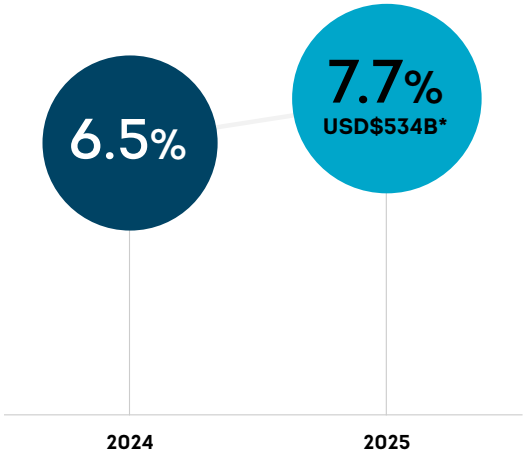
The cost of fraud rose globally

Business leaders surveyed in Canada, Hong Kong, India, the Philippines, UK and US reported their companies lost on average 7.7% of revenue in the past year due to fraud, which is up from 6.5% in 2024. That represents a total equivalent of USD$534 billion of fraud losses among the 1,200 business leaders surveyed in 2025.

Nearly a quarter (24%) of business leaders cited scam/authorized fraud as the most prominent cause of reported fraud losses — followed by account takeover and synthetic identity fraud (20% each). More business leaders reported experiencing more fraud over the past year. When asked how much various fraud types increased over the past year, 82% reported every type of fraud measured stayed the same or increased in the past year (up from 75% in 2024) — more than 40% reported increased fraud in every category.

Total Cost of Fraud

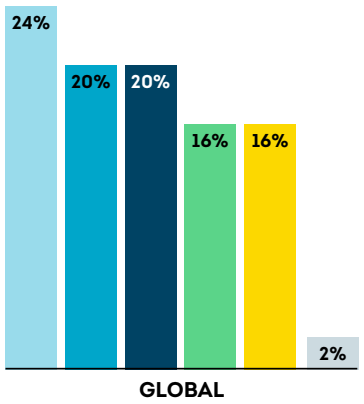
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding amount total among those surveyed globally



*USD conversion based on currency exchange value on July 16, 2025
**Not showing 2024 total due to the difference in the number of companies surveyed globally

Source: TransUnion business survey, 2025

Most Prominent Cause of Fraud Losses



- **Scam/Authorized fraud**
  Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Account takeover**
  Unauthorized 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
- **Third-party fraud**
  The use of stolen identity to open an account
- **Other**

Source: TransUnion business survey, 2025

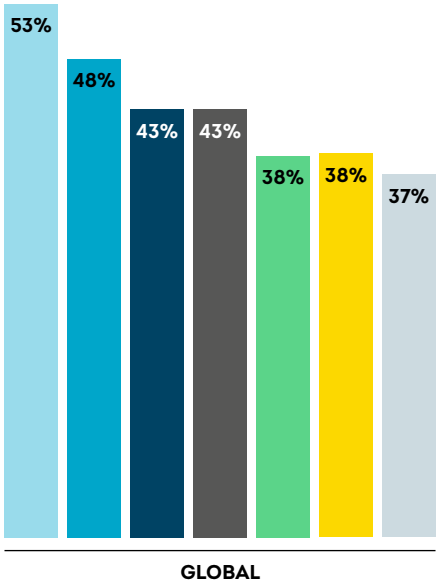
TransUnion

Fraud prevention techniques rely on identity and device signals

As the risk from consumer scams threatens identity integrity, organizations rely on a mixture of data, risk signals, technology and tools to help prevent fraud. More than half (53%) of business leaders surveyed ranked identity verification in their top three technologies for preventing fraud — followed by 48% who ranked device reputation as the most effective.

Technology Ranked as Most Effective for Preventing Fraud

The percentage of business leaders who ranked these technologies/solutions in their top three for preventing fraud.



Source: TransUnion business survey, 2025

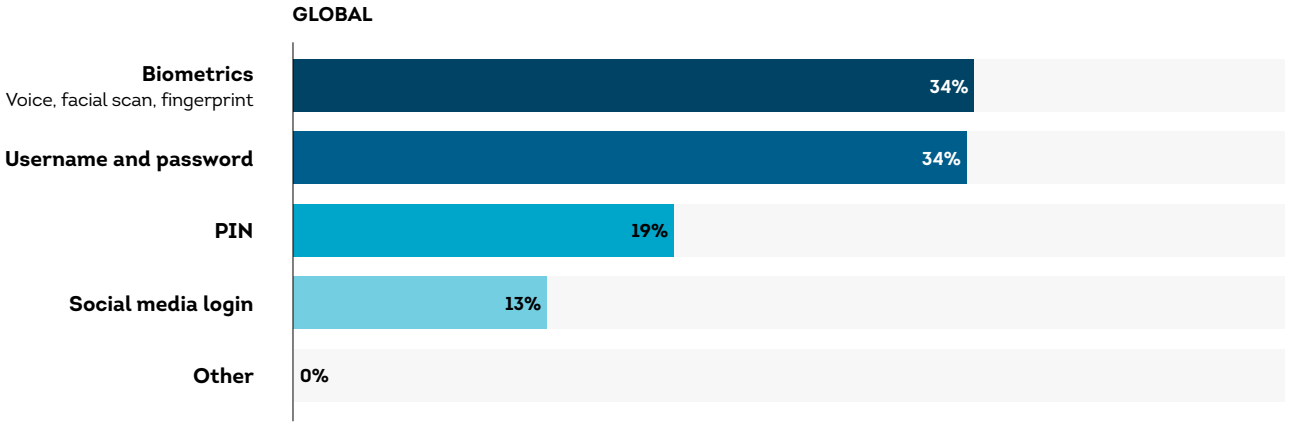
TransUnion

Dependence on passwords for customer authentication fading

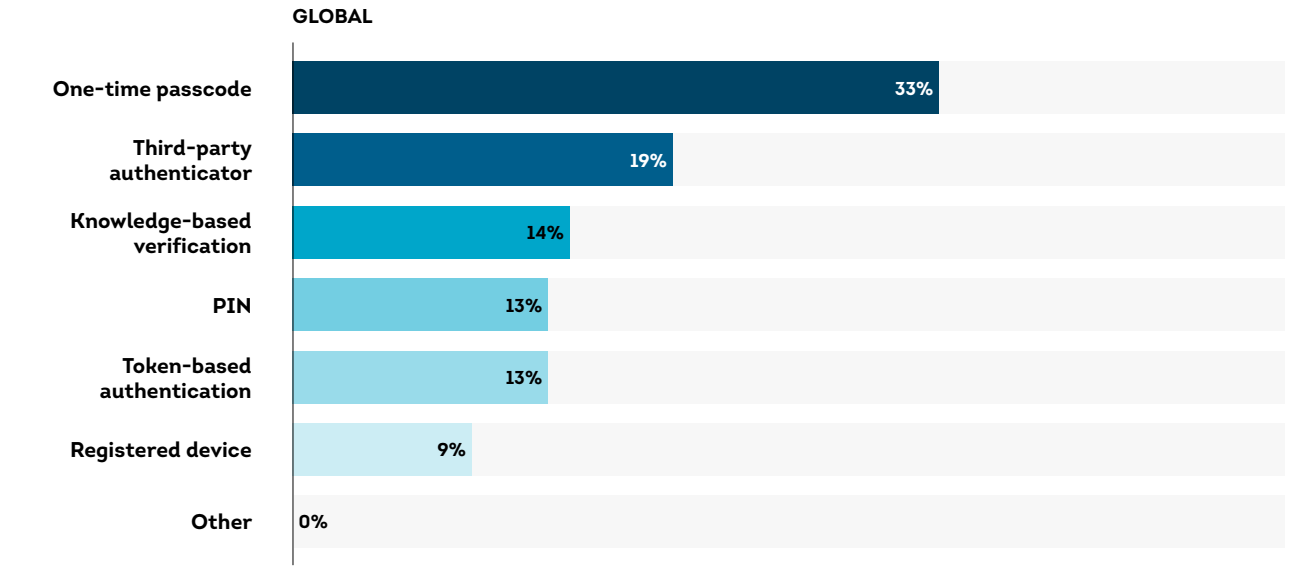
User accounts remain under threat from consumer scams and brand spoofing. Organizations appear to be shifting their approaches to embed a second factor into their authentication programs as standard practice. While more than a third (34%) of business leaders indicated they utilize usernames and passwords as the primary method of customer authentication, that's down five percentage points from 2024. Another 34% reported they use biometrics as the primary method of customer authentication, up five percentage points from 2024.

As far as a second factor for customer authentication, one-time passcodes (OTPs) remained the most popular: 33% of business leaders indicated they utilize them, down from 35% in 2024. Third-party authenticator apps was a distant second but increased in reported usage from 16% in 2024 to 19% in 2025.

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey, 2025

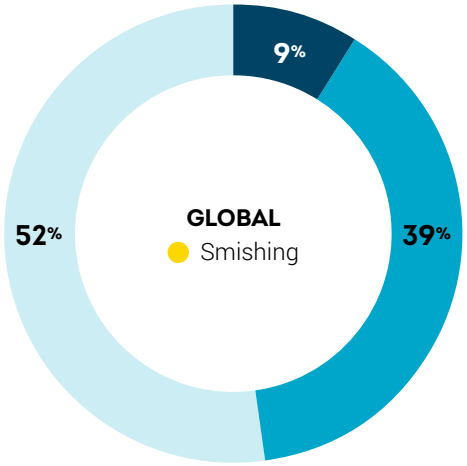
TransUnion

Consumers reported scams as most frequently experienced fraud

Nearly two in five (39%) consumers reported being targeted by an email, online, phone call or text messaging fraud scheme from February to May 2025. However, a significant portion (52%) of the population said they were unaware of being targeted. Among those who said they were targeted, the leading types of fraud consumers reported were smishing (36%), phishing (34%) and vishing (33%).

Consumers Targeted With Fraud

Percentage of consumers across 18 countries and regions who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from February to May 2025, and the most frequent scheme by which they reported being attacked.



Source: TransUnion consumer survey, 2025

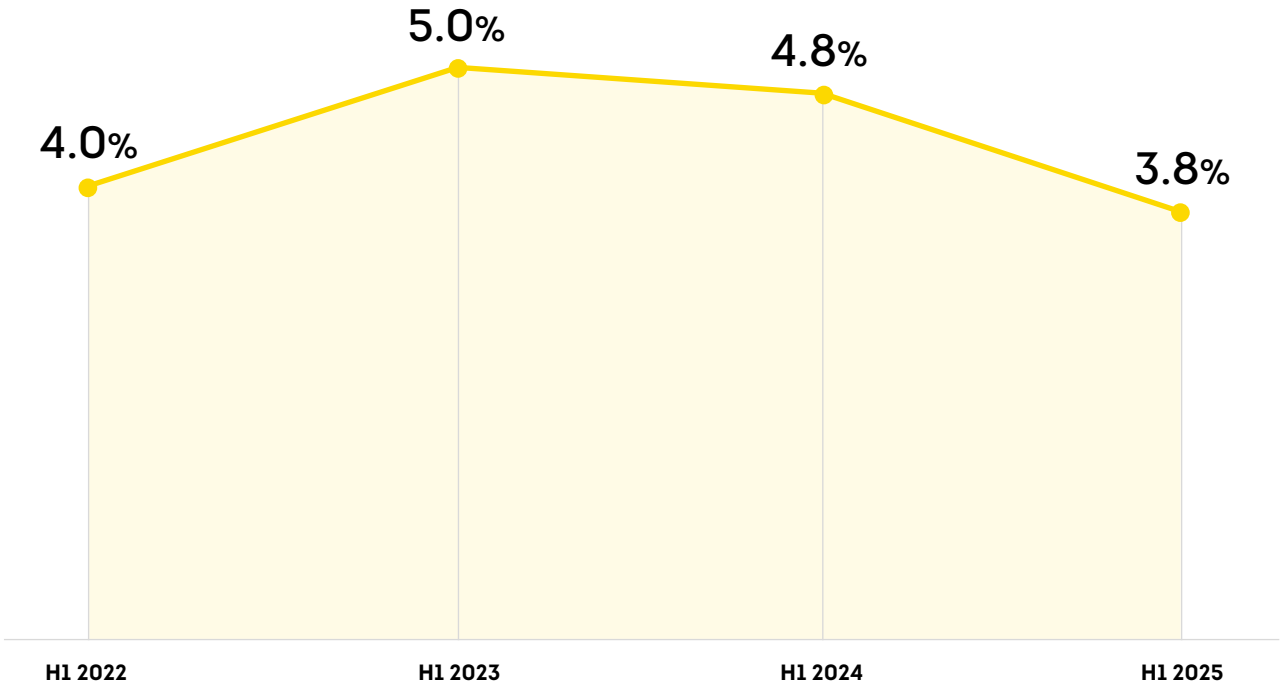
TransUnion

Digital Fraud Trends

Digital fraud rates fell for the second year in a row

Digital fraud rates fell in the first half of the year. The rate of suspected digital fraud globally among TransUnion fraud solution customers fell to 3.8% in H1 2025 from 4.8% in H1 2024 and 5.0% in H1 2023. While risky rates dropped globally, the Dominican Republic (8.6%), India (8.4%) and the Philippines (4.4%) topped the global rate.

