

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 organisation to fraud. Consumer scams targeting authorised 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 organisation 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 69 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/ authorised 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

- Anatomy of Digital Identity Risk** **4**

- Global Fraud Trends** **5**
 - Business and Consumer Fraud Experiences 6
 - Digital Fraud Trends 10
 - Digital Fraud Across the Consumer Lifecycle 13

- Regional Fraud Trends** **14**
 - Africa: Botswana, Kenya, Namibia, Rwanda, South Africa and Zambia 14
 - Asia: Hong Kong, India and the Philippines 20
 - Europe: Spain and the UK** **29**
 - Latin America: Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, Mexico, Nicaragua and Puerto Rico 38
 - North America: Canada 44
 - North America: US 53

- Conclusion** **68**

- Data Sourcing Methodology** **69**

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 specialised. 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 organisation 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

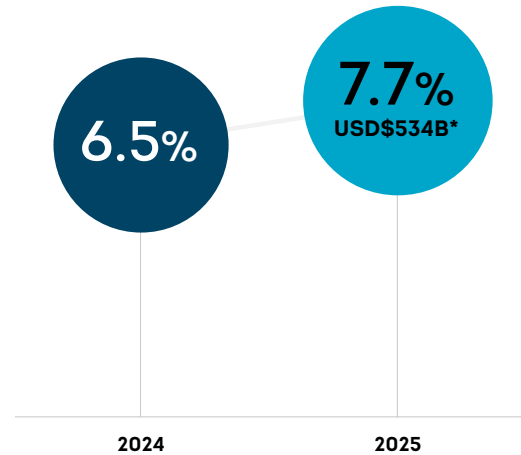
The cost of fraud rose globally

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/authorised 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

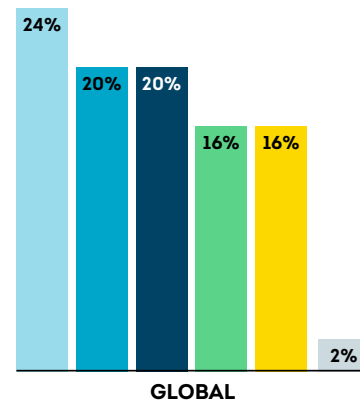


*USD conversion based on currency exchange value on July 16, 2025

^Not showing 2024 total due to the difference in the number of companies surveyed globally

Source: TransUnion business survey

Most Prominent Cause of Fraud Losses



Source: TransUnion business survey

Scam/Authorised fraud

Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)

Account takeover

Unauthorised individuals taking over someone's online account (e.g., bank, social media, email) without their permission

Synthetic identity fraud

Use of a combination of personally identifiable information to fabricate a person or entity to commit a dishonest act for financial or personal gain

First-party fraud

Identity misrepresentation or falsifying information for the purpose of financial gain

Third-party fraud

The use of stolen identity to open an account

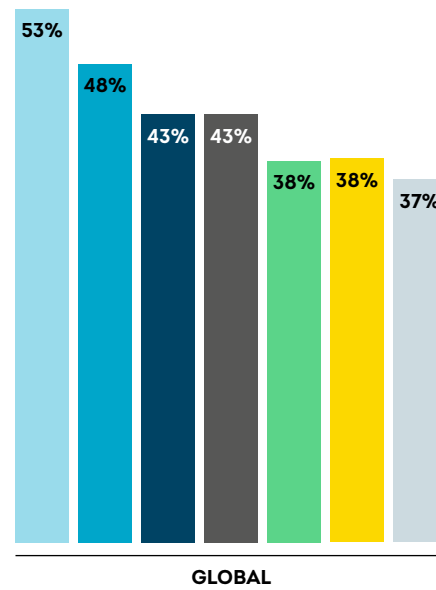
Other

Fraud prevention techniques rely on identity and device signals

As the risk from consumer scams threatens identity integrity, organisations rely on a mixture of data, risk signals, technology and tools to 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.



- Identity verification
- Device reputation
- Behavioural biometrics
- IP intelligence
- Email reputation
- Synthetic identity detection
- Phone number reputation

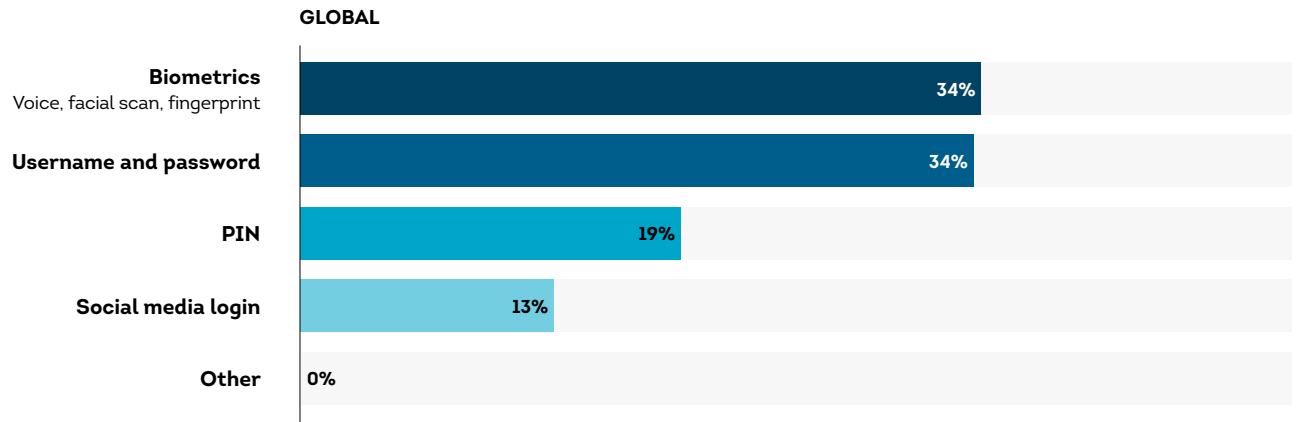
Source: TransUnion business survey

Dependence on passwords for customer authentication fading

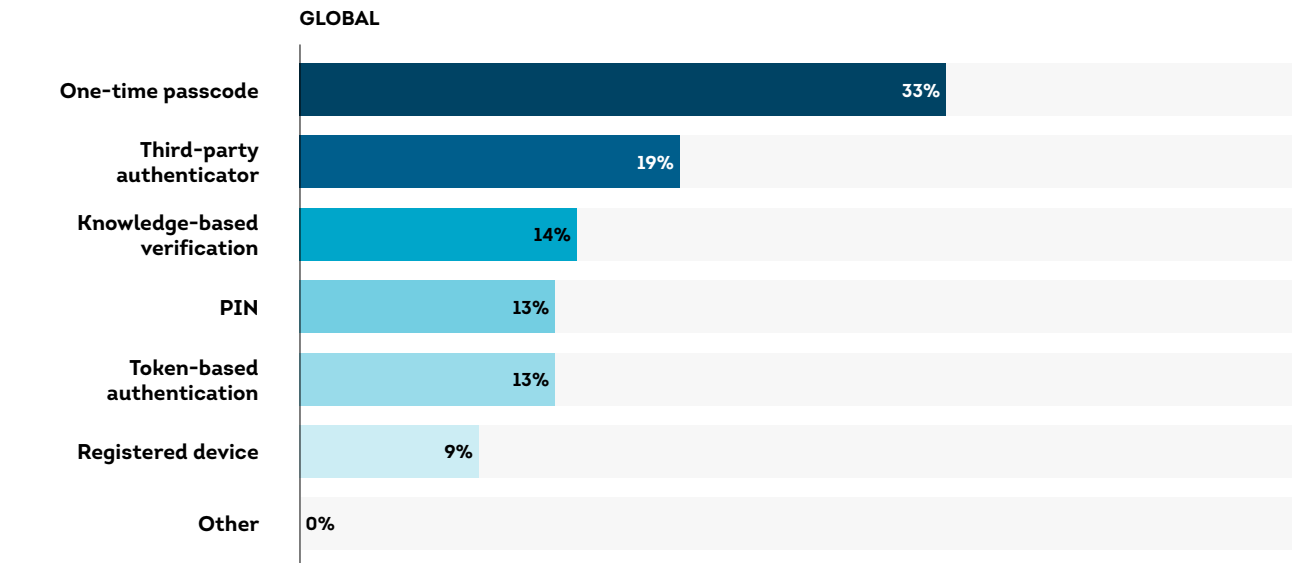
User accounts remain under threat from consumer scams and brand spoofing. Organisations appear to be shifting their approaches to embed a second factor into their authentication programs as standard practice. While more than a third (34%) of business leaders indicated they utilise usernames and passwords 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 utilise 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



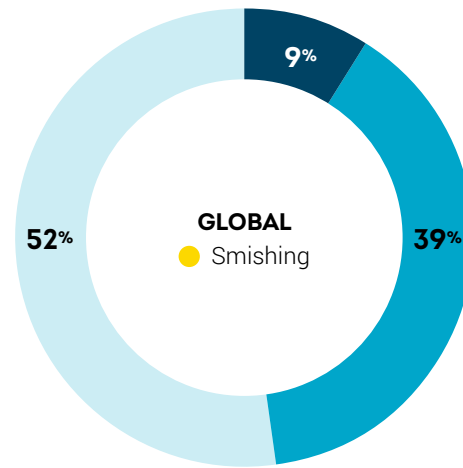
Source: TransUnion business survey

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

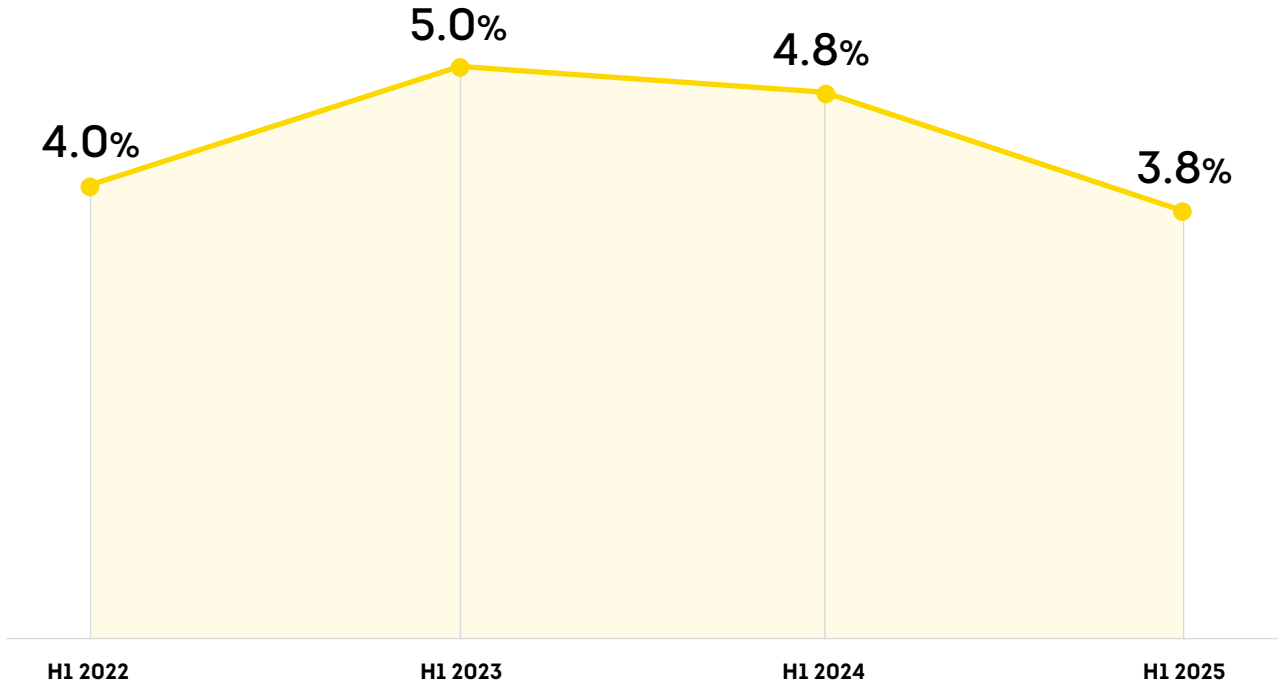
- Targeted and fell victim
- Targeted but didn't fall victim
- Not targeted
- Most reported fraud scheme