Rate of Suspected Digital Fraud Globally

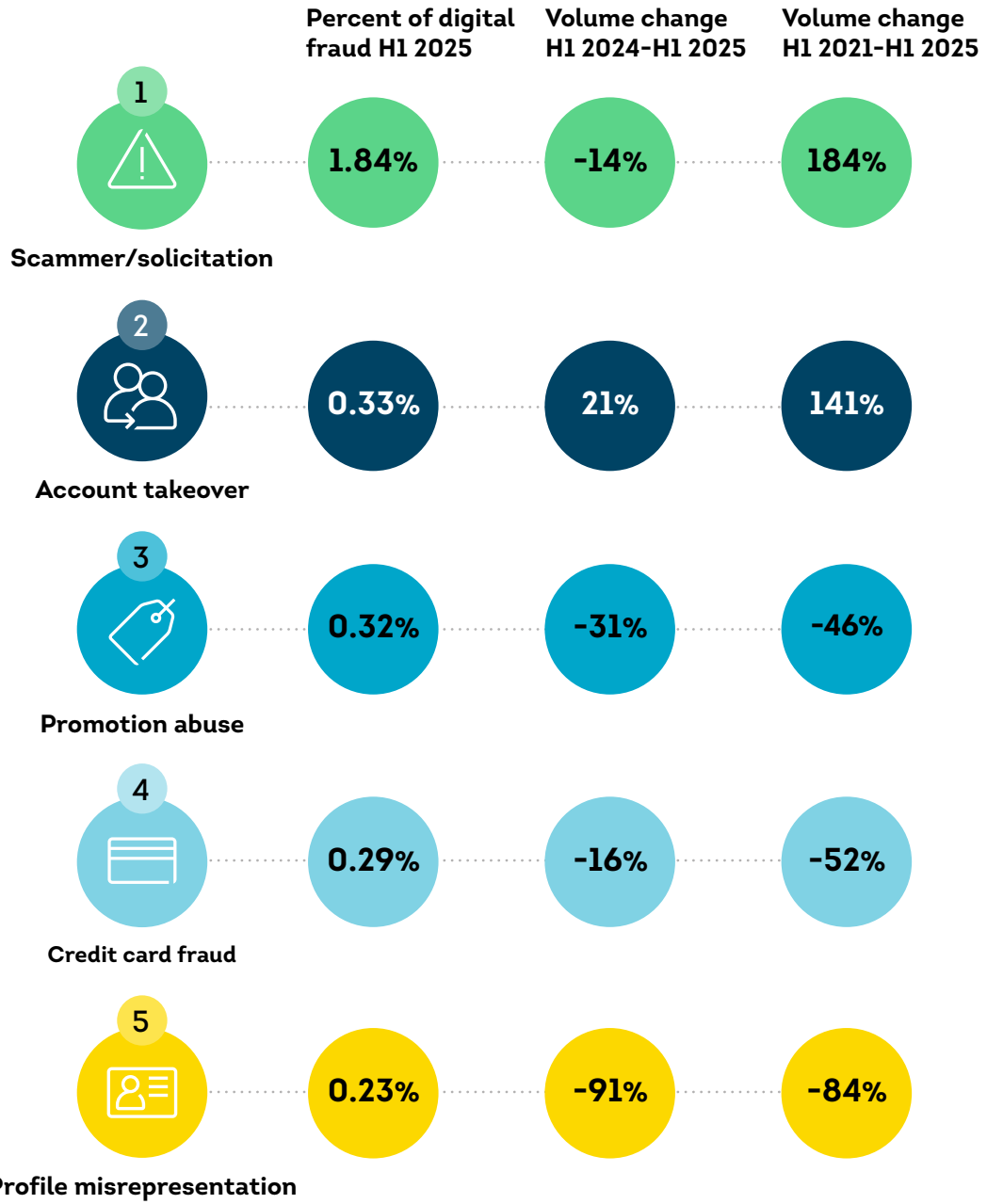


Source: TransUnion global intelligence network, 2025

Scammer/solicitation topped list of most common fraud types

At 1.8% of all suspected digital fraud types reported to TransUnion by its customers globally, scammer/solicitation (a scheme intended to trick a person into giving up something of value, i.e., account access, money, information) was the top type of digital fraud in H1 2025. However, account takeover (21% increase) was one of the fastest growing types of digital fraud volume-wise from H1 2024 to H1 2025. Scammer/solicitation fraud (184%) grew the most since H1 2021, according to TransUnion customers.

Top Digital Fraud Types and Their Growth Globally



Source: TransUnion global intelligence network, 2025

TransUnion

Not just child's play – video gaming had the highest digital fraud rates

The video gaming industry, which includes online and mobile games, experienced the largest percentage (13.5%) of suspected digital fraud attempts globally among sectors analyzed in H1 2025, representing a 28% rate and 3% volume increase in suspected digital fraud compared to H1 2024. Scammer/solicitation was the most reported fraud type by our video gaming customers.

Global Digital Fraud Attempts by Industry

- **Suspected fraud attempt rate H1 2025**
- **Top fraud type H1 2025**
- **Percent change in suspected digital fraud volume H1 2024-H1 2025**

Video gaming

H1 2025
13.5%
Scammer/solicitation

H1 2024-H1 2025
+3%

Communities
(online dating, forums, etc.)

H1 2025
8.3%
Profile misrepresentation

H1 2024-H1 2025
-33%

Gaming
(online sports betting, poker, etc.)

H1 2025
6.8%
Promotion abuse

H1 2024-H1 2025
+24%

Telecommunications

H1 2025
4.4%
Scammer/solicitation

H1 2024-H1 2025
+74%

Financial services

H1 2025
3.3%
Account takeover

H1 2024-H1 2025
-20%

Retail

H1 2025
2.6%
Credit card fraud

H1 2024-H1 2025
-64%

Government

H1 2025
2.3%
Credit card fraud

H1 2024-H1 2025
+52%

Logistics

H1 2025
2.3%
Shipping fraud

H1 2024-H1 2025
-42%

Insurance

H1 2025
1.2%
First-party application fraud

H1 2024-H1 2025
-47%

Travel & leisure

H1 2025
0.2%
Credit card fraud

H1 2024-H1 2025
-56%

Source: TransUnion global intelligence network, 2025

Digital Fraud Across the Consumer Lifecycle

Account creation is highest risk stage of the consumer lifecycle

Looking at risk by consumer lifecycle stage, new account creation is of particular concern — driven by bad actors using synthetic or stolen identities to open accounts and perpetrate all manners of first-party fraud. Of all global digital account creation transactions attempted in H1 2025 (representing 5% of all traffic volume), TransUnion found 8.3% were suspected to be digital fraud — a 28% increase over H1 2024.

Account creation risk dominated most industries in H1 2025, with the exception of financial services, insurance and government where financial transactions were the riskiest. The communities and gaming industries had the highest rates of suspected digital fraud during account creation among sectors analyzed at 21.6% and 20.0%, respectively.

Consumer Lifecycle Stage Examples

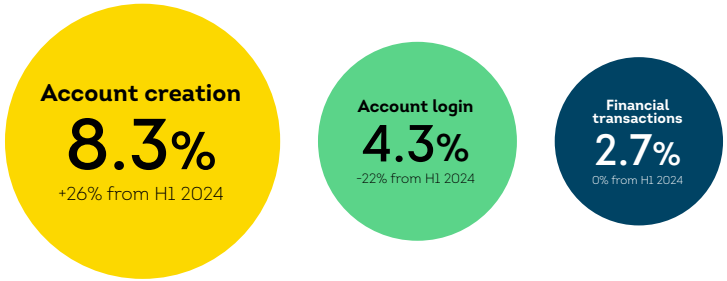
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

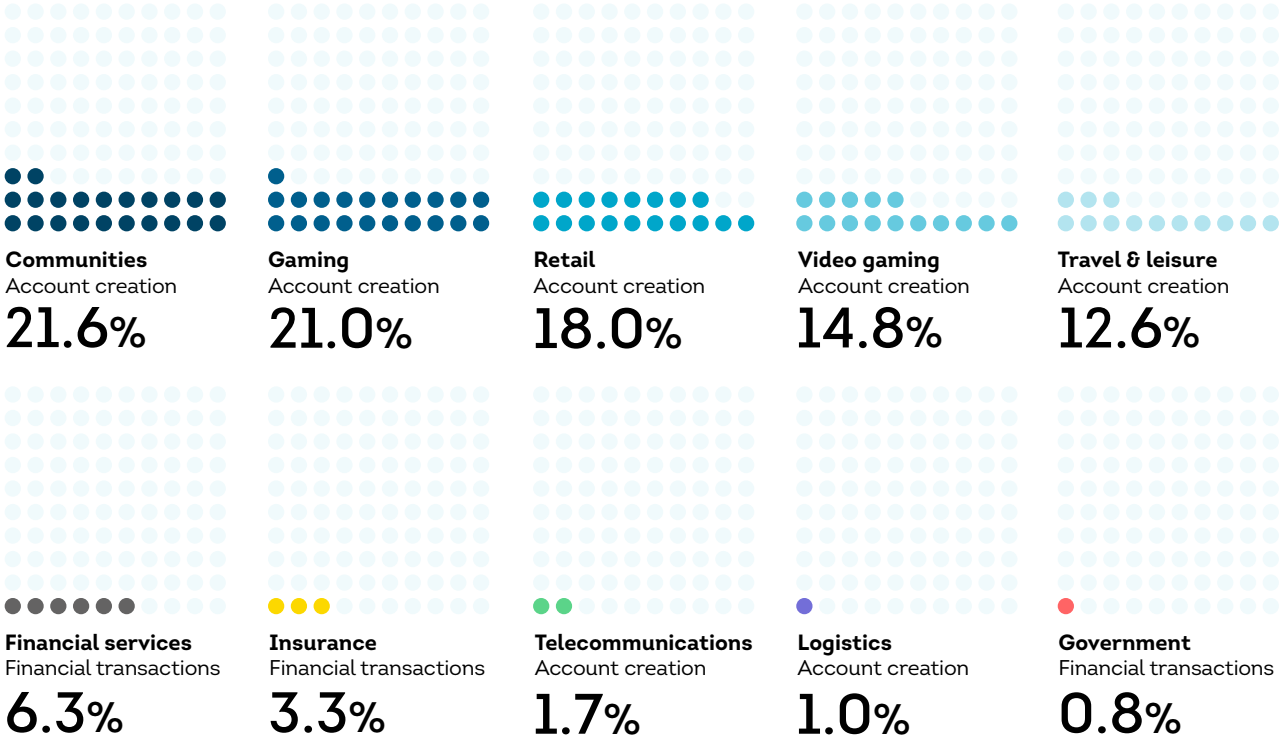
Percentage of each attempted transaction type suspected to be digital fraud globally in H1 2025



Source: TransUnion global intelligence network, 2025

Fraud Risk in the Digital Consumer Lifecycle by Industry

The consumer lifecycle stage with the highest rate of suspected digital fraud by industry and corresponding percentage in that stage globally in H1 2025



Source: TransUnion global intelligence network, 2025

TransUnion


CANADA

Canada Overview

Canadian business leaders are reporting rising losses, primarily from scams/authorized fraud, synthetic identity fraud and account takeover, while third-party fraud appears to be stabilizing. Encouragingly, more consumers appear to be informed and cautious when it comes to fraud, with slightly fewer reporting falling victim to targeted scams, a sign public awareness and business-led education efforts are making an impact. Still, phishing, smishing and vishing remain persistent threats. Identity verification tools, device reputation and behavioural biometrics are ranked as the most effective technologies in preventing fraud. These solutions are helping organizations improve detection accuracy, expand digital self-service and strike the right balance between security and convenience.

KEY TAKEAWAYS

Scam/authorized fraud and synthetic identity fraud drive major losses

29%
of fraud losses stem from scam/authorized fraud, according to Canadian business leaders

26%
of Canadian business leaders said fraud losses are due to synthetic identity fraud, up eight percentage points year over year

Identity verification and device reputation leads the fight against fraud

53%
of Canadian business leaders ranked identity verification as most effective for preventing fraud

46%
of Canadian business leaders see device reputation as a key technology for fraud defence

The total cost of fraud keeps climbing

7.2%
of equivalent revenue on average lost due to fraud among Canadian business leaders surveyed

7.7%
of equivalent revenue on average lost due to fraud among global business leaders surveyed

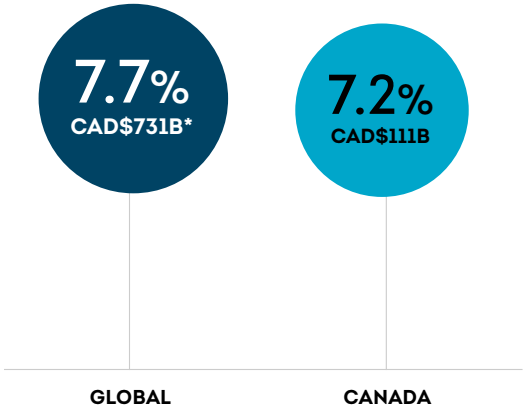
Fraud losses in Canada climb, with shifting causes

Business leaders surveyed in Canada said their companies lost the equivalent of 7.2% of their revenues due to fraud in the past year, amounting to CAD$111B, up from 6.2% and CAD$78B in 2024. While this was slightly below the global average of 7.7%, the increase reflects a growing challenge for Canadian businesses.

Scam/authorized fraud remained the most prominent cause of fraud loss at 29%, according to Canadian business leaders, though this category saw a slight decline from the previous year. Synthetic fraud, however, surged to 26% from 18%, marking the largest increase in Canada and surpassing the percentage in all other markets surveyed. Meanwhile, third-party fraud and account takeover declined by three and four percentage points, respectively, which could be attributed to stronger identity verification practices. Despite these improvements, fraudsters continue to adapt, shifting tactics and exploiting new vulnerabilities. Canadian organizations must remain vigilant as the landscape evolves, balancing innovation with resilience in the face of increasingly sophisticated threats.

Total Cost of Fraud

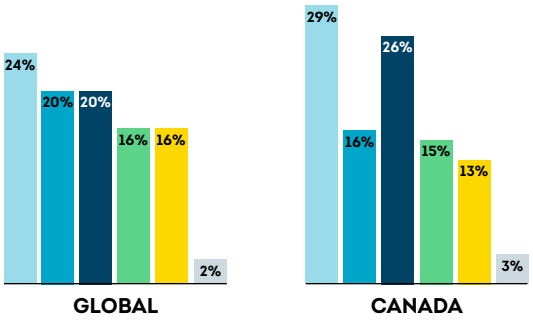
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding monetary amount total



*Based on currency exchange value on July 16, 2025

Source: TransUnion business survey, 2025

Most Prominent Cause of Fraud Losses



- **Scam/Authorized fraud**
  Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Account takeover**
  Unauthorized 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
- **Third-party fraud**
  The use of stolen identity to open an account
- **Other**

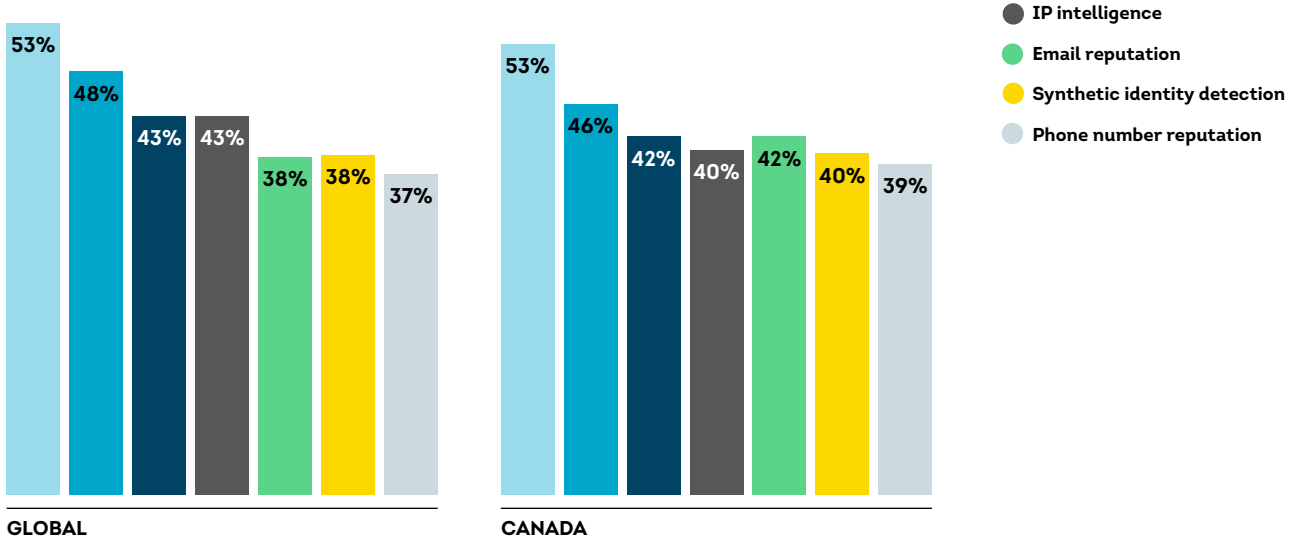
Source: TransUnion business survey, 2025

Technology strengthens Canada's fraud defence strategy

Technology continues to play a pivotal role in Canada's fight against fraud, with identity verification ranked as the most effective technology for preventing fraud by business leaders surveyed both nationally and globally. As consumers increasingly transact through digital channels, businesses are seeing strong results from combining device fingerprinting and reputation technologies with behavioural biometrics and intelligence signals from email, phone and IP address data. These layered approaches help detect fraud early while maintaining seamless user experiences. While high detection rates remain the top priority when investing in fraud prevention tools, Canadian organizations also emphasize the importance of minimal friction to reduce consumer abandonment. This balance between security and usability is critical as fraudsters evolve their tactics. By leveraging advanced technologies, businesses in Canada are not only improving fraud detection but also enhancing trust and operational efficiency in a rapidly digitizing economy.

Technology Ranked as Most Effective for Preventing Fraud

The percentage of business leaders who ranked these technologies/ solutions in their top three for preventing fraud



Source: TransUnion business survey, 2025

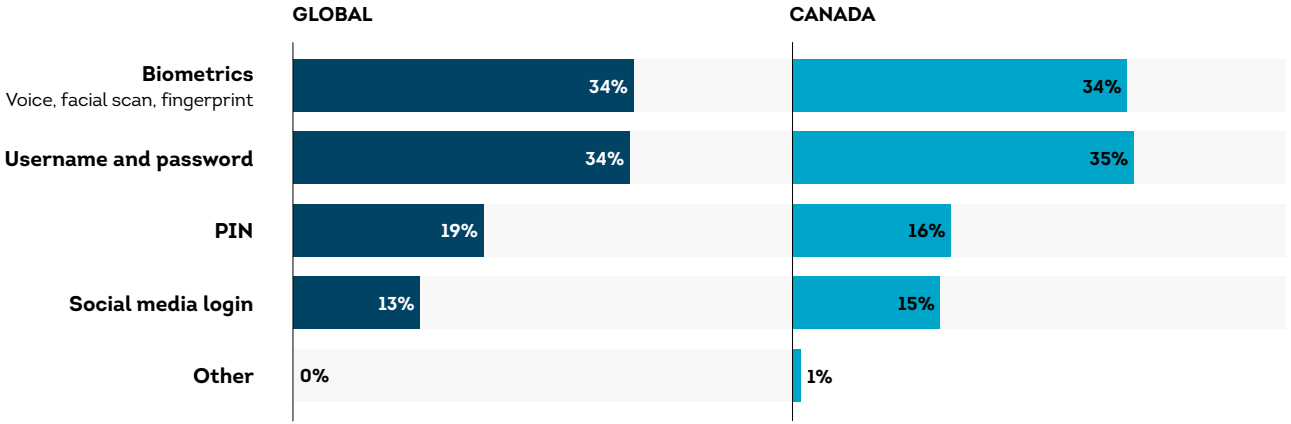
TransUnion

Evolving authentication practices reflect shifting fraud priorities

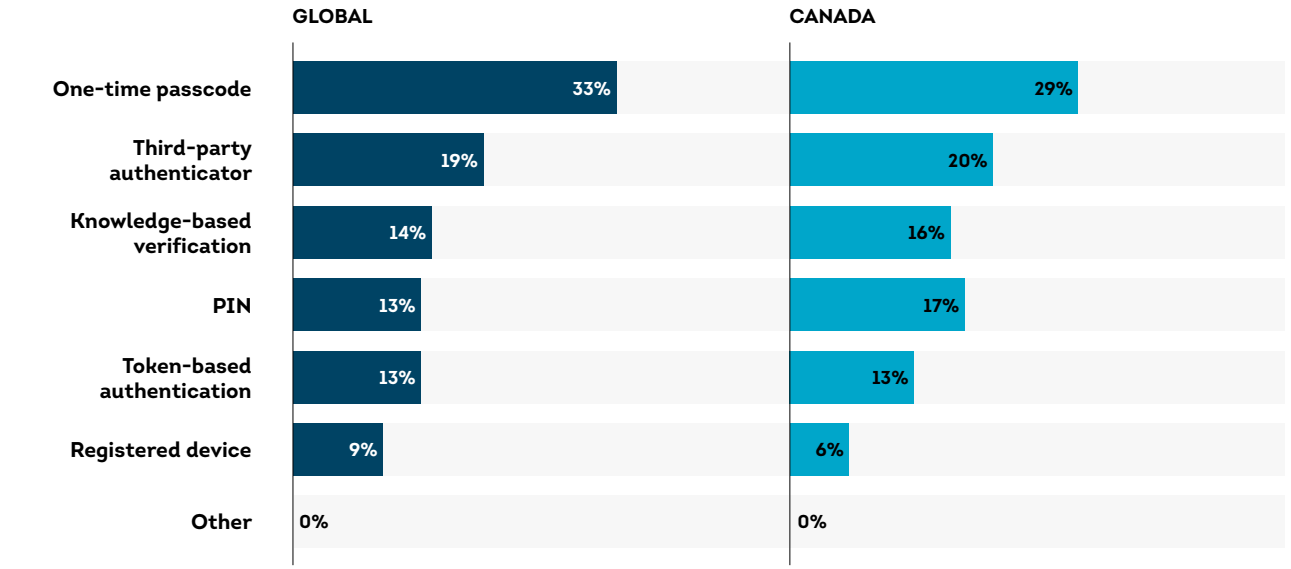
Authenticating consumers continues to be a vital part of fraud prevention strategies, especially as digital engagement grows. Despite its limitations, username and password remains the most widely used primary authentication method, according to Canadian business leaders. However, biometric authentication is gaining momentum with reported primary authentication usage in Canada increasing nine percentage points from 2024 (to 34% in 2025). One-time passcodes and third-party authenticators are the top two secondary methods used to authenticate consumers according to business leaders in Canada possibly due to their balance of security and convenience.

Notably, 34% of business leaders in Canada planned to eliminate certain authentication methods within the next 12 to 18 months, up 13 percentage points year over year. This shift reflects a broader effort to modernize identity verification practices and adapt to evolving fraud tactics. As fraudsters become more sophisticated, businesses are rethinking how to authenticate users in ways that are both secure and seamless, ensuring trust is maintained without compromising customer experiences.

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey, 2025

TransUnion

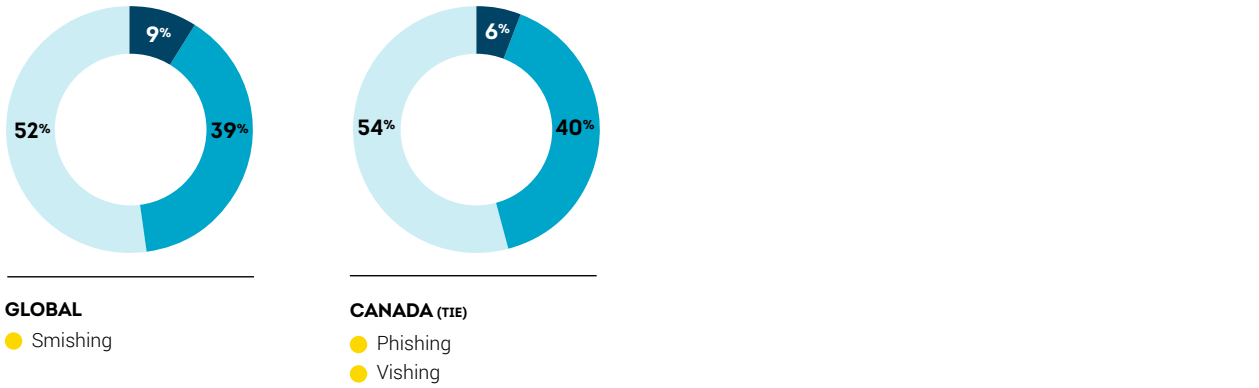
Consumers face emerging fraud threats

Nearly half (46%) of Canadian consumers reported being exposed to email, online, phone call or text messaging fraud attempts between February and May 2025. However, only 6% said they fell victim, lower than the global average of 9%. This suggests Canadians are becoming more alert and proactive in identifying suspicious activity. Phishing and vishing are the most common scams reported by consumers in Canada, with smishing increasing steadily. Globally, smishing has overtaken other methods as the most reported fraud scheme.

Fraudsters are becoming more calculated and refined in their approaches, crafting scams that closely mimic legitimate communications and behaviours. These scams are often personalized, leveraging stolen data and social engineering to bypass consumer defences. Canadian consumers are now facing threats that are more nuanced, making detection increasingly difficult. While the lower victimization rate is encouraging, the evolving nature of fraud highlights the need for continued awareness and education to help individuals recognize and respond to deceptive tactics with confidence.

Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from February to May 2025, and the most frequent scheme by which they reported being attacked.