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

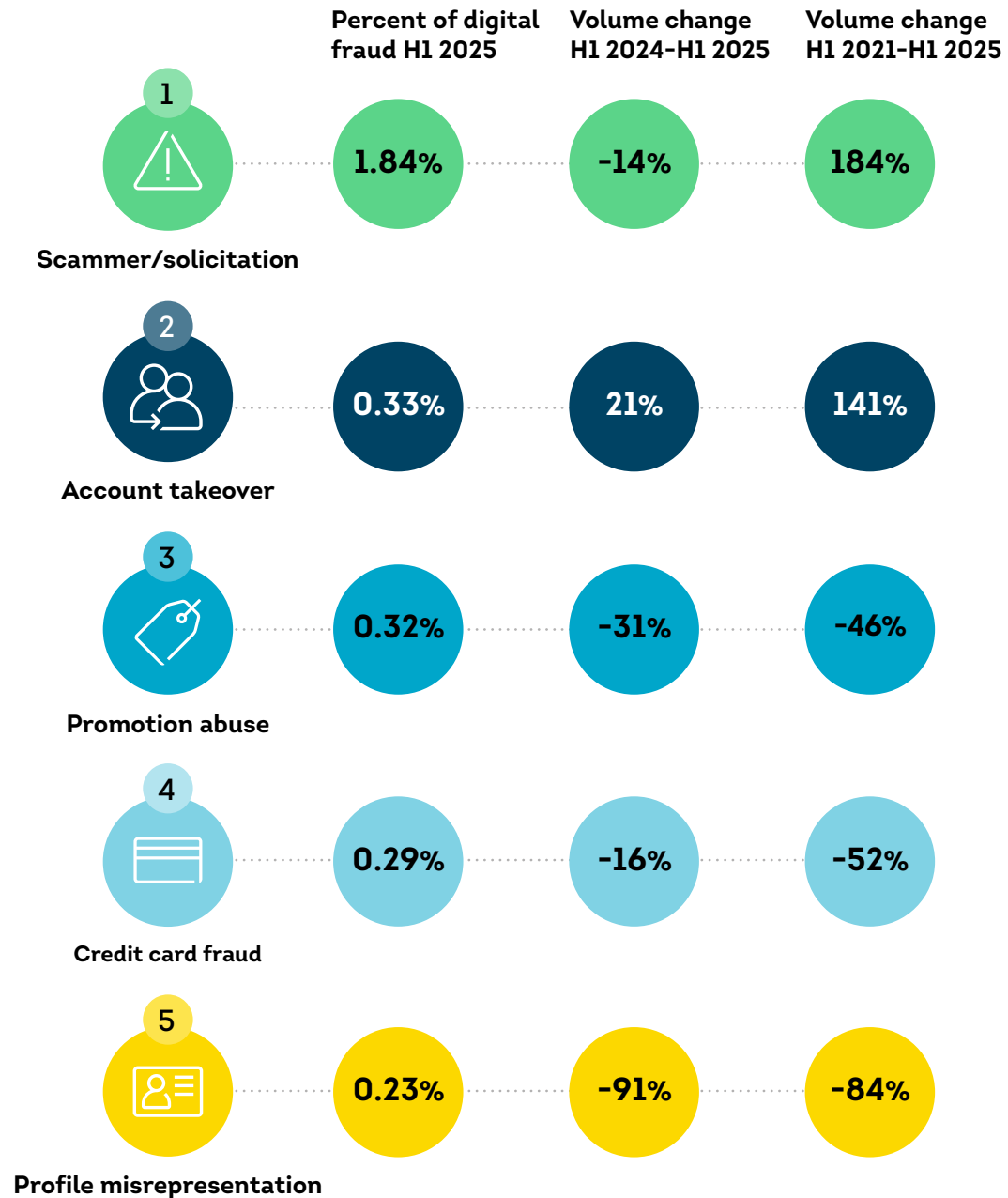


Source: TransUnion global intelligence network

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

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 analysed 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

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%

Video gaming

H1 2025

13.5%

Scammer/solicitation

H1 2024-H1 2025

+3%

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

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 analysed at 21.6% and 20.0%, respectively.

Consumer Lifecycle Stage Examples

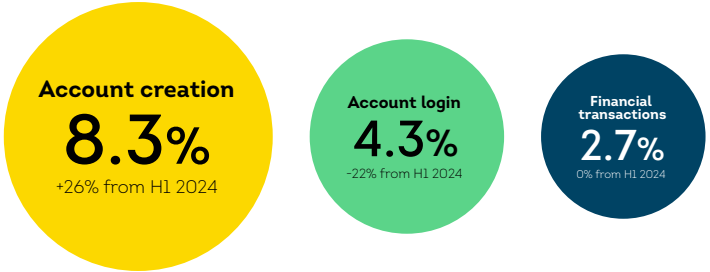
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

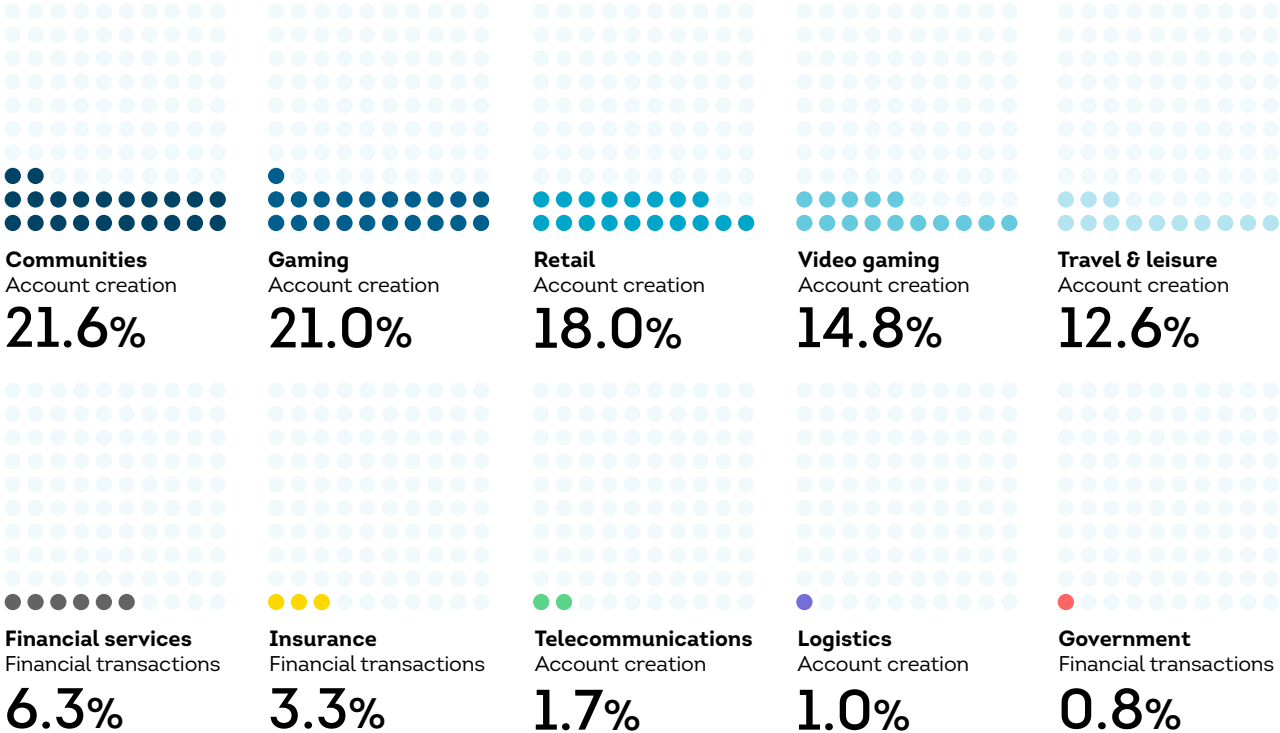
Percentage of each attempted transaction type suspected to be digital fraud globally in H1 2025



Source: TransUnion global intelligence network

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



AFRICA

Africa Overview

Africa is rapidly building a digital economy and must continue doing so securely. With stronger consumer fraud awareness, improved fraud controls and tailored fraud responses, the region is showing it can increase digital participation while effectively managing fraud risk. However, consumer expectations around security, trust and seamless user experiences place increased pressure on organisations, financial institutions and regulators to act decisively.

There's no one-size-fits-all approach to fraud in Africa. Each market faces unique industry threats, requiring tailored fraud prevention strategies. Insights from TransUnion show Kenya and South Africa demonstrate strong digital adoption – yet also experience elevated suspected digital fraud rates compared to other African countries. Zambia and Rwanda are seeing growing digital maturity but remain highly exposed to manipulation-based fraud, such as money mule schemes and social engineering. Namibia stands out for card-related fraud risk despite relatively low suspected digital fraud volumes.

African data in this section blends proprietary insights for digital fraud from TransUnion's global intelligence network in Botswana, Kenya, Namibia, Rwanda, South Africa and Zambia, as well as a consumer survey in those same countries.

KEY TAKEAWAYS

Fraudsters focus on immediate payoff

83%

of African countries reported money/gift card scams as the most reported fraud type experienced by surveyed consumers who said they were targeted by fraud in the last three months

Suspected digital fraud lower in Africa than globally

2.6%

of transactions where the consumer was in Kenya in H1 2025, were suspected of digital fraud, the highest rate for all African countries analysed but lower than 3.8% globally for the period

Account creation highest risk in consumer lifecycle for most of Africa

5 out of 6

African countries analysed had account creation as the stage in the consumer lifecycle with the highest rate of suspected digital fraud in H1 2025 with Zambia having the highest rate at 11.5%

Consumer Fraud Experiences

Consumer-reported email, online, phone call and text messaging fraud is widespread across nearly every African country TransUnion recently surveyed. Despite high targeting rates, only between 6% to 13% reported actually falling victim. This suggests education and defences are gaining traction.

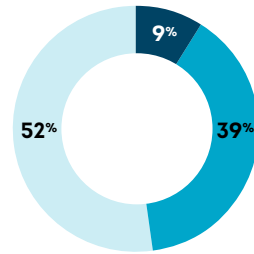
Trends over time show encouraging signs. Kenya's consumer reported fraud victimisation rate dropped from 11% in late last year to 10% in Q2 2025. Namibia also declined during this period. This pattern suggests fraud attempts are common – but more consumers are spotting and stopping them. It's a sign awareness efforts and security habits may be working, even as the threat environment remains intense.

What's also apparent in the TransUnion survey is different fraud types are reported by consumers in different African markets. However, money/ gift card scams were overwhelmingly the most reported fraud types across Africa.

Consumers Targeted With Fraud

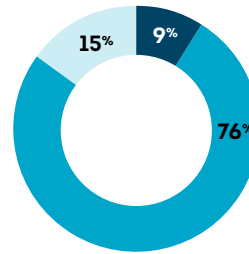
Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from February to May 2025, and the most frequent scheme by which they reported being attacked.

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



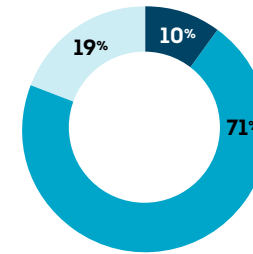
GLOBAL

- Smishing



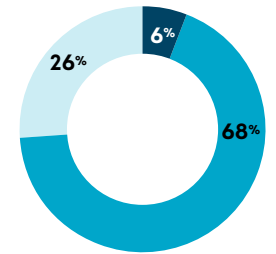
ZAMBIA

- Money/gift card



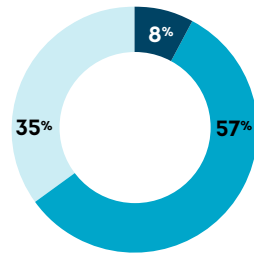
KENYA

- Vishing



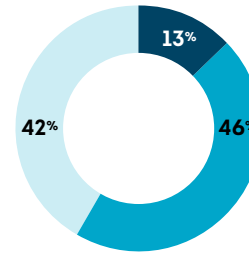
BOTSWANA

- Money/gift card



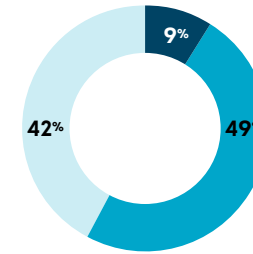
NAMIBIA

- Money/gift card



SOUTH AFRICA

- Money/gift card



RWANDA

- Money/gift card

Source: TransUnion consumer survey

Digital Fraud Trends

Declining suspected digital fraud in African markets

The share of digital transactions flagged as potentially fraudulent has declined across all African markets since 2022, outpacing progress in many global and emerging economies.

Botswana and Zambia showed some of the steepest declines in suspected digital fraud rates, both reaching 1.0% in H1 2025, indicating strong progress in fraud mitigation.

The rate of suspected digital fraud for transactions where the consumer was in South Africa was down from 4.3% in H1 2022 to 2.1% for H1 2025, indicating improved fraud prevention and maturing digital controls.

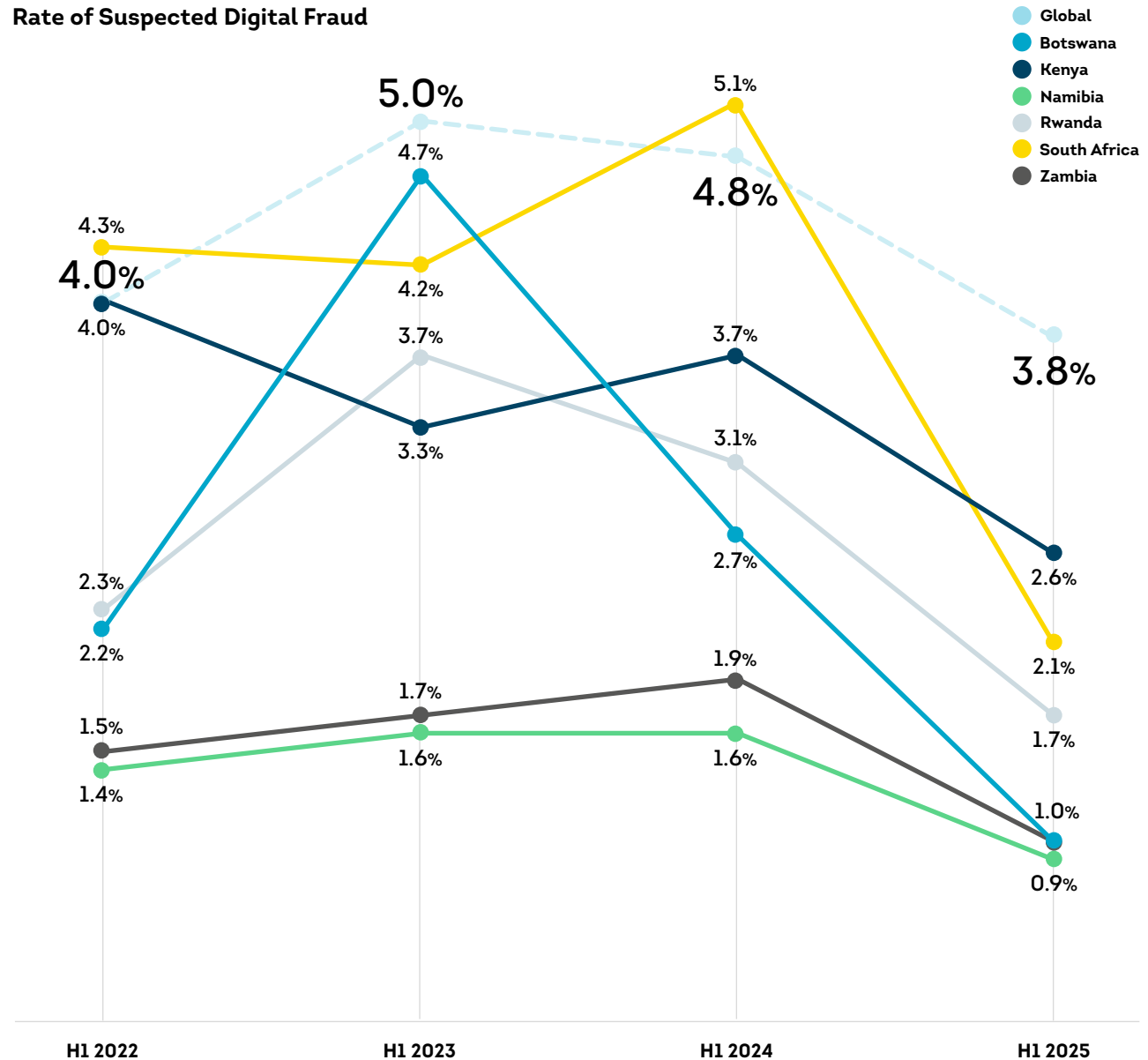
Kenya fell from 4.0% to 2.6% in the same period. This decline reflects the country's leadership in mobile finance and tightening fraud measures.