Source: TransUnion consumer survey, 2025

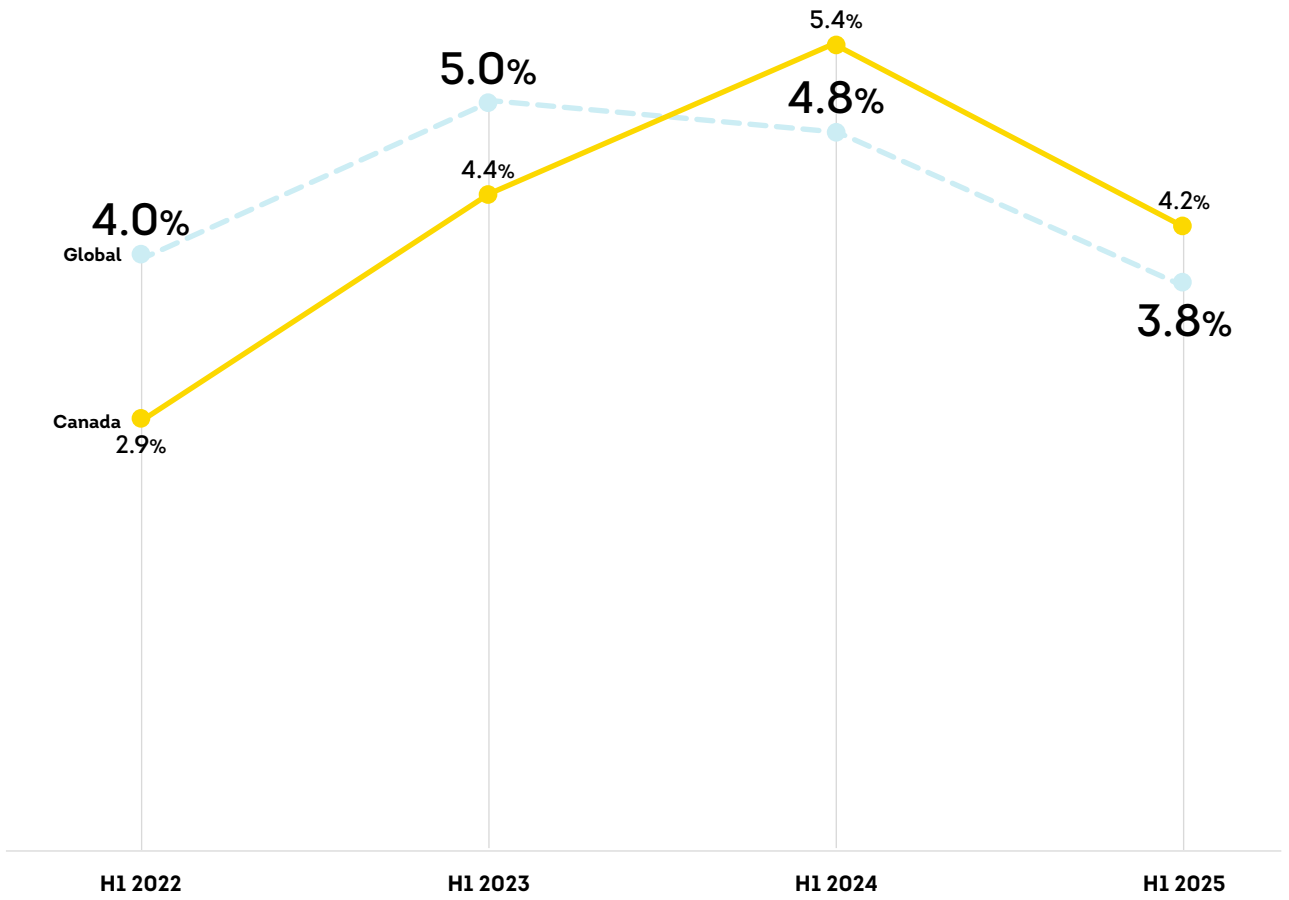
Digital Fraud Trends

Rate of suspected digital fraud declines in Canada

Canada has experienced a notable decline in the rate of suspected digital fraud attempts, dropping from 5.4% in the first half of 2024 to 4.2% in the same period of 2025, according to TransUnion data. This mirrors the global trend where the average rate also fell from 4.8% to 3.8%, suggesting broader improvements in fraud detection and prevention across regions.

While the reduction is encouraging, it comes amid increasingly complex and adaptive fraud tactics. Canadian businesses and consumers alike are benefiting from enhanced security measures and growing awareness, but the evolving nature of digital fraud means continued vigilance is essential. As fraudsters refine their methods, even small improvements in detection can have a significant impact on reducing risk and protecting digital interactions.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network, 2025

TransUnion

Online communities lead Canada's digital fraud exposure

In the first half of 2025, web-based communities, including forums and dating platforms, experienced the highest rate of suspected digital fraud attempts where the consumer was in Canada when transacting across all industries analyzed, reaching 11.4%. This sector also saw a 68% year-over-year increase in suspected digital fraud volume from Canada, underscoring how fraudsters are increasingly exploiting socially driven platforms where trust and engagement are high. Gaming followed closely with a 10.9% fraud attempt rate, increasing a modest 16% year over year in suspected digital fraud volume.

Meanwhile, traditional sectors like financial services and insurance have seen significant year-over-year declines in suspected digital fraud volume, likely due to stronger security protocols and improved identity verification. Video gaming, logistics, retail and telecommunications also showed reductions.

These trends could indicate fraudsters are evolving, not just avoiding industries with stronger defences but shifting from third-party fraud to more sophisticated methods like synthetic identity fraud. Even sectors with improved identity verification remain vulnerable. For Canadian organizations, staying ahead means reinforcing existing protections while anticipating emerging fraud tactics across digital environments.

Digital Fraud Attempts From Canada by Industry

- **Suspected fraud attempt rate H1 2025**
- **Percent change in suspected digital fraud volume H1 2024-H1 2025**

Communities
(online dating, forums, etc.)

H1 2025
11.4%

H1 2024-H1 2025
+68%

Gaming
(online sports betting, poker, etc.)

H1 2025
10.9%

H1 2024-H1 2025
+16%

Government

H1 2025
8.9%

H1 2024-H1 2025
+9%

Video gaming

H1 2025
6.3%

H1 2024-H1 2025
-39%

Logistics

H1 2025
2.2%

H1 2024-H1 2025
-39%

Financial services

H1 2025
2.1%

H1 2024-H1 2025
-40%

Insurance

H1 2025
2.0%

H1 2024-H1 2025
-27%

Retail

H1 2025
1.1%

H1 2024-H1 2025
-72%

Telecommunications

H1 2025
0.2%

H1 2024-H1 2025
-45%

Source: TransUnion global intelligence network, 2025

Consumer lifecycle stages show distinct fraud risks

Globally, suspected digital fraud rates varied across consumer lifecycle stages in the first half of 2025, with 8.3% of all account creations suspected to be digital fraud attempts, 4.3% of account logins and 2.7% of financial transactions. In Canada, the pattern shifts. Account login had the highest risk at 13.0% followed by account creation at 4.0% and financial transactions at just 0.8%. These differences highlight how fraud exposure varies by interaction type and geography.

As for where in the consumer lifecycle the most suspected digital fraud attempts occurred by industry for transactions where the consumer was in Canada in H1 2025, telecommunications led with a 35.1% rate at account creation followed by communities at 30.4%, also at account creation. Gaming had the highest risk at account login with a 12.7% suspected digital fraud rate for those types of transactions, while government (9.8%) and insurance (1.4%) also faced the highest risk at login. Financial services had the highest risk in the consumer lifecycle for financial transactions with a 4.0% suspected digital fraud rate for those types of transactions, and video gaming (12.2%) and retail (8.4%) showed an elevated risk at account creation. These figures highlight the need for tailored fraud prevention strategies across lifecycle stages and industries.

Consumer Lifecycle Stage Examples

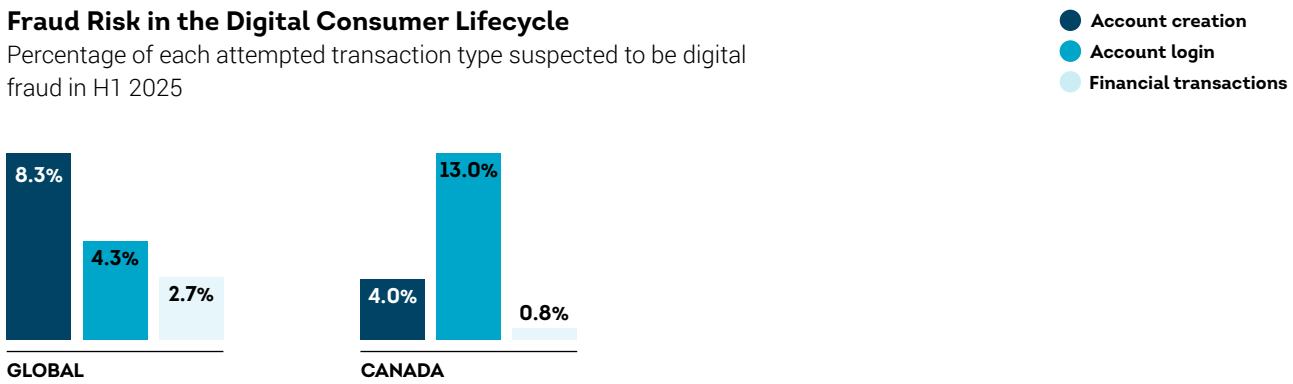
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

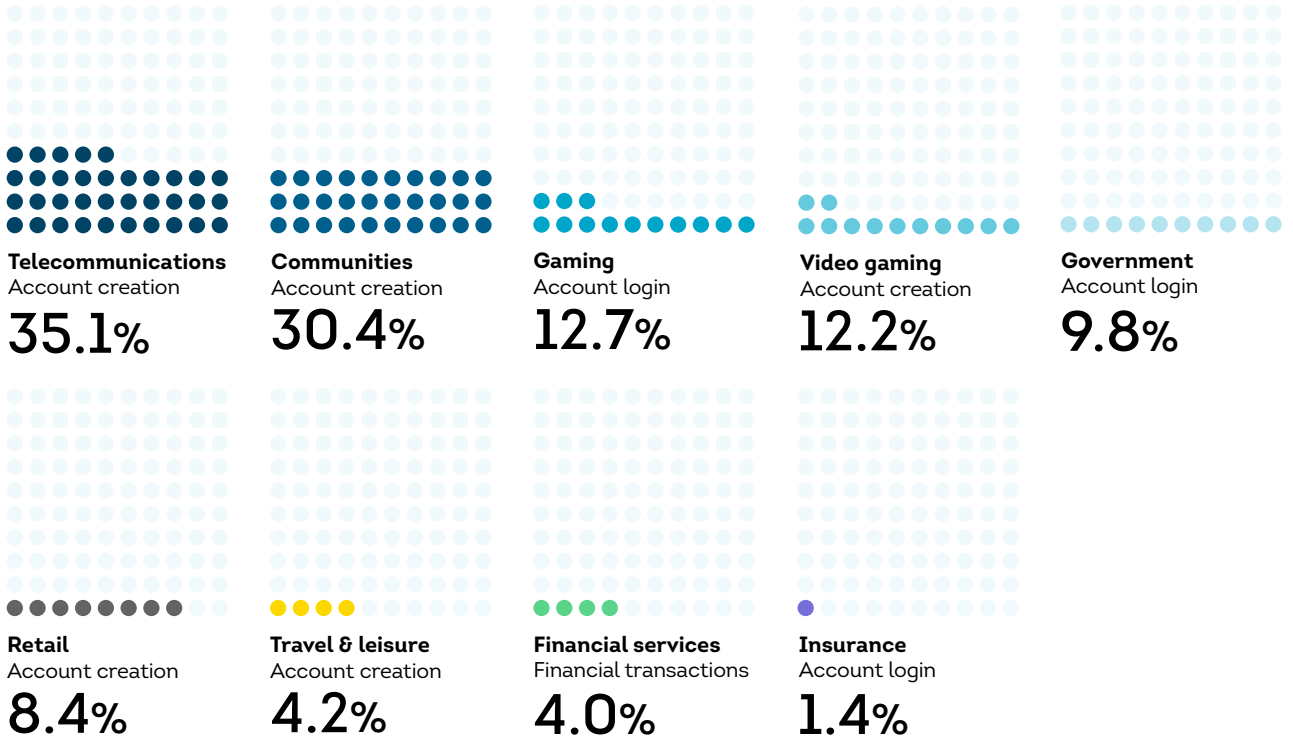
Percentage of each attempted transaction type suspected to be digital fraud in H1 2025



Source: TransUnion global intelligence network, 2025

Fraud Risk in the Digital Consumer Lifecycle by Industry

The consumer lifecycle stage with the highest rate of suspected digital fraud from Canada by industry and the corresponding percentage in that stage in H1 2025



Source: TransUnion global intelligence network, 2025


UNITED
STATES

United States Overview

Fraud schemes are getting more sophisticated, and the US is a target-rich environment for bad actors. US fraud prevention leaders recognize the risk and urgency to bolster their defences to keep up as more of their business is done online. It's no small task. Compromised identities from non-stop data breaches and consumer scams increase risk across the consumer lifecycle. In the first half of 2025, this issue played out in many ways. US business leaders identified account takeover (ATO) fraud as the leading reason for fraud losses. Given the identity theft scams consumers face, coupled with their preferences for more vulnerable account authentication methods, customer accounts will be prime targets for attack.

At the same time, account creation was the riskiest stage of the digital consumer lifecycle — and it's no wonder. With the use of GenAI tools, fraudsters can create credible synthetic identities. These identities, complete with deepfake documents, legitimate credit histories and doctored online accounts, are hard to distinguish from real people. Given the pipeline of consumer data from data breaches and consumer scams in the US, it's only getting more difficult to see digital identity risk clearly.