Rwanda dropped from 2.3% to 1.7% since H1 2022, showing a steady downward trend.

Namibia maintained the lowest and most stable fraud rates from 2022 to 2025, consistently under 2%.

Global fraud rates remained consistently higher than most African markets, though they also showed a downward trend in H1 2025.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

Industry-specific digital fraud hotspots in Africa

Fraudsters are targeting industries differently across African markets, revealing localised vulnerabilities shaped by digital maturity, consumer behaviour and fraudster tactics.

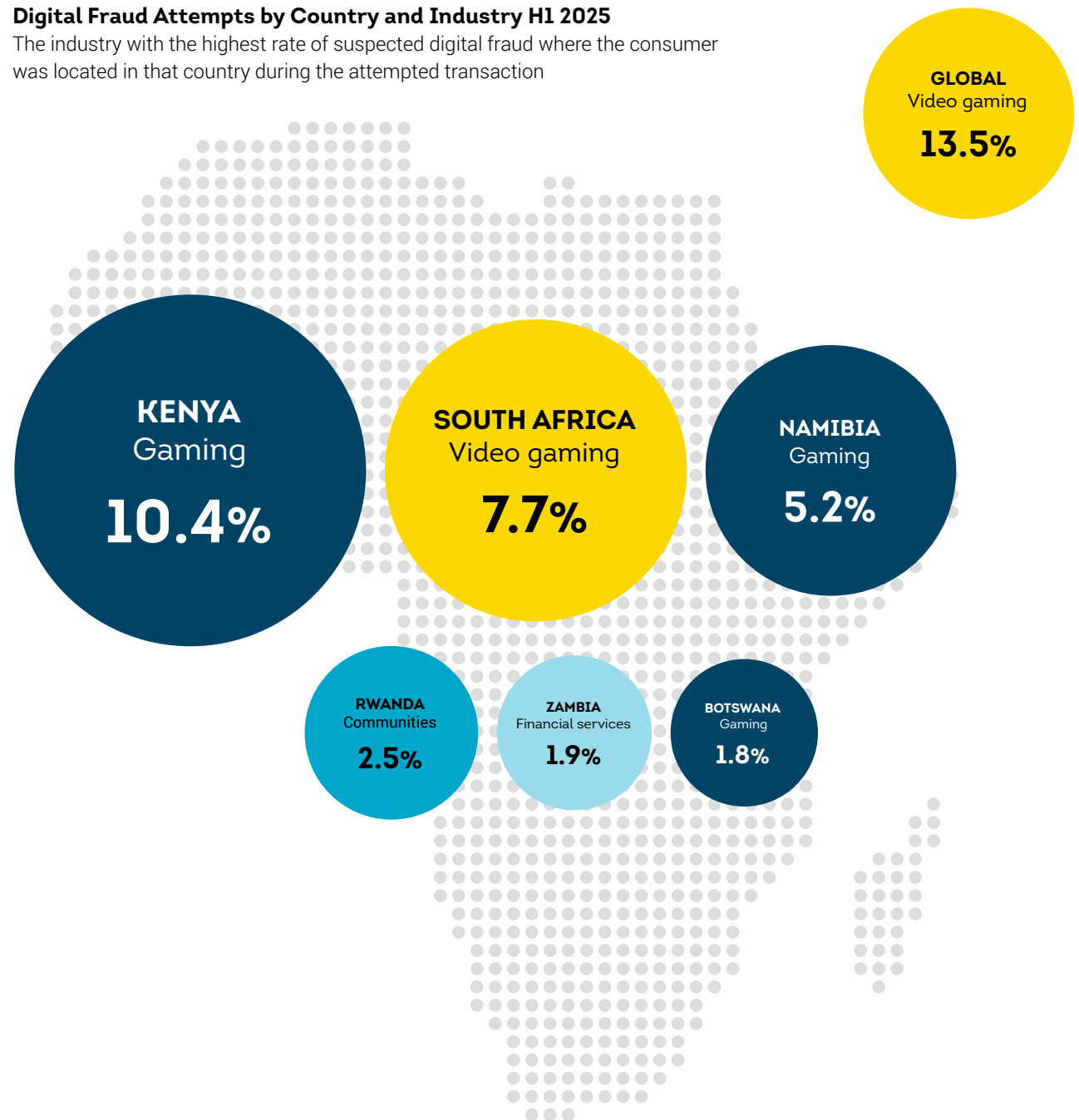
In H1 2025, there was a tendency for both gaming (online sports betting, poker, etc.) and video gaming to attract suspected fraudsters in Africa. Of transactions where the consumer was in Kenya, Namibia and Botswana, the rate of suspected digital fraud in gaming was the highest among those industries analysed during that period at 10.4%, 5.2% and 1.8%, respectively. In South Africa, the rate of suspected digital fraud in video gaming was the highest at 7.7%. Higher fraud in gaming and video gaming reflects their rapid growth and appeal to younger, digitally active consumers — often with weaker security habits. Globally, video gaming (13.5%) was the most fraud-prone industry.

Of transactions from Rwanda in H1 2025, communities (2.5%) stood out as the industry with the highest rate of suspected digital fraud. Financial services was the industry with the highest suspected digital fraud rate coming from Zambia at 1.9%.

African markets reveal industry-specific vulnerabilities — from gaming and video gaming to retail to financial services — demanding tailored fraud prevention strategies across countries, industries and consumer interaction points.

Digital Fraud Attempts by Country and Industry H1 2025

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



Digital fraud in the consumer lifecycle

Africa's digital fraud landscape is front loaded. It appears fraudsters are aggressively probing weak points at the onboarding and login stages, especially in markets with rapid digital adoption but uneven fraud defences.

Zambia (11.5%) and Rwanda (8.6%) reported the highest rate of suspected digital fraud during account creation attempts, both exceeding the global average (8.3%) and signalling heightened vulnerability during onboarding.

Kenya (4.4%) and Namibia (2.8%) showed moderate suspected digital fraud rates during account creation, while South Africa (2.2%) and Botswana (2.6%) remained well below global levels, suggesting relatively stronger controls or lower attack volumes.

The rate of suspected digital fraud was the highest in the consumer lifecycle at account login for South Africa (2.6%), aligning with the global trend of fraud shifting to account takeover attempts.

Financial transaction fraud remained low across all African markets (0.2%–0.9%), significantly below the global average of 2.7%, indicating fraudsters may be focusing more on identity compromise than direct monetary theft in the region.

Consumer Lifecycle Stage Examples

Account creation: Account signup, registration and loan origination

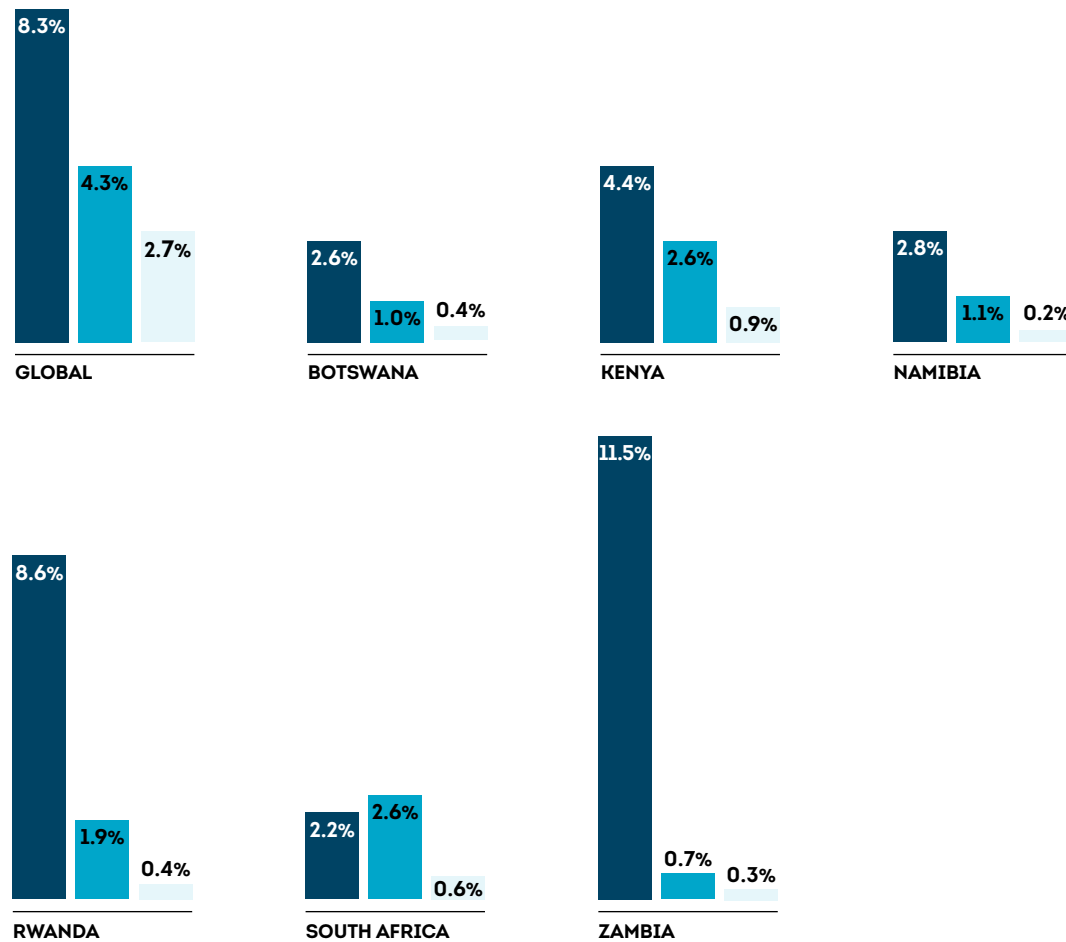
Account login: Login and failed login events

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

- Account creation
- Account login
- Financial transactions



Source: TransUnion global intelligence network



INDIA

HONG KONG

PHILIPPINES

ASIA

Asia Overview

Fraud threats are evolving differently across Asian markets. In Hong Kong, organisations appear less alarmed by fraud risks compared to other regions, yet they continue to report facing significant exposure to sophisticated attacks like account takeover and identity-based fraud. This disconnect suggests a need for better awareness and proactive fraud strategies.

The Philippines is grappling with a broader spectrum of fraud, particularly first-party fraud, which is more prevalent there than in any other market according to business leaders surveyed. Filipino organisations appear to be adapting quickly to these threats. India faces significant fraud threats from scams, identity theft and synthetic identities. While digital growth accelerates, fraud controls lag. Weak onboarding and limited analytics leave gaps in prevention.

All markets recognise the value of technologies like identity verification and device intelligence, but their approaches to implementation and readiness vary. These findings underscore the importance of tailoring fraud strategies to local realities — balancing technology, process and awareness to stay ahead of increasingly complex threats.

Asian data in this section blends proprietary insights for digital fraud from TransUnion's global intelligence network, a business survey and a consumer survey in Hong Kong, India and the Philippines.

KEY TAKEAWAYS

Fraud concerns are high and types differ by market

28%

of business leaders surveyed in India cited scams/authorised fraud as the most prominent cause of fraud losses

70% and 51%

of Filipino and Hong Kong business leaders surveyed, respectively, reported being extremely or very concerned about the impact of fraud on their businesses

Consumers are impacted as synthetic fraud emerges

19%, 17% and 16%

of Filipino, Indian and Hong Kong business leaders, respectively, said the most prominent cause of fraud loss is synthetic identity fraud

65%, 43% and 37%

of Filipino, Indian and Hong Kong consumers, respectively, reported being targeted with email, online, phone call or text messaging fraud from February to May 2025

Technologies to prevent fraud consistent across markets

56%, 53% and 51%

of Filipino, Hong Kong and Indian business leaders, respectively, ranked identity verification as most effective for preventing fraud

49%, 49% and 48%

of Hong Kong, Indian and Filipino business leaders, respectively, ranked device reputation as second most effective for preventing fraud

Business and Consumer Fraud Experiences

The cost of fraud

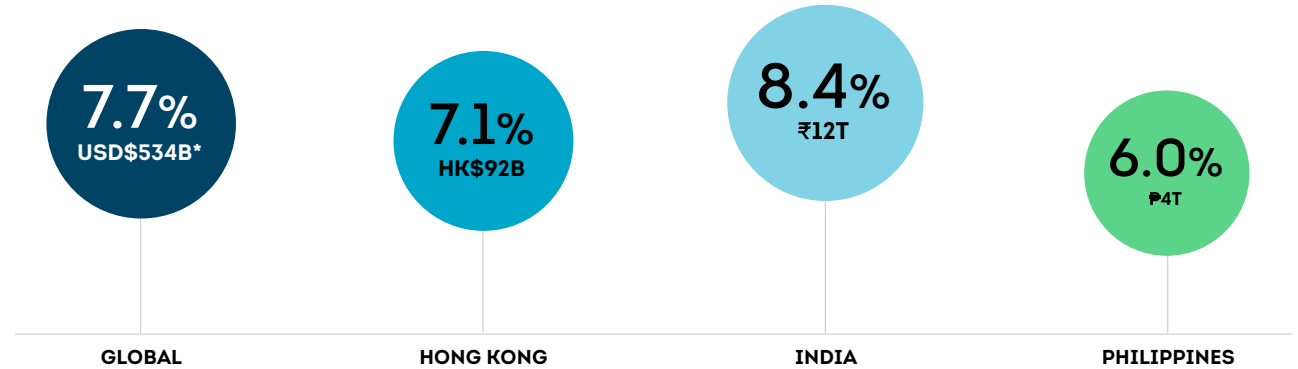
Hong Kong business leaders claim their companies lost the equivalent of 7.1% of their revenues in the past year due to fraud, representing HK\$92B among the 200 business leaders surveyed. According to them, the most prominent cause of fraud losses this year was third-party fraud – followed by account takeover, indicating a strong presence of identity theft and unauthorised access.

Indian business leaders claimed their companies lost the equivalent of 8.4% of their revenues in the past year due to fraud, representing ₹12T of fraud losses among the 200 business leaders surveyed. That’s higher than 7.4% last year in India and the global average of 7.7% this year. According to them, the most prominent cause of fraud losses this year was scams/authorised fraud followed by third-party fraud.

Philippine business leaders reported their companies lost the equivalent of 6% of their revenues in the last year due to fraud, representing ₱4T among the 200 business leaders surveyed. According to them, the most prominent cause of fraud loss was scam/authorised fraud and first-party fraud (which tied), reflecting a dual threat from deception and internal misrepresentation.

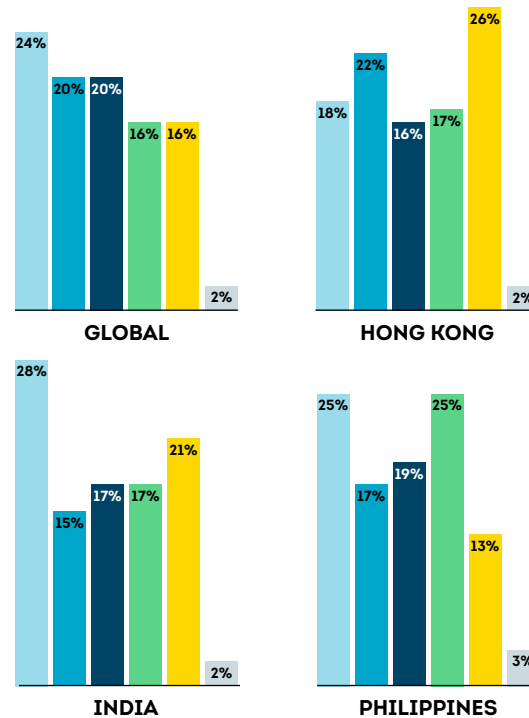
Total Cost of Fraud

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

Most Prominent Cause of Fraud Losses



● Scam/Authorised fraud

Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)

● Account takeover

Unauthorised individuals taking over someone’s online account (e.g., bank, social media, email) without their permission

● Synthetic identity fraud

Use of a combination of personally identifiable information to fabricate a person or entity to commit a dishonest act for financial or personal gain

● First-party fraud

Identity misrepresentation or falsifying information for the purpose of financial gain

● Third-party fraud

The use of stolen identity to open an account

● Other

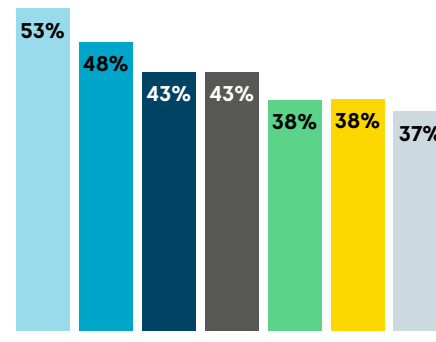
Identity verification seen as most effective across all markets

Surveyed business leaders ranked identity verification as the most effective technology for preventing fraud globally and regionally: 56% in the Philippines, 53% in Hong Kong and 51% in India. Device reputation and behavioural biometrics are gaining traction, especially in Hong Kong (49% and 44%, respectively) and the Philippines (48% and 41%, respectively), while India had device reputation (49%) and IP Intelligence (48%) as the second and third most effective technology, reflecting a shift toward multilayered identity intelligence.

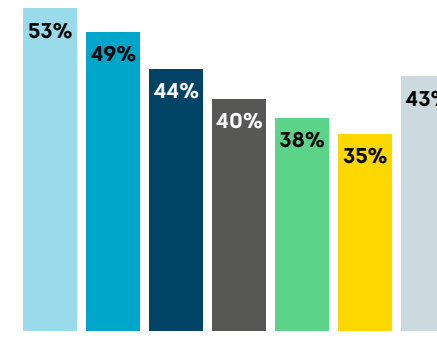
The Philippines showed stronger adoption of email reputation (44%), aligning with phishing being the most reported fraud scheme by Filipinos in TransUnion's recent consumer survey. Phone number reputation was more emphasised in Hong Kong (43%) than globally, likely due to vishing being the top reported fraud type by consumers in our recent TransUnion survey.

In Hong Kong where retail saw the highest rate of suspected digital fraud in H1 2025, technologies like device reputation and IP intelligence help detect anomalies in ecommerce transactions. In the Philippines where community platforms had the highest rate of suspected digital fraud in H1 2025, behavioural biometrics and synthetic identity detection are critical to identifying scammer/solicitation patterns.

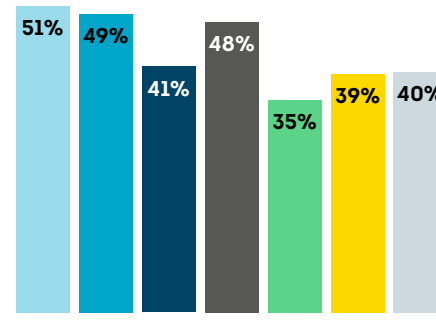
Technology Ranked as Most Effective for Preventing Fraud



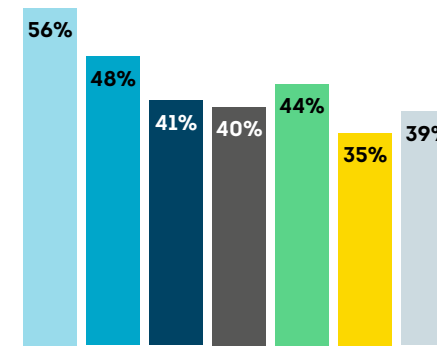
GLOBAL



HONG KONG



INDIA



PHILIPPINES

- Identity verification
- Device reputation
- Behavioural biometrics
- IP intelligence
- Email reputation
- Synthetic identity detection
- Phone number reputation

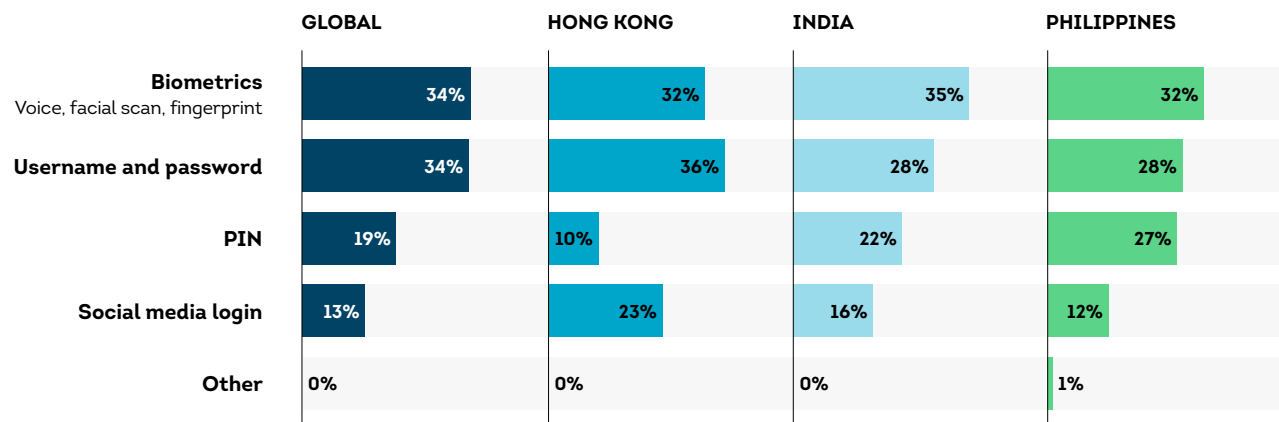
Source: TransUnion business survey

Authentication practices dominated by biometrics

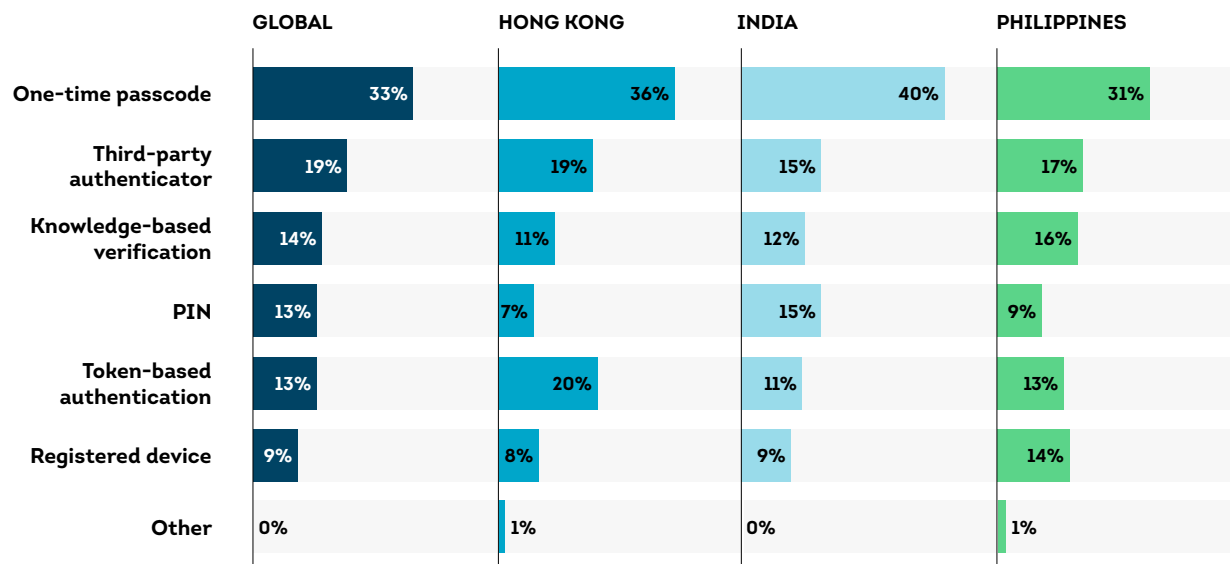
According to business leaders surveyed in Hong Kong, in order to authenticate consumers, they rely most on username/password (36%) – followed by biometrics (32%) and social media login (23%). PIN usage was relatively low (10%). India business leaders reported relying most on biometrics (35%) – followed by username/password (28%) and PIN (22%). Social media login was a distant last at 16%. The Philippines showed a more balanced approach with biometrics (32%), PIN (27%) and username/password (28%) all commonly used.

When business leaders were asked what their secondary method of customer authentication was, the number one answer for Hong Kong was one-time passcodes (36%) followed by token-based authentication (20%). India also led with one-time passcodes (40%) followed by PIN (15%), both higher than the global averages. Philippines had one-time passcodes (31%) followed by third-party authenticator (17%) and knowledge-based verification (16%).

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey

Consumer-reported fraud highest in the Philippines but widespread

Consumers in Hong Kong, India and the Philippines reported whether or not they were targeted with online, email, phone call or text messaging fraud from February to May 2025.

Hong Kong

More than a third (37%) of consumers said they were targeted by fraud schemes, with only 4% reporting falling victim. The most reported fraud scheme was vishing, reflecting the region's vulnerability to deceptive digital communications. These figures suggest while awareness is growing, fraud resilience remains a challenge, especially in digital.

India

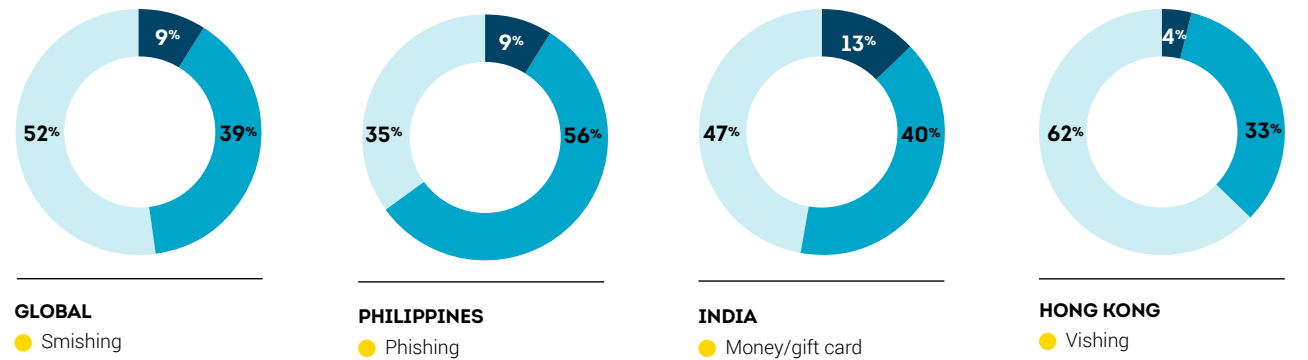
More than half (53%) of consumers reported being targeted by fraud schemes and of those, 13% said they had fallen victim, indicating a high conversion rate from targeting to actual loss. Both numbers are higher than the global average of 48% targeted and 9% fallen victim. The most reported fraud scheme was money/gift card scam, potentially reflecting the region's vulnerability to underpenetrated financial knowledge.

Philippines

Nearly two-thirds (65%) of consumers reported being targeted – one of the highest rates globally. Of these, 9% said they fell victim, in line with the global average. Phishing led as the top fraud scheme. The high targeting rate underscores the need for consumer education, multi-factor authentication and real-time fraud detection tools.