KEY TAKEAWAYS

Cost of fraud rising for organizations

9.8%
of equivalent revenue on average lost due to fraud, up 46% from 2024, representing USD$114 billion of fraud loss in the past year among 200 business leaders surveyed in the US

USD$2.7 billion
in lender exposure to suspected synthetic identities for US auto loans, bank credit cards, retail credit cards and unsecured personal loans

Stolen identity supply chain feeding more sophisticated fraud

77%
of US data breaches included full Social Security number in H1 2025, an 8% increase over H1 2024 and an all-time high since TransUnion started reporting it in 2020

51%
of US consumers reported being targeted by email, online, phone call and text messaging fraud – led by phishing, smishing and vishing designed to steal identity credentials – from February to May 2025

Account creation posed highest fraud risk across the consumer lifecycle

4.2%
of all US digital account creation attempts were suspected of digital fraud; this was the highest risk stage in the consumer lifecycle, and higher than overall suspected digital fraud rate of 3.5% for all US transactions

47%
of US business leaders surveyed identified new account fraud types – first-party, third-party and synthetic identity – as leading sources of fraud losses in the past year

Business and Consumer Fraud Experiences

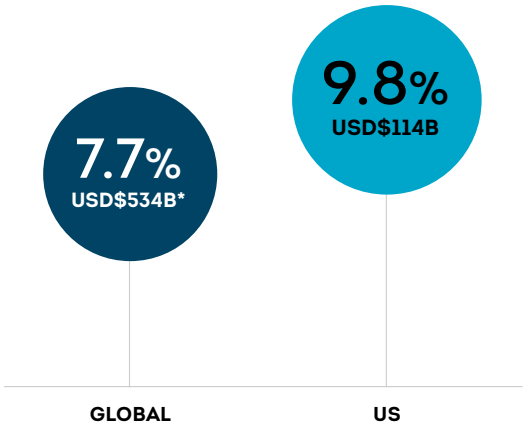
The cost of fraud rising

Reducing exposure to fraud losses is a key role for fraud risk leaders. Their peers surveyed in the US reported their companies lost (on average) the equivalent of 9.8% of revenue due to fraud in the past year. This is a 46% increase over 2024. US leaders also reported fraud losses as a percentage of revenue that was 27% higher than the global average of 7.7%. In the US, that represents a total of USD$114 billion of fraud losses among the 200 businesses leaders surveyed.

Nearly a third (31%) of US business leaders cited ATO as the most prominent cause of reported fraud losses followed by synthetic identity fraud (24%) and scam/authorized fraud (23%).

Total Cost of Fraud

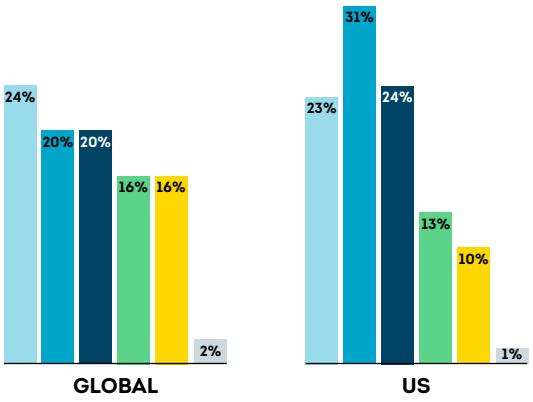
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding monetary amount total



*USD conversion based on currency exchange value on July 16, 2025.

Source: TransUnion business survey, 2025

Most Prominent Cause of Fraud Losses



- **Scam/Authorized fraud**
  Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Account takeover**
  Unauthorized 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
- **Third-party fraud**
  The use of stolen identity to open an account
- **Other**

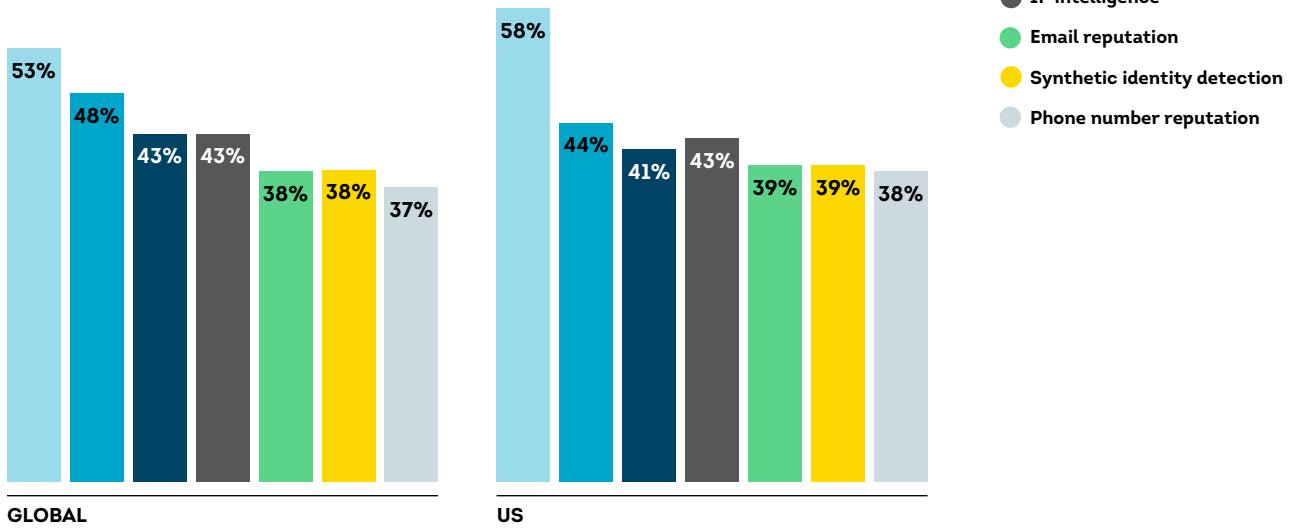
Source: TransUnion business survey, 2025

Identity verification ranked as top fraud-fighting technology

Identity verification continues to be the cornerstone of fraud prevention technology in the US. More than half (58%) of US business leaders surveyed ranked identity verification in their top three most effective technologies for preventing fraud. Following identity verification, device reputation (44%), IP intelligence (43%) and behavioural biometrics (41%) were ranked as the most effective.

Technology Ranked as Most Effective for Preventing Fraud

The percentage of business leaders who ranked these technologies/ solutions in their top three for preventing fraud



Source: TransUnion business survey, 2025

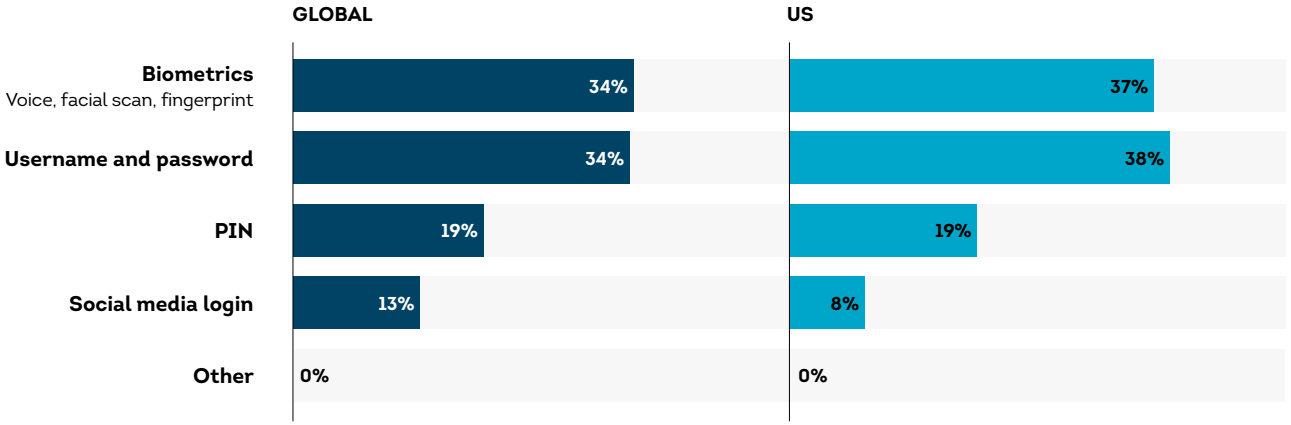
TransUnion

Biometrics catch up with passwords as primary authentication method

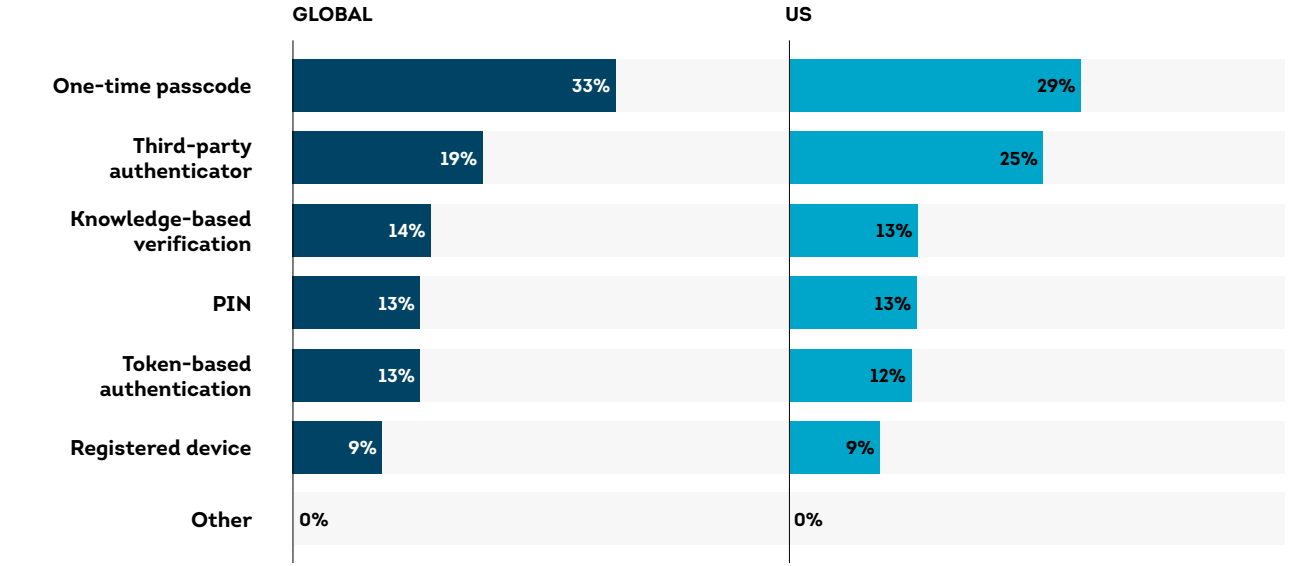
User credentials remain under threat from consumer scams and data breaches. It's no wonder US business leaders reported ATO as the primary reason behind fraud losses. To stem the tide, US business leaders appear to be moving away from simple username and password authentication to embedding biometric verification into their authentication programs. While more than a third (38%) of US business leaders said they still utilize usernames and passwords as their primary methods of customer authentication, that's down 14% from 2024. Another 37% reported they use biometrics as their primary method of customer authentication, up 42% from 2024.

One-time passcodes remained the most popular second factor for customer authentication, with 29% of US business leaders indicating they utilize them, down from 35% in 2024. Third-party authenticator apps (the second most popular second factor for customer authentication, according to US business leaders) increased in reported usage from 20% in 2024 to 25% in 2025.

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey, 2025

TransUnion

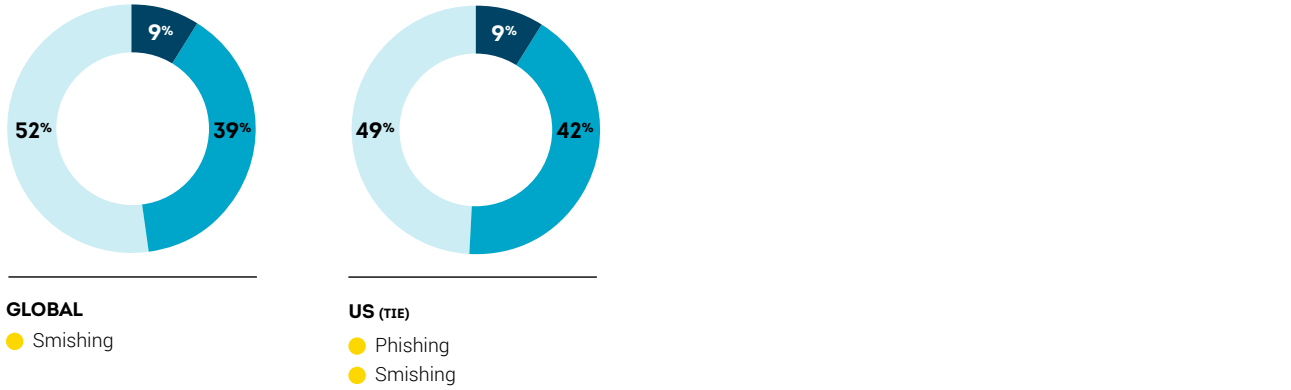
Phishing and smishing tied for most common consumer-reported fraud scheme

More than half (51%) of US consumers reported being targeted by an email, online, phone call or text messaging fraud scheme, and 9% said they fell victim from February to May 2025. However, a significant portion of the population didn't recognize potential fraud; 49% said they were unaware of being targeted by fraud schemes.