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

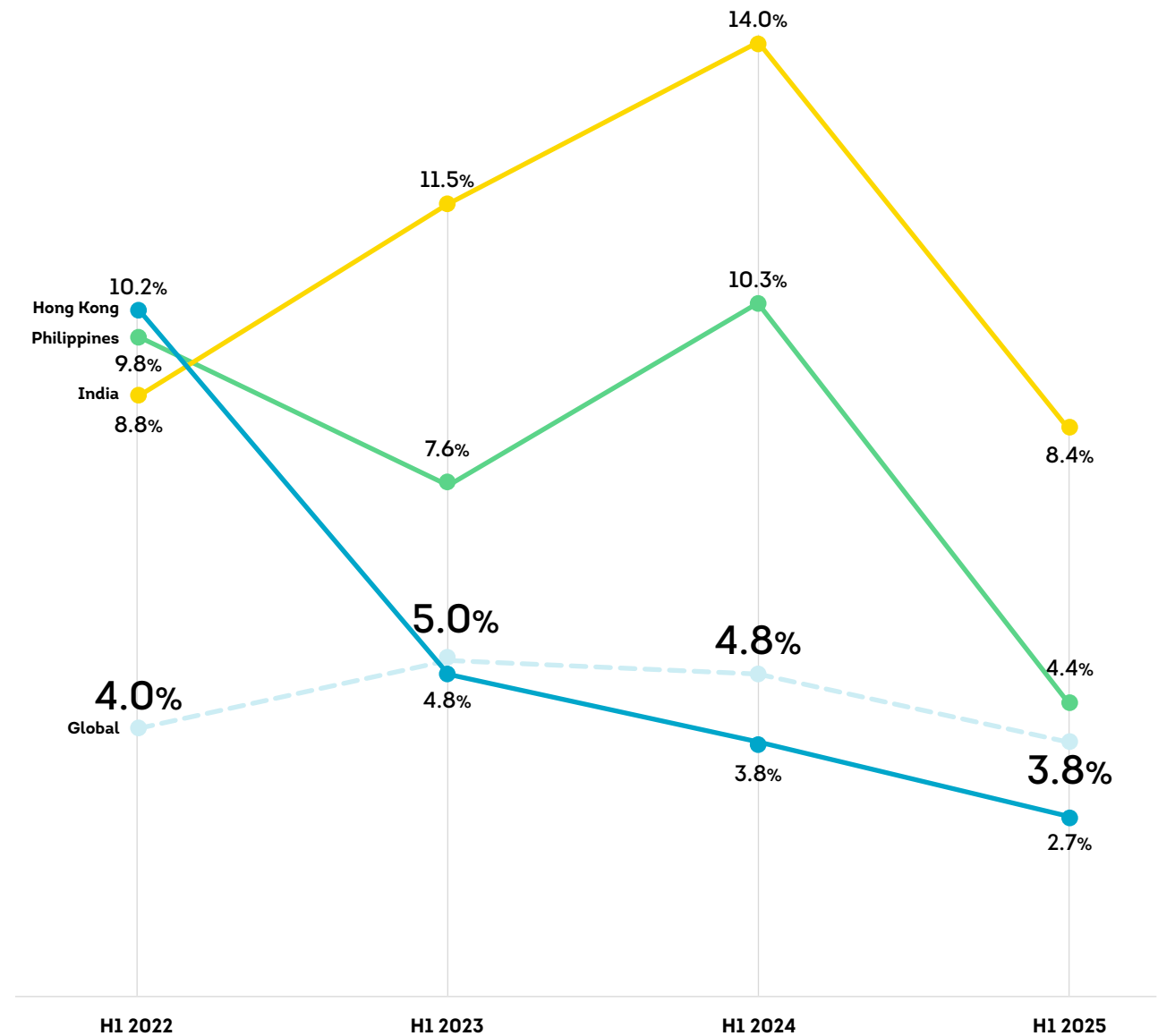
Digital Fraud Trends

Hong Kong's suspected digital fraud rate fell from 10.2% in H1 2022 to 2.7% in H1 2025 – a 73% drop. This decline could reflect strong adoption of fraud tools like identity verification and device reputation, as well as rising consumer awareness.

India represents a more volatile fraud landscape – with fluctuating rates over the past four years. After peaking in H1 2023 and H1 2024, the fraud rate dropped by around half in 2025, signalling significant progress. This volatility may be attributed to high consumer targeting. India had a high percentage of consumers who said they were targeted with email, online, phone call and text messaging fraud. While Indian business leaders reported significant adoption of technologies like identity verification, device reputation and IP Intelligence.

The Philippines saw the suspected digital fraud rate peak over the last few years (10.3% in H1 2024) before dropping to 4.4% in H1 2025. The recent decrease may stem from more business fraud prevention tech adoption and consumer education.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

Regional fraud trends vary by industry

Hong Kong: Retail sector under pressure

The retail sector experienced the highest rate (19.4%) of suspected digital fraud in H1 2025 for transactions where the consumer was in Hong Kong among industries analysed in the region. This elevated risk suggests fraudsters are targeting ecommerce and consumer-facing platforms, likely exploiting payment flows, checkout processes and account creation vulnerabilities. Despite Hong Kong's overall decline in fraud rates, the retail sector remains a critical area for continued investment in fraud detection, device intelligence and secure authentication.

Philippines: Community platforms had highest fraud risk

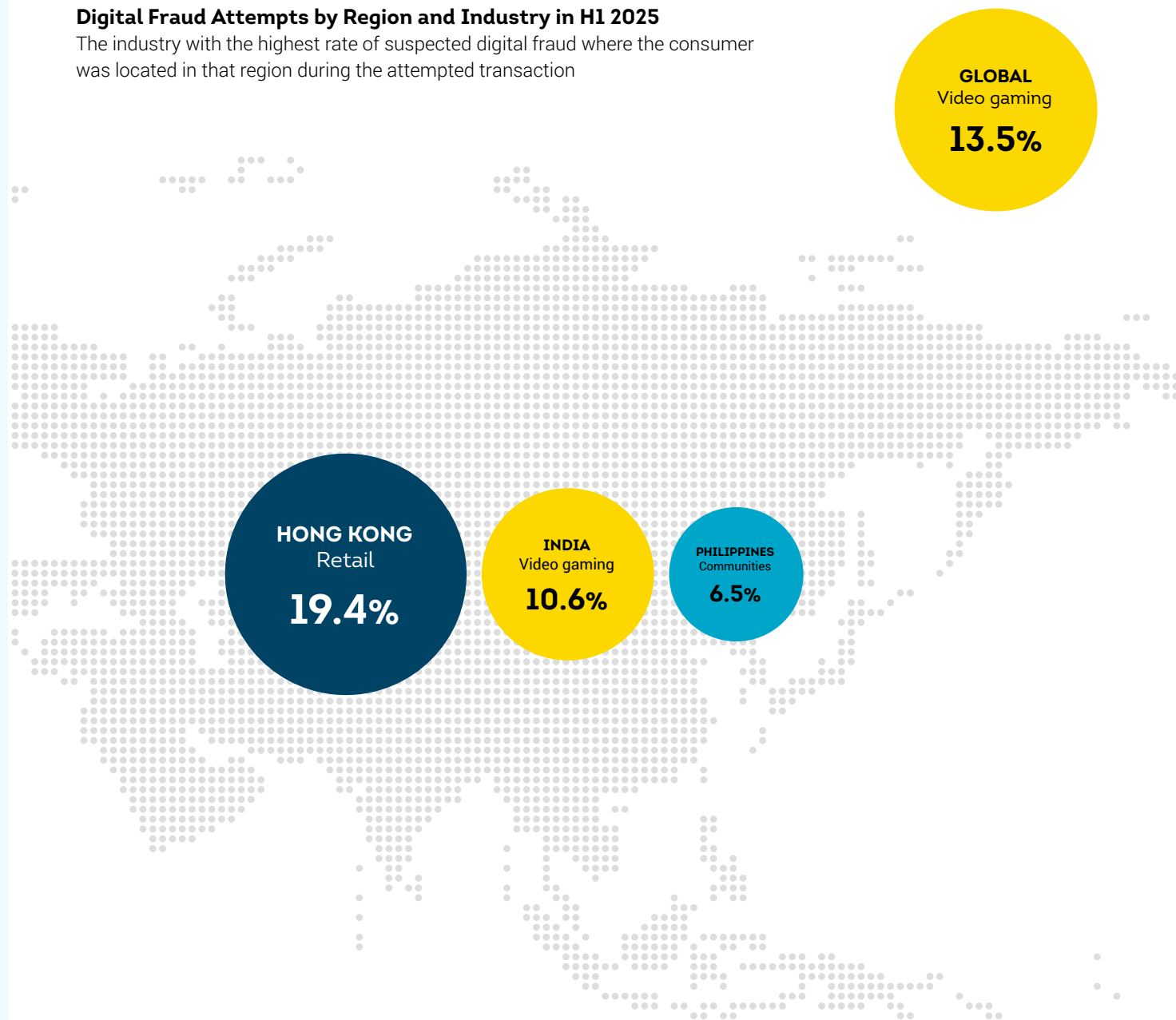
For transactions where the consumer was in the Philippines, community-based platforms had the highest rate of suspected digital among industries analysed at 6.5%, reflecting the exploitation of social trust and user-generated content. The high fraud rate in this sector underscores the need for stronger identity verification, behavioural analytics and moderation tools to detect and prevent fraudulent interactions.

India: Gaming sector most vulnerable

For transactions where the consumer was in India, video gaming had the highest rate of suspected fraud among industries analysed at 10.6%. This may be due to the mushrooming of video gaming apps coupled with the industry trying to acquire customers quickly. Many of the users are young, making them gullible for scams and account takeover.

Digital Fraud Attempts by Region and Industry in H1 2025

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



Source: TransUnion global intelligence network

Account login the highest risk digital stage for two of three markets

Hong Kong

The suspected digital fraud rate in H1 2025 for account logins where the consumer was in Hong Kong when transacting was 10.8%, more than two times higher than global average. This was potentially driven by phishing and credential theft. For account creation from Hong Kong, the rate was 3.8%, less than half the global average, suggesting strong onboarding controls. For financial transactions, the 0.3% rate was among the lowest globally, indicating robust payment security.

India

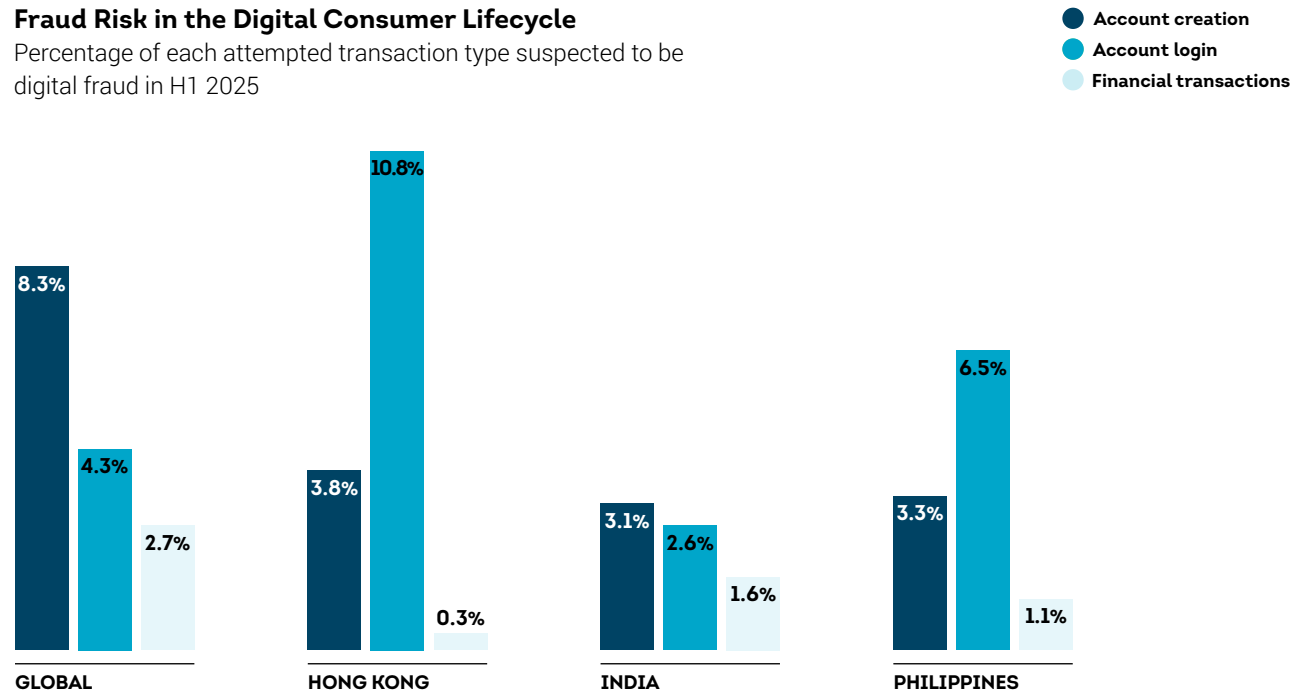
The suspected digital fraud rate in H1 2025 for account login attempts where the consumer was in India when transacting was 2.6%. Fraud during this stage could reflect widespread social engineering, phishing and smishing attacks. For account creation attempts from India, the rate was 3.1%. This shows the need for a stronger focus on identity verification solutions at the account opening phase. For financial transaction attempts, the 1.6% rate was lower than the global average. This suggests strong fraud mitigation methods deployed during payments.

Philippines

The suspected digital fraud rate in H1 2025 for account logins where the consumer was in the Philippines when transacting was 6.5%, above the global average. This could reflect widespread phishing and smishing attacks in the region. For account creation from the Philippines, the rate was lower than globally at 3.3%. For financial transactions, the 1.1% rate was also below the global average.

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

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



● UNITED KINGDOM

● SPAIN

EUROPE

Europe Overview

Within the UK and across Europe, the specter of fraud continues to manifest as a critical concern for consumers, organisations and the broader community. At the same time, attack vectors continue to evolve through GenAI, deepfakes and the burgeoning fraud-as-a-service industry. Added to this are the impacts of sluggish economic growth and a more relaxed attitude toward first-party fraud combined with higher customer experience expectations. Layer on recent and pending regulatory changes, and business leaders face a wave of challenges to mitigate the growing cost of fraud.

However, TransUnion insights reveal there's cause for some optimism: Data-led strategies enabled by leading technology can help reduce the risk of fraud loss while enhancing the customer experience. To evidence this, users of TransUnion solutions have reported a continued decline in risky digital transactions where the consumer is in the UK and Spain. This demonstrates achieving safe, profitable growth with genuine users, improved detection of bad actors, and reduced costs related to false positives and referrals can coexist.

European data in this section blends proprietary insights for digital fraud from TransUnion's global intelligence network in Spain and the UK, a business survey in the UK and a consumer survey in Spain and the UK.

KEY TAKEAWAYS

Cause for concern – the rising (and real) impact of fraud

69%
of UK fraud leaders said they were very or extremely concerned about the impact of fraud on their businesses

7.4%
of equivalent revenue lost due to fraud – representing £88 billion of fraud loss in the past year among 200 UK business leaders surveyed

New fraud types require new defences

54%
of UK fraud leaders ranked device reputation in their top three fraud preventing technologies, outpacing identity verification and making the UK the only market surveyed to rank device technology as highest preference

34%
of UK fraud leaders reported leveraging biometrics as a primary authentication tool, growing from 31% in 2024 but potentially remaining underutilised

To be aware or not to be aware – are consumers really?

53%
of UK consumers said they weren't targeted by email, online, phone call or text messaging fraud from February to May 2025; this rose to 72% in Spain

5%
of UK consumers said they were targeted and fell victim to email, online, phone call or text messaging fraud, down from 6% late last year; in Spain, this fell from 10% to 7%

Concern around and the cost of fraud rises

Fraud ranked as the most prevalent crime in England and Wales – accounting for more than 40% of reported crime, according to the Crime Survey for England and Wales for the year ending September 2024. Therefore, it's not surprising UK fraud leaders TransUnion surveyed who reported being very or extremely concerned about the impact of fraud on their businesses rose from 55% in 2024 to 69% in 2025. This year's response is in line with the global average of 70%.

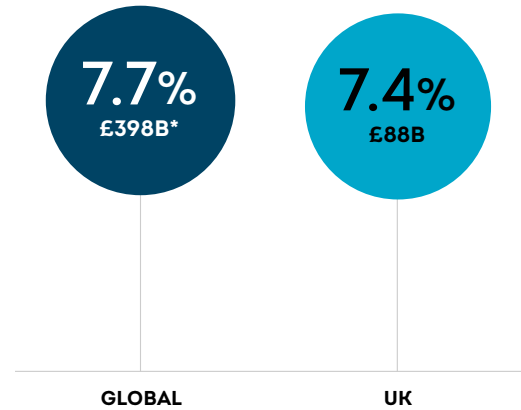
This concern correlates with rises in estimated losses. Global leaders reported an increase from 6.5% of equivalent revenue lost to fraud in 2024 to 7.7% in 2025. In contrast, UK fraud leaders reported a more significant jump, rising from 5.7% in 2024 to 7.4% in 2025 (equating to £88b across the 200 UK leaders surveyed in 2025).

UK Fraud leaders identified scam/authorised fraud (23%), synthetic identity (23%) and account takeover (20%) as the three primary causes of fraud losses.

At a sector level, UK financial services leaders cited synthetic identity the most at 26%. For UK retail organisations, account takeover and synthetic identity were both cited the most at 26%. Within UK telecommunications companies, 31% of leaders highlighted both synthetic identity and scam/authorised fraud the most.

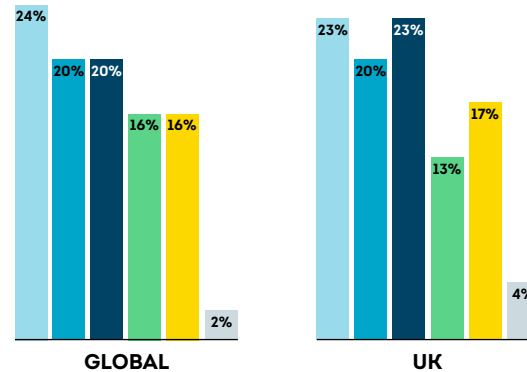
Total Cost of Fraud

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

Most Prominent Cause of Fraud Losses



Source: TransUnion business survey

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

Identity verification the most effective fraud prevention method

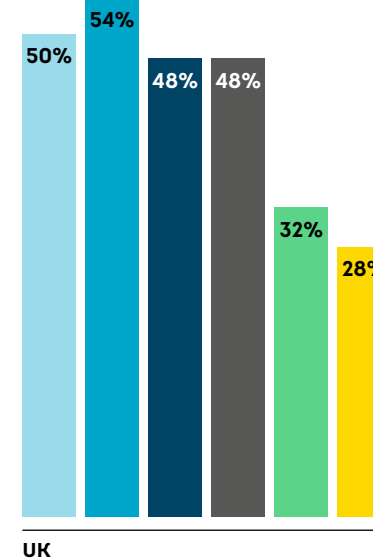
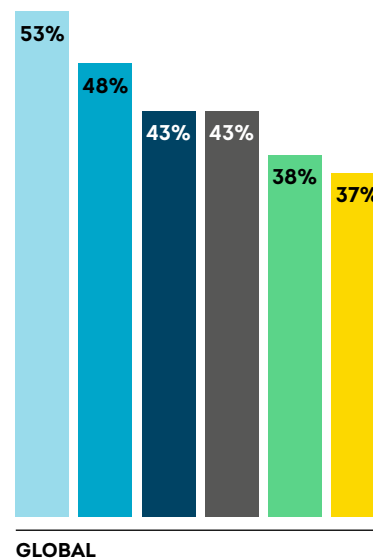
With rising fraud challenges and often static budgets, fraud leaders are increasingly looking to maximise the effectiveness of their data and technology investments. With advancements in technologies used by bad actors, it's imperative organisations don't solely rely only on traditional methods of fraud detection. Notwithstanding this, positive identity verification (which can include advancements in deepfake detection, liveness checks and biometrics) remains the preferred method by global leaders across regions, with 50% or more respondents in every market citing this as one of their three preferred fraud-fighting technologies.

The UK stood out, however, with device reputation (54%) most cited as preferred – followed by identity verification (50%), and IP intelligence and behavioural solutions (both 48%). Notably, traditional digital signals, such as email reputation (32%) and phone number reputation (28%), appeared to be less favoured by UK fraud leaders compared to others globally.

Preferred technologies vary by industry

At a sector level, there was limited consistency in terms of the top three preferred technologies, demonstrating the range of threat vectors that need to be managed. While UK financial services leaders point to identity verification (58%), device intelligence (49%) and behavioural insights (47%), UK retail leaders report relying most on device intelligence (60%). For telco operators, leaders put the most reliance on IP intelligence (73%).

Technology Ranked as Most Effective for Preventing Fraud



- Identity verification
- Device reputation
- Behavioural biometrics
- IP intelligence
- Email reputation
- Phone number reputation

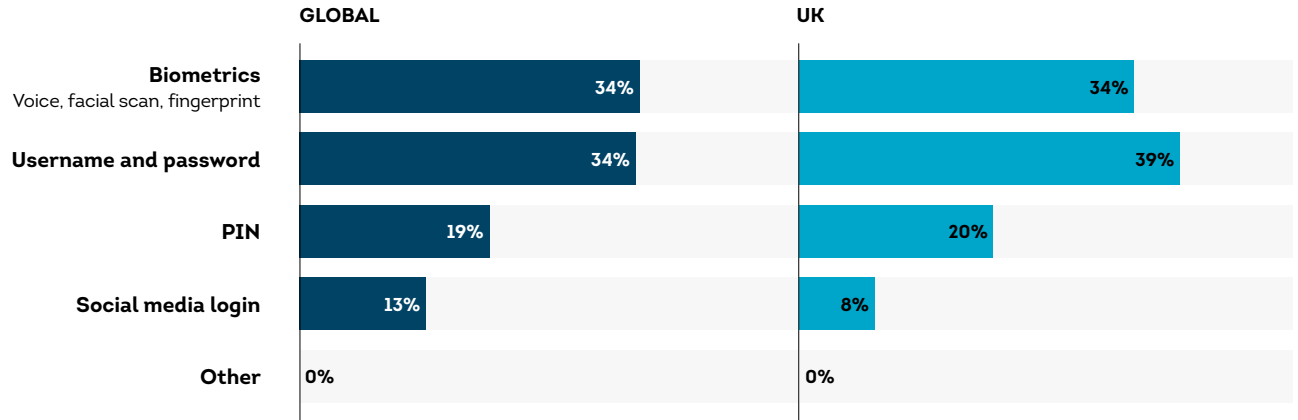
Source: TransUnion business survey

Evolution from traditional authentication methods

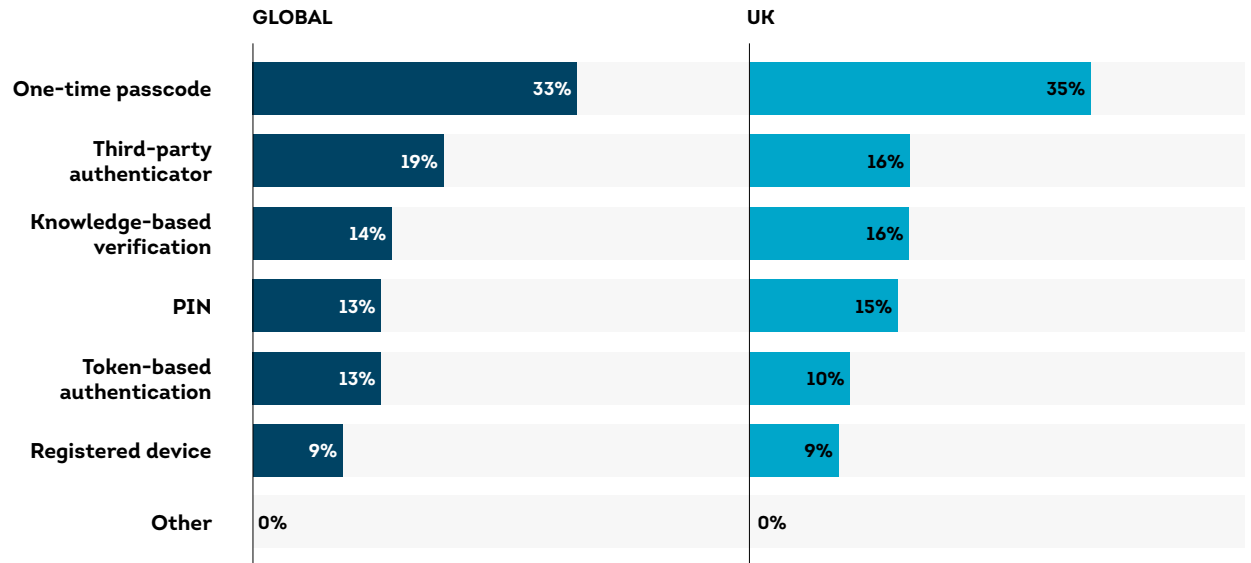
Authentication through the consumer lifecycle remains a consistent challenge for organisations. In particular, how to make it as seamless as possible for genuine consumers but ensure a continued view to establish and augment ongoing trust, and – in particular – identify bad actors who insert themselves throughout. Evolving from traditional methods has been a focus for fraud leaders, though our survey observed a continued reliance on traditional methods, such as username/password, which UK business leaders said were their top primary methods of authentication at 39%. The UK has traditionally been a leader in the use of biometrics as a primary method of authentication, and this continued to grow from 31% in 2024 to 34% in 2025. UK leaders continue to avoid social media credentials; only 8% of UK organisations leveraged this as a primary authentication method compared to a global average of 13%.

Secondary methods of authentication revealed interesting insights – and perhaps confirmed a case for change. In the UK, there remains strong reliance on one-time passcodes (35%), which are well-known to be susceptible to social engineering and access via bad actors. Knowledge-based verification (another traditional though problematic authentication technique) remained at 16% usage in the UK. Organisations should consider alternatives, such as biometrics, behavioural signals and device authentication.

Primary Method Used to Authenticate Customers



Secondary Method Used to Authenticate Customers



Source: TransUnion business survey

Consumer fraud awareness remains relatively low

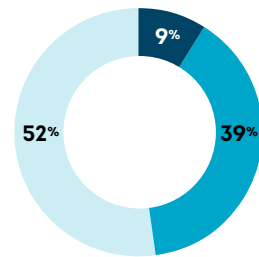
Concerted efforts to raise consumer awareness around fraud threats – and how to avoid, mitigate and report them – may be starting to take effect. Our consumer surveys found a reduction in consumers who said they were targeted and fell victim to email, phone, phone call or text messaging fraud in the last three months: In Spain, this fell from 10% in late-2024 to 7% in mid-2025, and the UK had a smaller decrease from 6% to 5%. For consumers who reported being targeted and not falling victim, this also fell: 25% to 21% in Spain and 44% to 42% in the UK.

Interestingly, fraud awareness remains relatively low – considering the preponderance of fraud attempts across all channels. Consumers who reported not being targeted by fraud in last three months rose to 53% in the UK and 72% in Spain from 50% and 65%, respectively in late 2024. Rather than signalling a reduction in fraud attempts, this may actually indicate an evolution in attacks from traditional phishing and smishing types to social media, marketplace and money/gift card scams – which consumers may be less familiar with and able to identify.

Organisations need to think creatively regarding how to maintain relevancy of their messaging. For example, rather than relying on generic messaging during a financial services transaction journey, financial institutions can consider leveraging AI and other customer datasets to better target messages based on behaviour and history. Alternatively, consideration should be given to a segment of transactions (for example, high-value or unusual transactions) to be queued for step-up authentication.