Phishing (fraudulent emails, websites, social posts, QR codes, etc. meant to steal data) and smishing (fraudulent text messages meant to trick someone into revealing data) were each reported by 46% of US consumers who said they were targeted with fraud, making them the leading types of fraud they experienced.

Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from February to May 2025, and the most frequent scheme by which they reported being attacked.



Source: TransUnion consumer survey, 2025

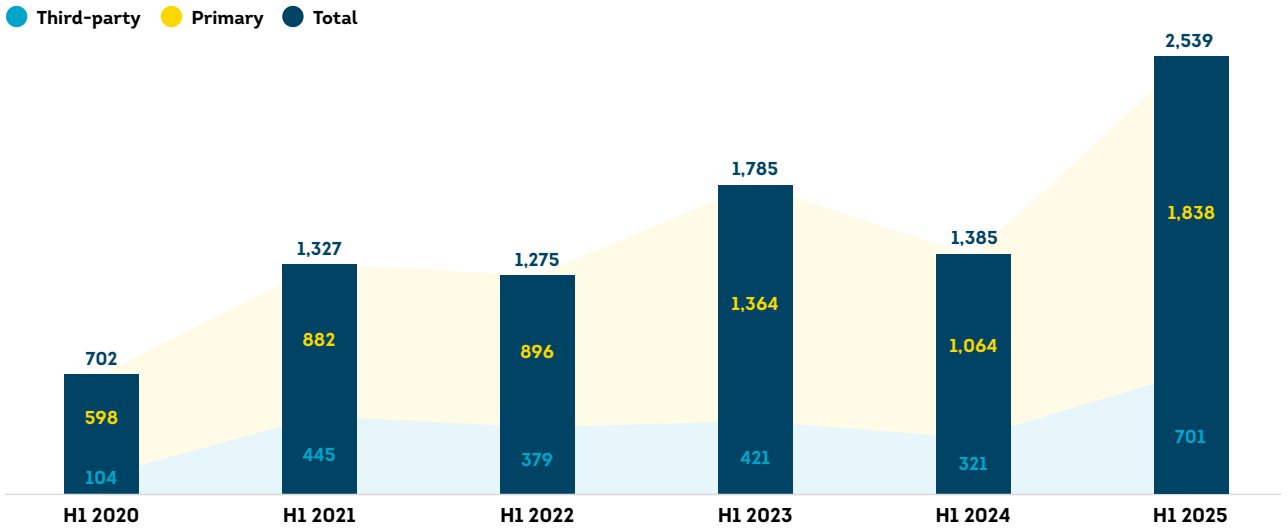
Identity Data Exposure Trends

Number of and severity of US data breaches at record levels

Criminals continue to shift their data breach attacks to gather high-quality credentials. With more frequent attacks targeting fewer individuals per incident, the US experienced an 83% increase in data breach volume in the first half of 2025 compared to the same time in 2024 — and the highest level during the time period measured. However, the median number of individuals impacted per breach dropped to 301 in H1 2025 compared to 616 during the same time in 2024 — and down from a six-year period high of 5,278 in 2022. These attacks may seek data that's not readily available to criminals using the dark web data marketplace to source identity data for fraud schemes. It also aligns with frequently reported consumer fraud scams, including smishing, phishing and vishing.

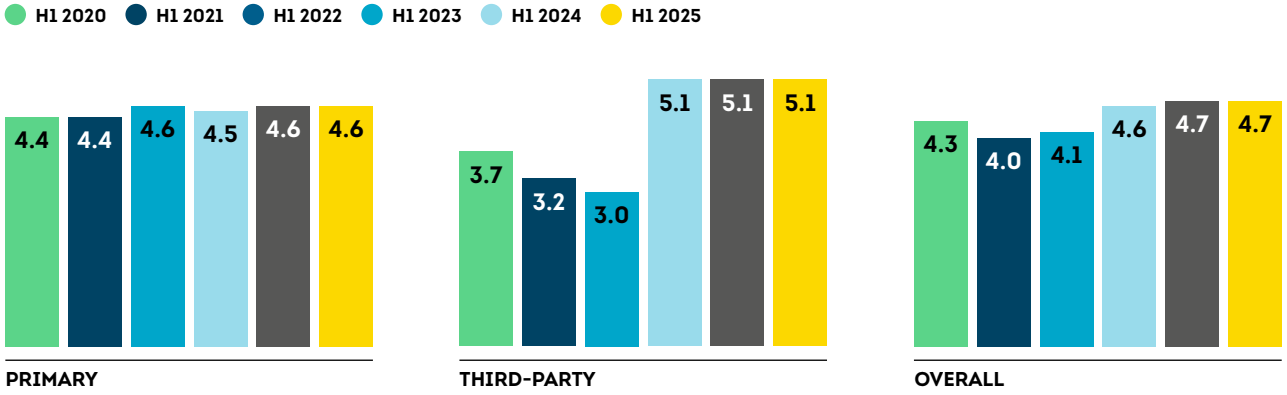
Due to the targeting of high-risk credentials like Social Security numbers, average breach severity (the ability of a breach to enable identity fraud) as measured by TransUnion TruEmpower™ Breach Risk Score (BRS) — a leading indicator of future fraud — remained at the highest level in the period examined. Third-party breaches involving attacks on organizations providing business services to brands remained significantly riskier than those targeting consumer-facing organizations.

US Data Breach Volume



Source: TransUnion global intelligence network, 2025

Average Breach Risk Score for US Data Breaches



Source: TransUnion global intelligence network, 2025

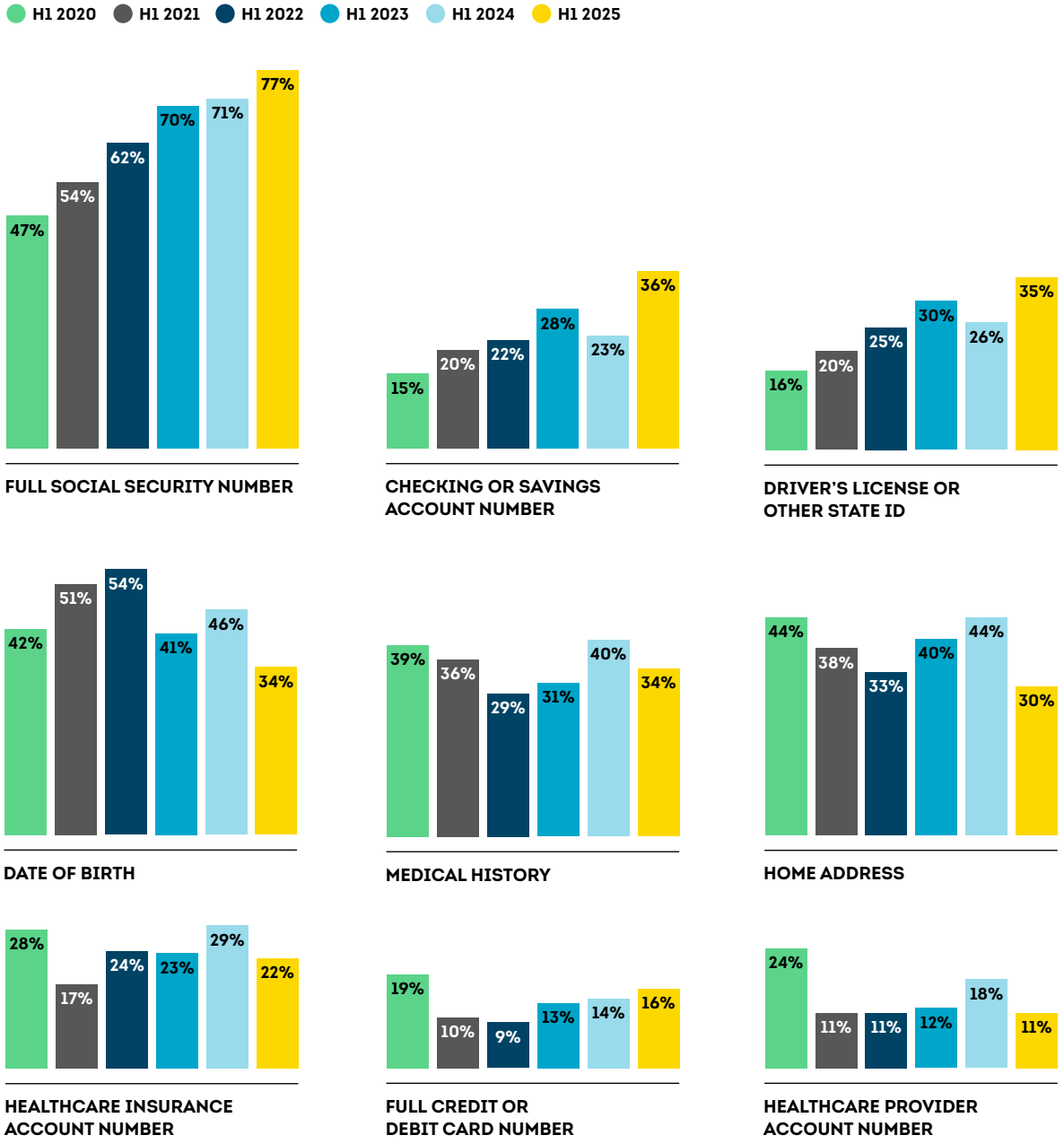
A primary data breach represents a direct attack on an organization. A third-party data breach, also known as a supply-chain attack, value-chain attack or backdoor breach, is when an attacker accesses an entity's network via third-party vendors or suppliers — payroll processing or medical billing, for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

High-value identity credentials prioritized by criminals

In the first half of 2025, criminals appeared to focus on high-value credentials to enable future fraud and consumer scams. TransUnion found full Social Security numbers were exposed in 77% of US data breaches in H1 2025 (an 8% increase over H1 2024 and the highest point in this research), which could support new account, synthetic, tax refund and government benefits identity fraud, among others. Checking/savings account data exposure showed significant growth, reaching 36% from 23% in H1 2024 — possibly leading to more ATO or ACH/payments fraud. Driver's license data exposure also grew from 26% in H1 2024 to 35% in H1 2025, possibly fuelling identification document AI deepfakes.

Top 10 Exposed Identity Credentials in US Data Breaches H1 2025

Percentage of credentials exposed in a data breach



Source: TransUnion global intelligence network, 2025

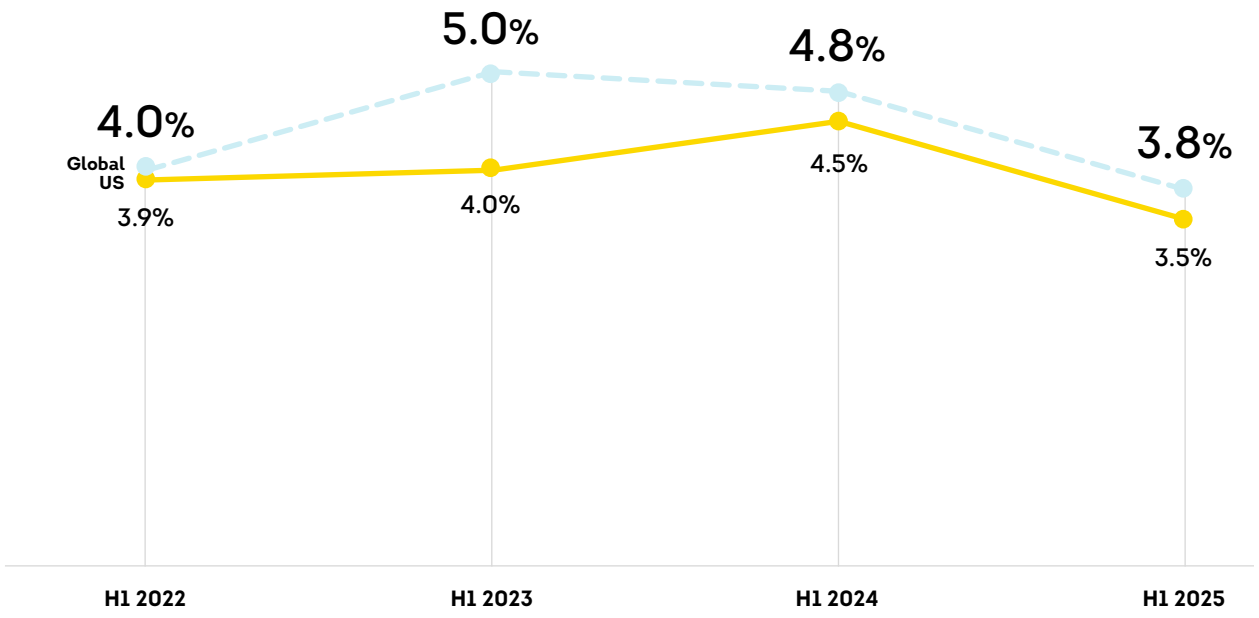
TransUnion

Digital Fraud Trends

Suspected digital fraud rate falls

US digital fraud risk fell in the first half of the year for the first time in three years in H1 2025. The rate of suspected digital fraud for attempted transactions where the consumer was in the US fell to 3.5% in H1 2025 after spiking in H1 2024 at 4.5%. This was slightly lower than the global average of 3.8% in H1 2025. The drop in the digital fraud rate is most likely a combination of organizations increasing use of multifactor authentication to stymie ATO attacks and consumers being more suspicious of phishing, vishing and smishing schemes. At the same time, compromised identities are supporting increasingly sophisticated fraud attacks that will continue to represent risk for your organization.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network, 2025

TransUnion

Communities industry experienced the highest digital fraud risk

The communities industry, which includes web properties like online forums and dating sites, experienced the largest percentage (13.7%) of suspected digital fraud for attempted transactions where the consumer was in the US in H1 2025. This represents a 139% volume increase in suspected digital fraud from H1 2022 to H1 2025 and 64% from H1 2024 to H1 2025. Online community users rely on organizations to provide trust and safety — protecting them from seller and other scams while using their platforms. Maybe not surprising, communities customers of TransUnion reported profile misrepresentation and scammer/solicitation as the most frequent types of digital fraud they witnessed in H1 2025 globally, illustrating the value of these platforms for fraudsters.

Fraud Attempts From United States by Industry

- **Suspected fraud attempt rate H1 2025**
- **Percent change in suspected digital fraud volume H1 2024-H1 2025**

Communities
(online dating, forums, etc.)

H1 2025
13.7%

H1 2024-H1 2025
+64%

Gaming
(online sports betting, poker, etc.)

H1 2025
9.6%

H1 2024-H1 2025
-10%

Video gaming

H1 2025
8.3%

H1 2024-H1 2025
-38%

Retail

H1 2025
3.5%

H1 2024-H1 2025
-46%

Financial services

H1 2025
3.4%

H1 2024-H1 2025
-18%

Logistics

H1 2025
1.9%

H1 2024-H1 2025
-70%

Government

H1 2025
0.9%

H1 2024-H1 2025
+49%

Insurance

H1 2025
0.4%

H1 2024-H1 2025
-40%

Telecommunications

H1 2025
0.4%

H1 2024-H1 2025
-32%

Travel & leisure

H1 2025
0.2%

H1 2024-H1 2025
-35%

Source: TransUnion global intelligence network, 2025

Call Centre Fraud Trends

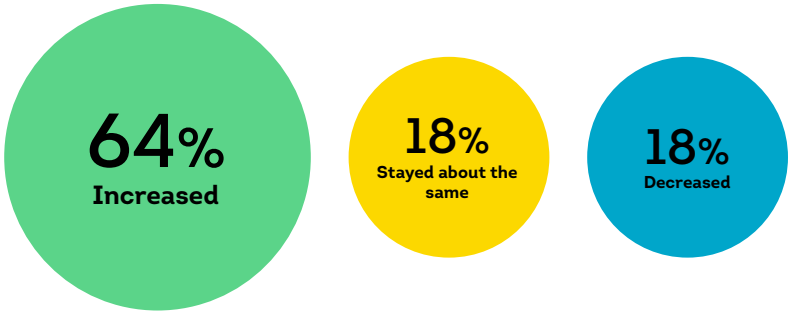
Inbound calls are risky because of the vital role call centres play in the customer experience — representing a high-trust touchpoint for consumers. Among US business leaders surveyed, 64% indicated fraudsters increased their attacks on call centres in the past year, up from 44% from 2024. More than half of business leaders surveyed reported rising levels of criminal tactics targeting call centres, including call spoofing to impersonate consumers, and use of virtual call services and stolen identity information to pass knowledge-based authentication questions.

High-risk calls into call centres rose

TransUnion documented a slight increase (to 6.1%) in the percentage of high-risk calls into US call centres from H1 2024 to H1 2025. The highest risk phone calls increased during that period across half of the channels measured.

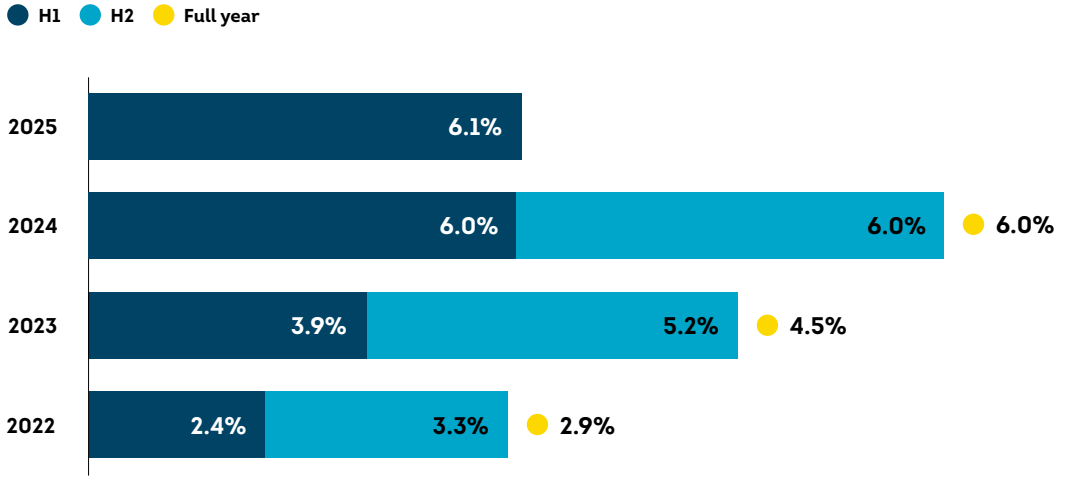
Increased Frequency of Call Centre Fraud Attacks

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, 2025

High-Risk Calls Into Call Centres

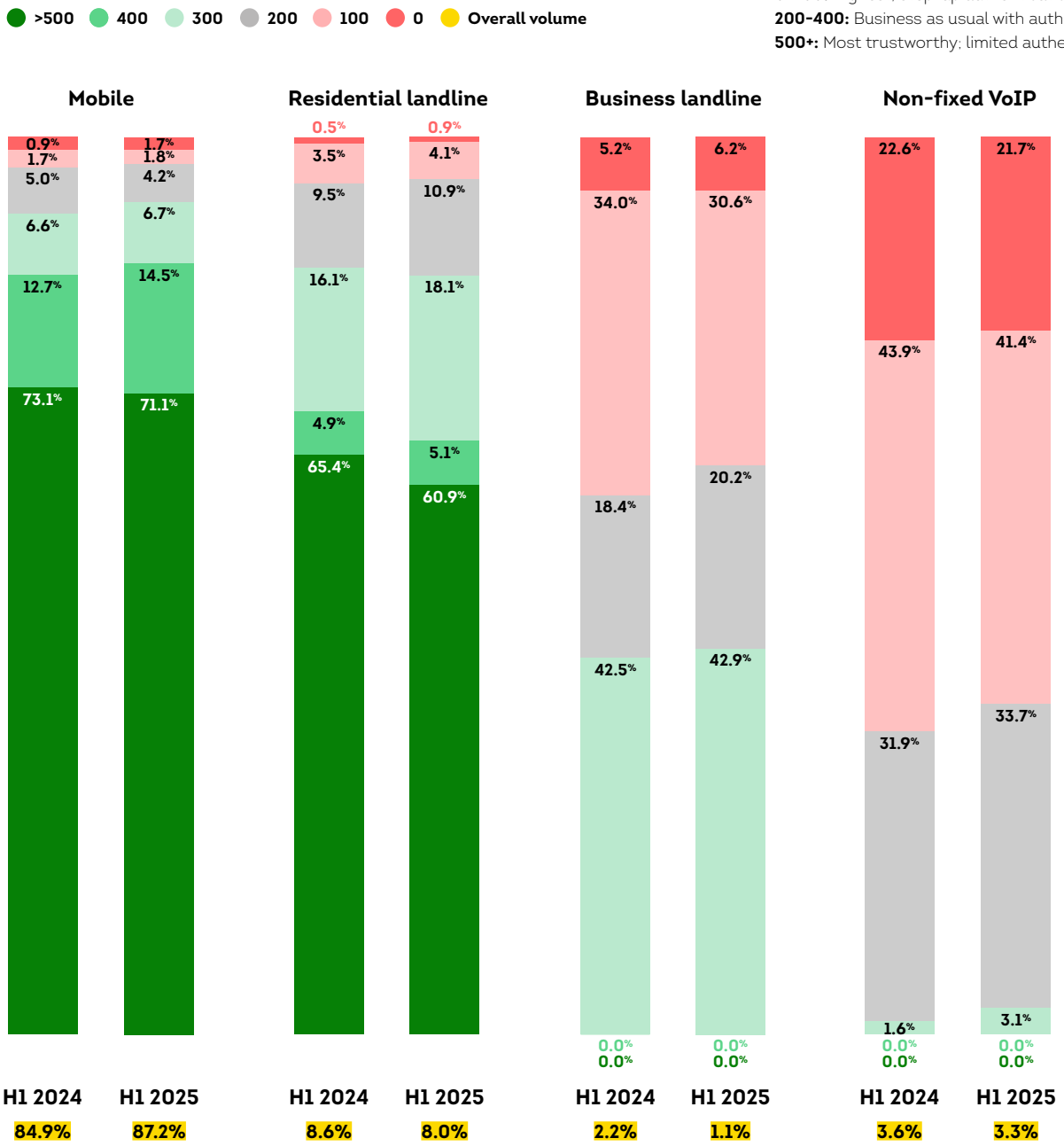


Source: TransUnion global intelligence network, 2025

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

TransUnion documented the vast majority (87.2%) of calls received by its US call centre customers in H1 2025 were from mobile phones, and these calls are getting riskier. While just 3.5% of mobile calls were identified as being the highest risk for fraud, that's a 35% increase from 2.6% in H1 2024. 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 3.3% of total call volume, 63.1% of those calls were identified as high risk for fraud in H1 2025.

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 global intelligence network, 2025

TransUnion

Risky identities impact all stages of the consumer lifecycle

Not every digital customer interaction presents the same risk to organizations. In H1 2025, account creation showed particular risk both in the US and globally. Account creation attempts had the highest rate (4.2%) of suspected digital fraud in the consumer lifecycle for transactions where the user was in the US in H1 2025 — yet substantially lower than the 8.3% globally. Account logins (a major issue for US fraud managers reporting ATO as the largest source of fraud loss) was the second riskiest in the consumer lifecycle with a suspected digital fraud rate of 3.8% for transactions where the user was in the US in H1 2025.

Account creation digital risk is being driven by specific industries in the US; 37.8% of telecommunications, 24.6% of retail and 22.9% of communities account creation transactions from the US were suspected digital fraud in H1 2025. At the same time, insurance had the highest account login risk with 29.7% of login transactions from the US suspected of digital fraud.

Consumer Lifecycle Stage Examples

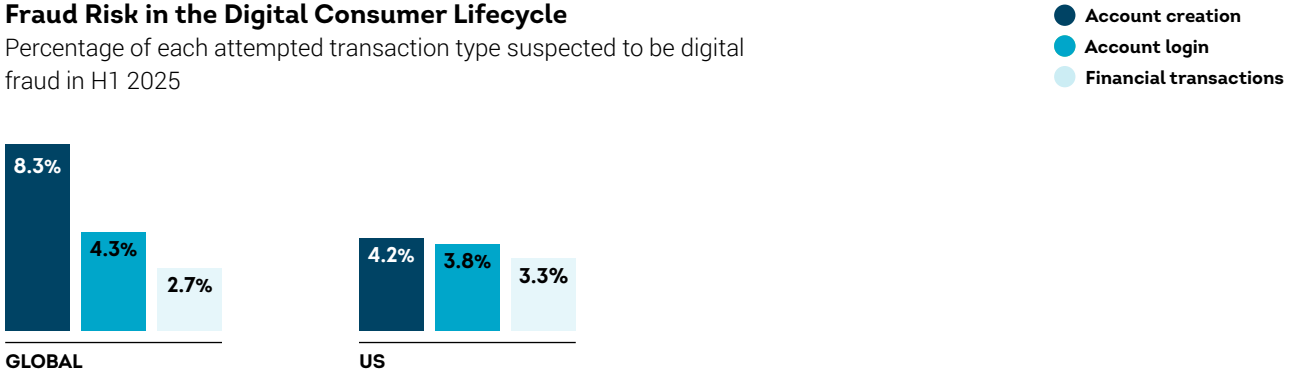
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