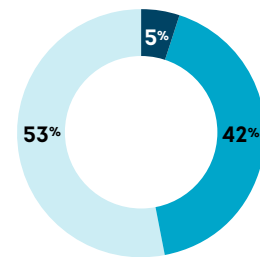
Consumers Targeted With Fraud

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.



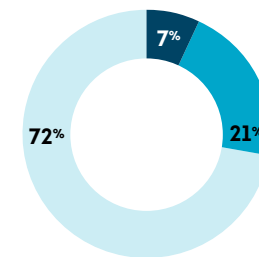
GLOBAL

- Smishing



UK

- Phishing



SPAIN

- Smishing

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

Source: TransUnion consumer survey

Digital Fraud Trends

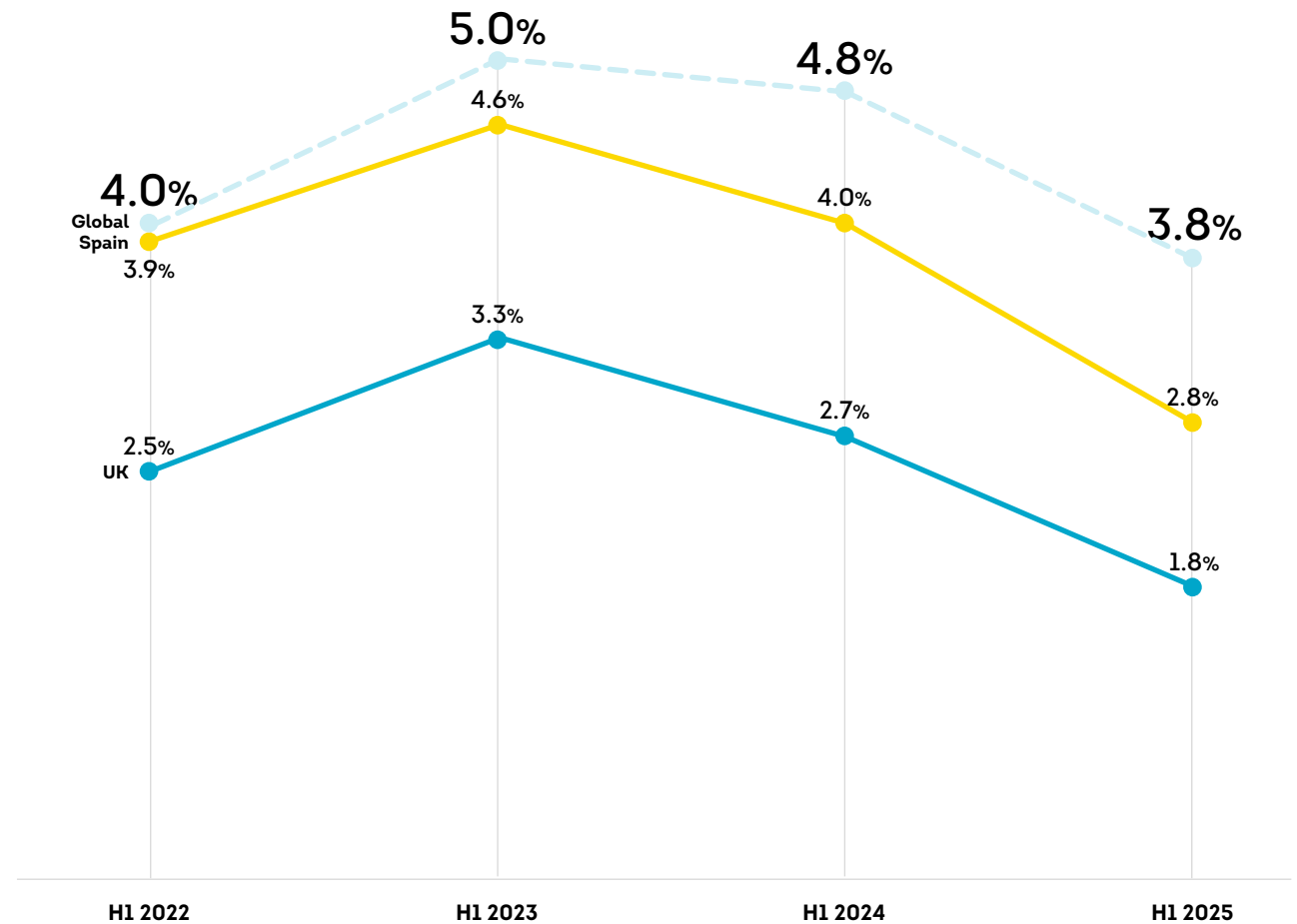
Enhancements to fraud detection could be moderating fraud rate

As mature organisations fine-tune fraud strategies and less mature organisations adopt new technologies, TransUnion is observing a trend of reduced suspected digital fraud attempts across sectors and regions. Globally, there's been a decline to 3.8%, while Spain has experienced a more pronounced drop from a four-year high of 4.6% in H1 2023 to 2.8% in H1 2025. Similarly, the UK has seen a drop from 3.3% in H1 2023 to 1.8% in H1 2025.

These reductions could be partly attributed to:

- Collaboration with clients: Working closely with clients to fine-tune and optimise rulesets, clients have provided valuable feedback on rule performance, in addition to fraud outcome data helping identify areas where false deny rates were high and adjustments could be made.
- Enhanced algorithms and machine learning: Significant improvements have been made in the underlying analytical capability of fraud rule optimisation. Machine learning models are more adept at distinguishing between legitimate and fraudulent activity, resulting in fewer false positives.
- Enhanced underlying data: A strong data foundation remains key to leverage flags and predictive models related to device and behavioural insights. For example, strong capture rate, returning device recognition strength and non-human activity detection, as well as consortia breadth.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

Communities industry continues to experience the highest suspected digital fraud rate

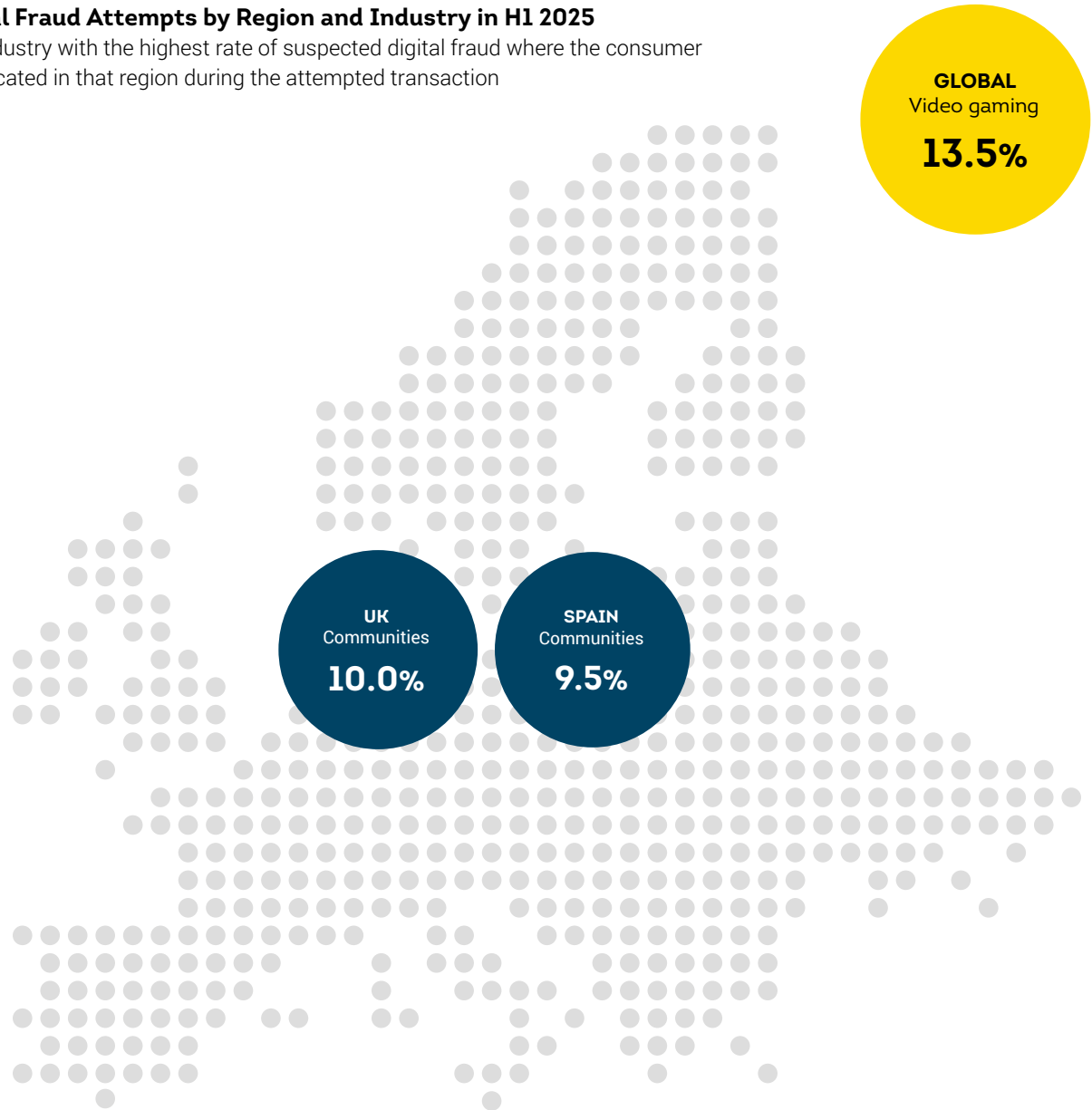
Communities, which include organisations like online forums and dating sites, showed some lowering in the rate of suspected digital fraud attempts in the first half of 2025 for transactions where the consumer was in Spain or the UK. However, it remains the industry with the highest rate across analysed sectors in the UK and Spain (it was also the highest in H1 and H2 2024) as bad actors take advantage of inherent trust in community-based platforms through scams and solicitation. In the UK, communities saw a large jump from 8.7% in H1 2023 to 14.1% in H1 2024 – but then a decline to 12.1% in H2 2024 and 10.0% in H1 2025. Similarly, in Spain, the sector saw a jump from 9.6% in H1 2023 to 14.9% in H1 2024, and a steady reduction to 13.1% in H2 2024 and 9.5% in H1 2025.

In the UK, government was the sector with the next highest level of suspected digital fraud attempts (at 6.9% in H1 2025), which was down from 2H 2024 at 7.1% but up from H1 2024 at 5.9%. Positively, gaming has seen a steady decline in suspected digital fraud attempts – potentially as a result of increased usage of a range of next-generation tools, such as biometrics, behavioural signals and IP intelligence. In H2 2025, the rate of suspected digital fraud in gaming of 2.9% showed a strong drop from 4.4% in H1 2024.

In Spain, gaming was the sector with the second highest rate of suspected digital fraud attempts at 8.0%, up from 6.6% in H1 2024.

Digital Fraud Attempts by Region and Industry in H1 2025

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



Source: TransUnion global intelligence network

Despite improvement, suspected digital fraud in consumer lifecycle most prevalent during account creation

Across the globe, the onboarding stage of the digital consumer lifecycle consistently shows the greatest level of suspected fraud attempts: 8.3% was recorded for account creation in H1 2025. The same holds true in both the UK and Spain. In Spain, there's been a reduction from 8.8% in H1 2024 to 6.8% in H1 2025, a 23% reduction. Meanwhile in the UK, there has been a reduction from 6.1% in H1 2024 to 4.9% in H1 2025, a 20% decrease.

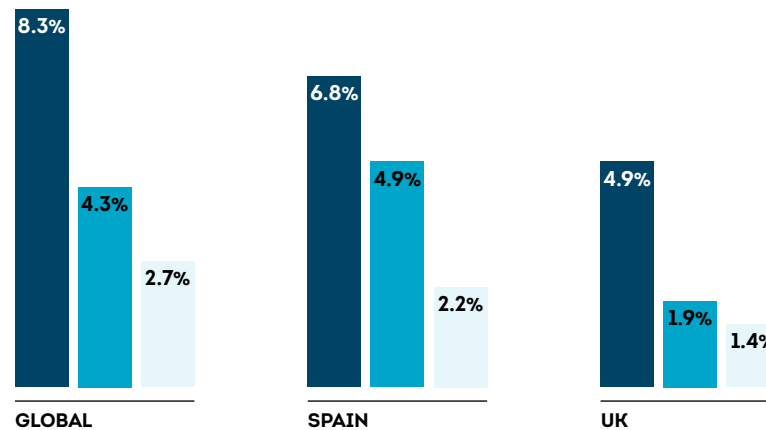
With the rising threat of account takeover through solicitation and remote tooling, the UK experienced an increase in logins with suspected digital fraud attempts, rising from 2.8% in H1 2024 to 3.2% in H2 2024, though this reduced to 1.9% in H1 2025. Spain observed an even greater reduction at this stage of the consumer lifecycle, moving from 10.3% in H1 2024 to 4.9% in H1 2025. Notably, the Spain rate was higher than the global rate of 4.3%.

Globally, financial transactions saw 2.7% of suspected digital fraud attempts in H1 2025. As per other stages in the consumer lifecycle, the UK observed a decrease from 2.7% in H1 2024 to 1.4% most recently. Interestingly, however, Spain saw an increase from 1.7% in H1 2024 to 2.2% in H1 2025, suggesting Spanish organisations may need to consider additional controls at critical, high-value points of their consumer lifecycles.

Fraud Risk in the Digital Consumer Lifecycle

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

- Account creation
- Account login
- Financial transactions



Source: TransUnion global intelligence network

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

LATIN AMERICA



Latin America Overview

Thanks to the investments companies have made – and continue to make – in strategies aimed at establishing identity and mitigating fraud across our region, the rate of suspected digital fraud attempts has decreased for transactions where the consumer was located in all Latin American countries we analysed except for Puerto Rico where it increased a small 2% in the first half of the year compared to the same period in 2024. However, a high percentage of suspicious transactions continues to be observed in the creation of new accounts through digital channels.