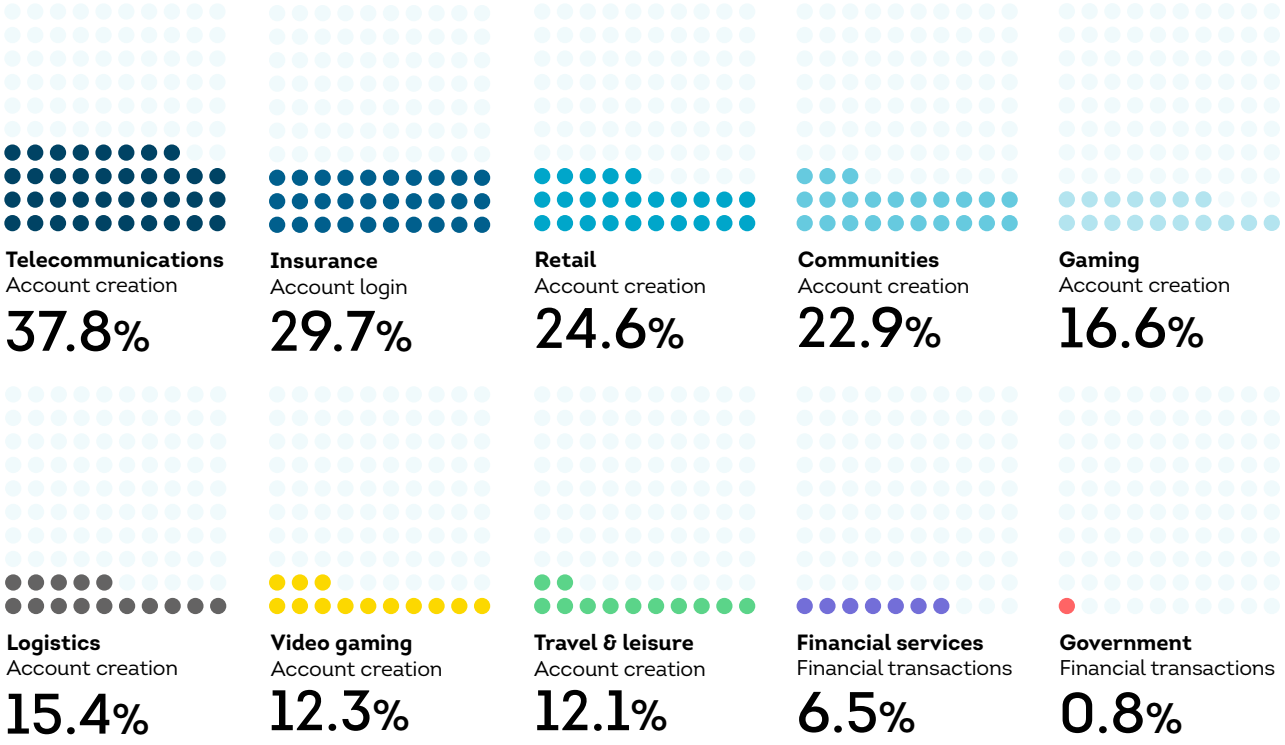
Percentage of each attempted transaction type suspected to be digital fraud in H1 2025



Source: TransUnion global intelligence network, 2025

Fraud Risk in the Digital Consumer Lifecycle by Industry

The consumer lifecycle stage with the highest rate of suspected digital fraud by industry and the corresponding percentage in that stage from the US in 2024



Source: TransUnion global intelligence network, 2025

TransUnion

Synthetic identity lending exposure illustrated new account origination risk

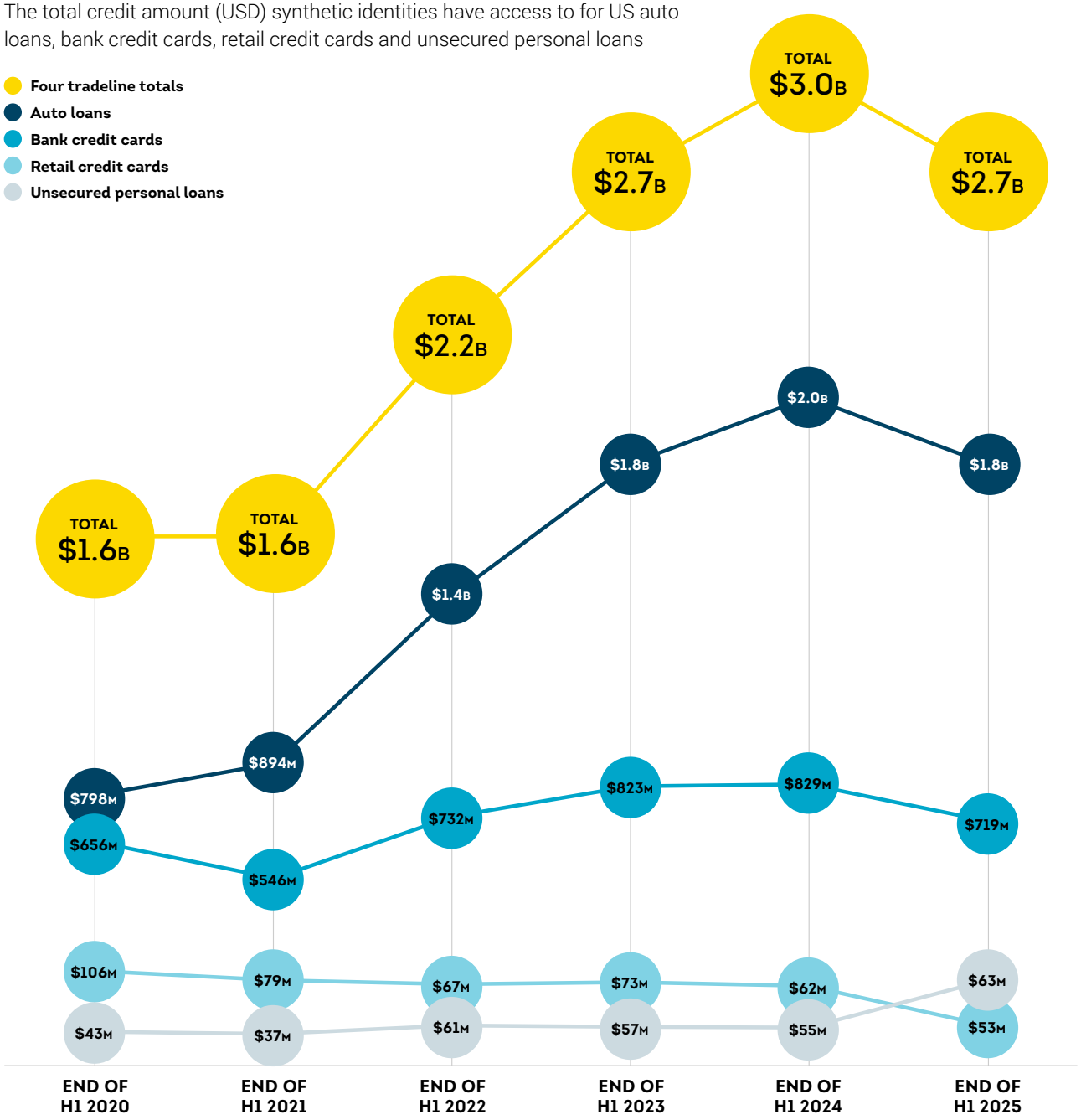
With a wealth of stolen identity credentials combined with GenAI, synthetic identity fraud is a persistent threat. Nearly a quarter (24%) of US business leaders surveyed by TransUnion stated synthetic identity fraud was the leading source of fraud losses for their organizations.

According to TransUnion's consumer credit data, total exposure to synthetic identities among accounts opened by US lenders for auto loans, bank credit cards, retail credit cards and unsecured personal loans was USD$2.7 billion in potential losses at end of H1 2025.

Using credit accounts to build credible personal history is a key tactic for synthetic identities — a highly effective identity backstopping technique — making them difficult to detect. With the growth of GenAI tools to create realistic deepfake documents and synthetic identities at scale, criminals have the means to commit synthetic fraud in other industries like retail, ecommerce, healthcare, government, telecommunications, FinTech and education.

Synthetic Identity Risk for US Lenders H1 2020–H1 2025

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 global intelligence network, 2025

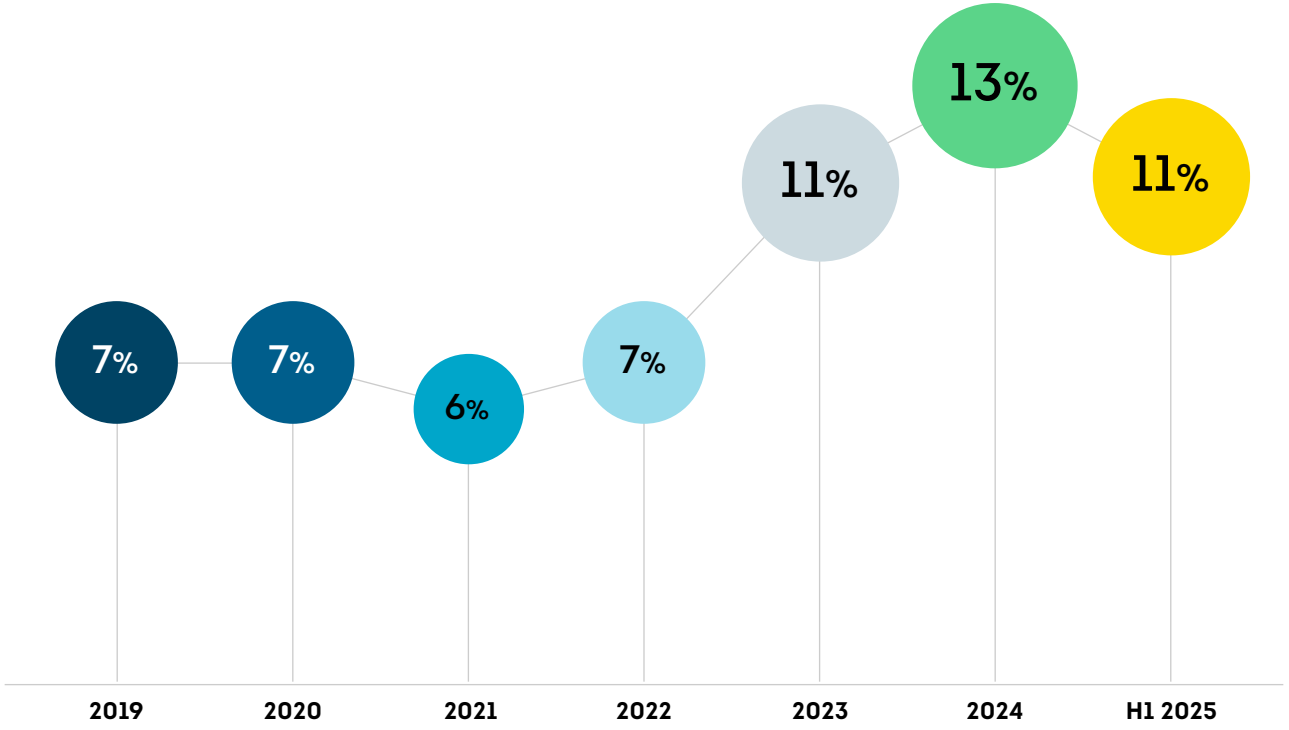
TransUnion

Credit washing extends new account fraud risk

As identity fraud evolves, criminals who commit first- or third-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 H1 2025, consumer credit report disputes in the US claiming fraud represented 11% of all disputes, remaining close to the high during the analysis period of 13% in all of 2024.

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



Source: TransUnion global intelligence network, 2025

Conclusion

No matter where you are in the world, rising fraud risk and monetary losses are growing concerns for organizations of all sizes and in all industries. For the remainder of 2025 and beyond, threats for consumers and organizations alike will continue as serious data breaches and scams lead to more compromised identities and credentials. Protecting your organization and customers is non-negotiable. You must assume a security posture that all identity data and credentials presented to your organization are compromised. As digital identity risk rises across the consumer lifecycle, investment in smarter fraud detection — resolving identity more effectively — is a must.

You should prioritize an enterprise-wide approach to fraud prevention to overcome fragmented systems that are more vulnerable to exploitation. At the same time, you should bolster each layer of your defences, especially due to the AI threat vector. Each existing layer — identity verification, document verification, authentication, session monitoring, etc. — needs increased risk signals, applying better risk scoring and revising your fraud strategies to be adaptive to evolving threats. Employ strategies aimed at reducing consumer identity fragmentation through better data and risk signals, advanced analytics and integrated technology. Reducing inconsistent and siloed identity data will enable you to detect possible fraud more effectively, minimize unnecessary customer friction and avoid additional expenses 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), Hong Kong (200) India (200), and the Philippines (200), UK (200) and US (200) from May 29–June 6, 2025 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 with a minimum annual revenue of CAD$300M in Canada, HK$200M in Hong Kong, ₹1B in India, ₱1B in the Philippines, £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 May 5–25 2025 in Botswana (251 respondents), Brazil (949), Canada (982), Chile (888), Colombia (933), the Dominican Republic (601), Guatemala (478), Hong Kong (968), India (999), Kenya (433), Namibia (291), the Philippines (943), Rwanda (345), South Africa (922), Spain (957), the UK (1,000), the US (2,998) and Zambia (325) 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, Guatemala and Spain). To ensure data sourcing methodology 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 TransUnion's 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 represent 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 June 30, 2025. The lender exposure measures were based upon TransUnion's proprietary formula to capture potential total loss at risk for lenders.

ABOUT TRANSUNION (NYSE: TRU)

TransUnion is a global information and insights company with over 13,000 associates operating in more than 30 countries. We make trust possible by ensuring each person is reliably represented in the marketplace. We do this with a Tru™ picture of each person: an actionable view of consumers, stewarded with care. Through our acquisitions and technology investments we have developed innovative solutions that extend beyond our strong foundation in core credit into areas such as marketing, fraud, risk and advanced analytics. As a result, consumers and businesses can transact with confidence and achieve great things. We call this Information for Good® – and it leads to economic opportunity, great experiences and personal empowerment for millions of people around the world.

Combine powerful fraud detection with advanced insights to protect your business and your customers. Learn more about **TransUnion Fraud prevention solution** today.

TransUnion