Consumers remain both targets and victims of various fraud schemes, with Latin Americans we surveyed reporting smishing and vishing as the most prevalent. As such, fraud prevention strategies must continue to place the consumer at the centre, emphasising the protection of personal information and credentials. This should be achieved through sustained education and awareness campaigns aimed at mitigating schemes like account takeover.

Latin American data in this section blends proprietary insights for digital fraud from TransUnion's global intelligence network in Brazil, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Mexico, Nicaragua and Puerto Rico; and a consumer survey in Brazil, Chile, Colombia, the Dominican Republic and Guatemala.

KEY TAKEAWAYS

Target in sight – consumers remain exposed to fraudulent schemes

34%

of consumers in the Latin America countries we surveyed said they were targeted by email, online, phone call and text messaging fraud from February to May 2025, with Chile and Colombia having the highest rates

34%

of those who said they were targeted in Latin America reported being attacked with vishing, making it the most cited fraud scheme in the region

Relentless attempts – unabated suspicious transactions

11%

increase in the rate of suspected digital fraud for financial transaction attempts from Latin American countries analysed in the first half of 2025 compared to the first half of 2024

5%

of digital account creation attempts from Latin American countries analysed suspected to be digital fraud in H1 2025

Cost remains high – fraudsters persist in exploiting opportunities

25%

of business executives we surveyed reported their companies lost the equivalent of 10% or more of their revenues in the past year

42%

of business executives we surveyed believed account takeover attacks start online – followed by 20% indicating they begin with mobile applications

Consumer Fraud Experiences

Fraudsters targeting consumers through their preferred channels

While more than one-third (34%) of consumers surveyed in Latin America reported being targeted by an email, online, phone call or text messaging fraud scheme in the last three months (less than the global rate of 48%), a significant portion of the population may not recognise potential fraud: 66% said they were unaware of being targeted.

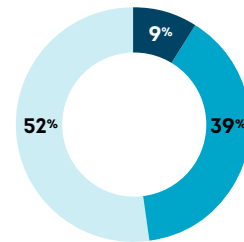
Among those who said they were targeted, vishing at 34% and smishing at 31% were the leading types of fraud consumers reported experiencing among those who said they were targeted in the last three months.

While criminals will attack at any time using any channel, they appear to focus on popular channels. In Chile and Colombia where mobile phone subscriptions are higher than other Latin American countries,¹ the most common attack vector reported by consumers was vishing.

Consumers Targeted With Fraud

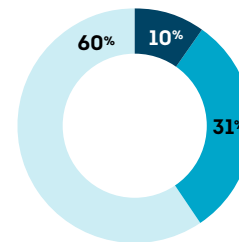
Percentage of consumers who said fraudsters targeted them with email, online, phone call or text messaging fraud attempts from February to May 2025, and the most frequent scheme by which they reported being attacked.

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



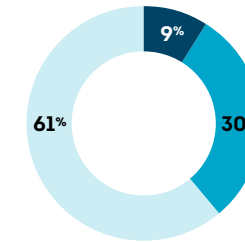
GLOBAL

- Smishing



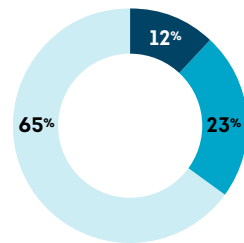
CHILE

- Vishing



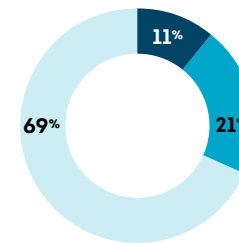
COLOMBIA (TIE)

- Smishing
- Vishing



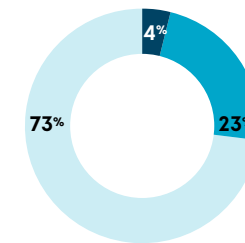
GUATEMALA (TIE)

- Money/gift card
- Third-party seller scams on legitimate sites



DOMINICAN REPUBLIC (TIE)

- Money/gift card
- Third-party seller scams on legitimate sites



BRAZIL

- Vishing

Source: TransUnion consumer survey

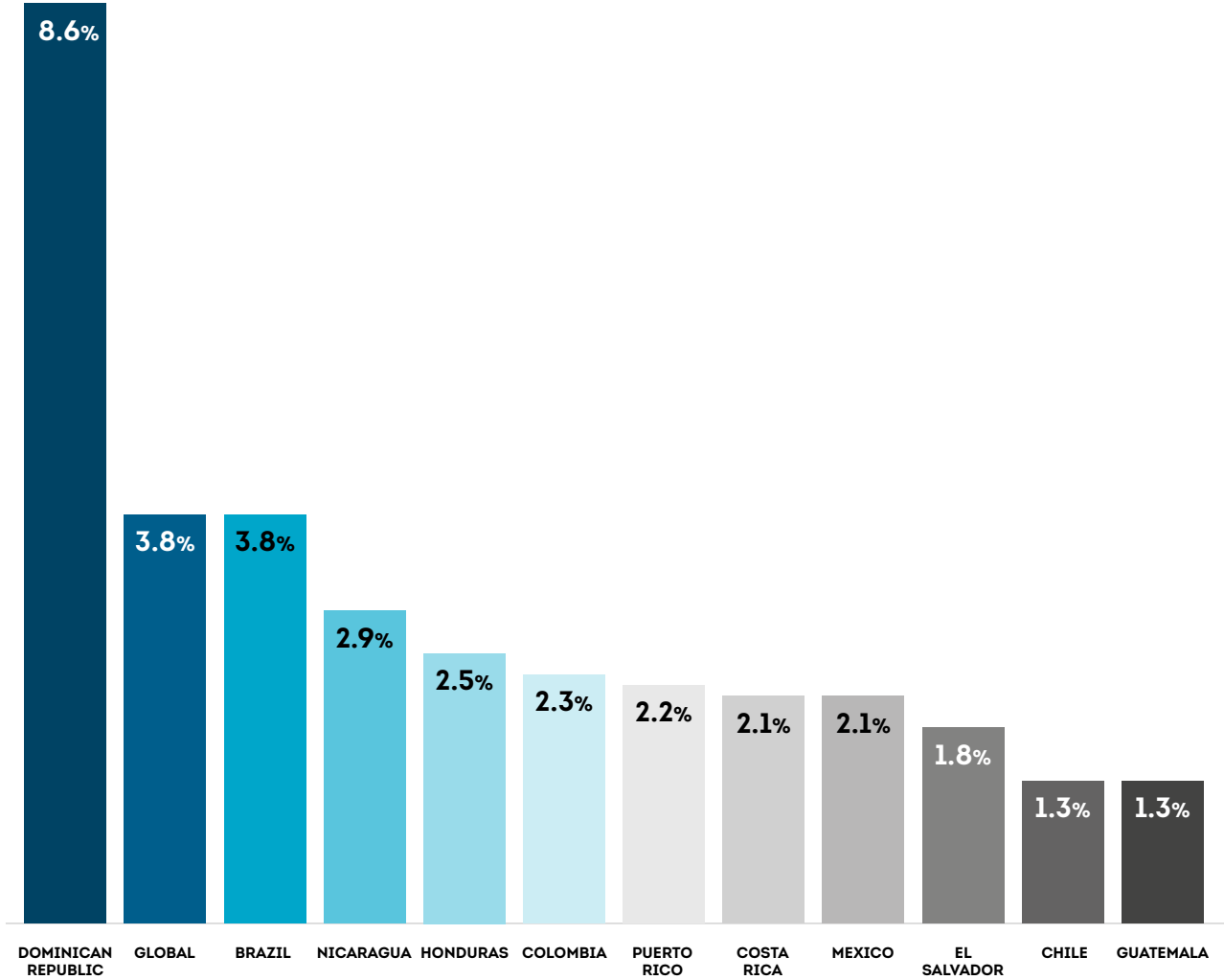
¹ World Bank Group: Mobile cellular subscriptions (per 100 people) – Colombia, Chile, Dominican Republic, Brazil, Guatemala | Data

Digital Fraud Trends

Suspected digital fraud rates stabilised, higher in key Latin American markets

The global rate of suspected digital fraud attempts among TransUnion customers remained below 5% in the first half of 2025, registering at 3.8%. This reflects the continued effectiveness of fraud prevention strategies across key markets. In the Latin American markets we analysed, three markets (Brazil, the Dominican Republic and Nicaragua) reported rates above the regional average of 2.8%, highlighting the need for enhanced fraud mitigation efforts in these geographies. These elevated levels suggest fraudsters are actively targeting specific markets where vulnerabilities may still exist.

Rate of Suspected Digital Fraud
H1 2025



Source: TransUnion global intelligence network

Certain sectors targeted by fraudsters in certain countries

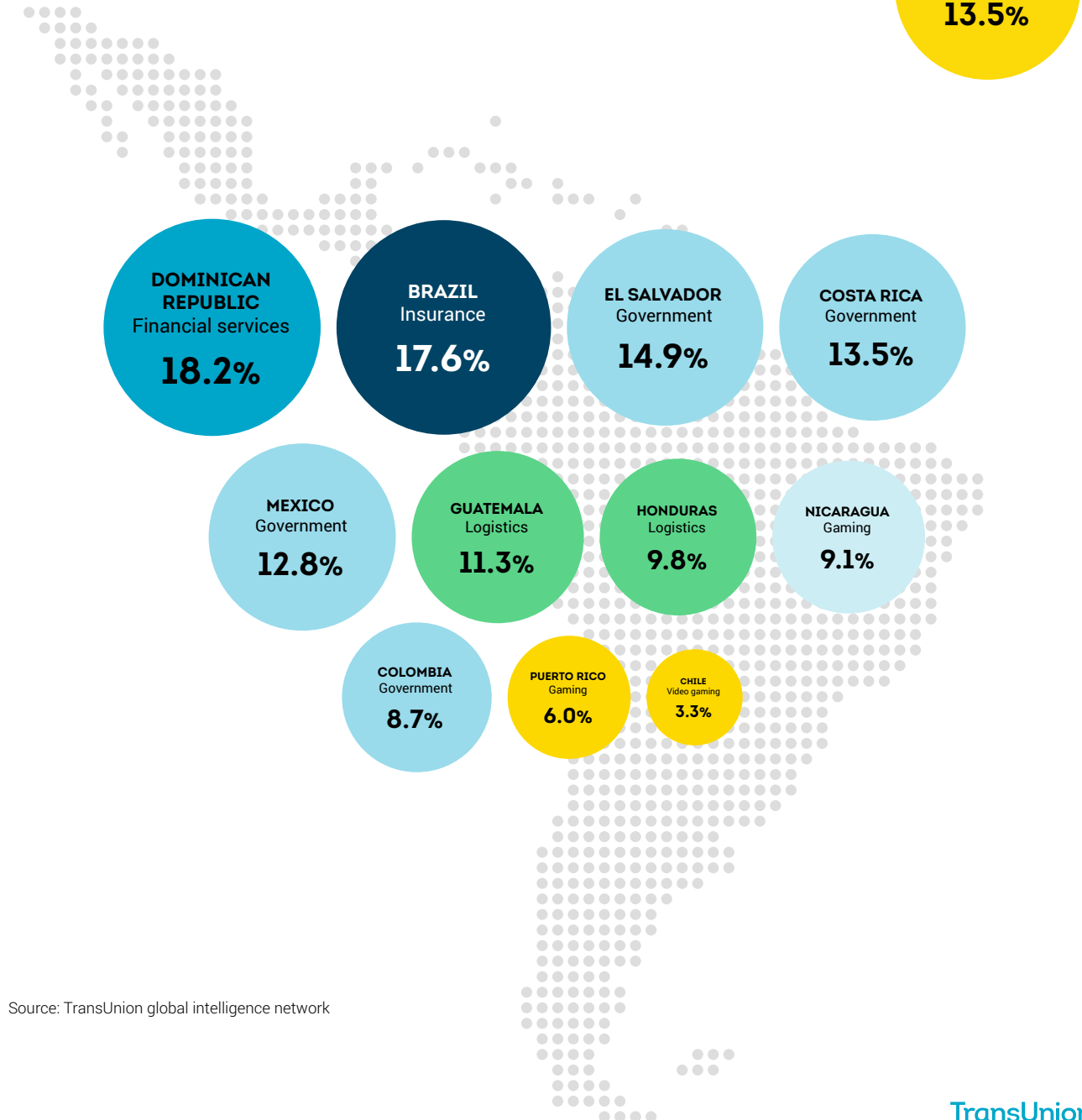
Among industries analysed globally, the video gaming sector recorded the highest percentage of suspected digital fraud attempts in the first half of 2025, reaching 13.5%. This represents a significant 28% increase in volume compared to the same period in 2024, underscoring the growing vulnerability of this sector to fraudulent activity.

In Latin America, specific industries within individual markets also exhibited elevated fraud rates. For instance, for transactions where the consumer was in the Dominican Republic, the financial services sector reported the highest rate (18.2%) of suspected digital fraud across industries analysed in H1 2025. In Brazil, the insurance sector led with a rate of 17.6%. These figures highlight the need for targeted fraud prevention strategies within these verticals.

Across many other countries analysed in the region, the government sector had the highest rate, with an average increase of 80% compared to H1 2024 in Latin America. This trend reflects the continued efforts of fraudsters to exploit sectors handling sensitive personal data.

Digital Fraud Attempts by Country and Industry in H1 2025

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



Source: TransUnion global intelligence network

Risky identities impact all stages of the consumer lifecycle

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

Account creation had the highest growth in fraud risk across the digital consumer lifecycle, increasing by 26% globally from H1 2024 to H1 2025. For transactions where the consumer was in Latin America, account creation emerged as the riskiest digital transaction type, with 5% of those transaction types suspected to be digital fraud attempts. Account creation was also the riskiest transaction type in the consumer lifecycle with a global rate of 8.3%.

Costa Rica and the Dominican Republic led the region among countries analysed in account creation fraud risk, reporting rates of 10.6% and 14.2%, respectively. These trends highlight the growing need for robust identity verification and fraud prevention strategies at the earliest stages of digital engagement.

Consumer Lifecycle Stage Examples

Account creation: Account signup, registration and loan origination

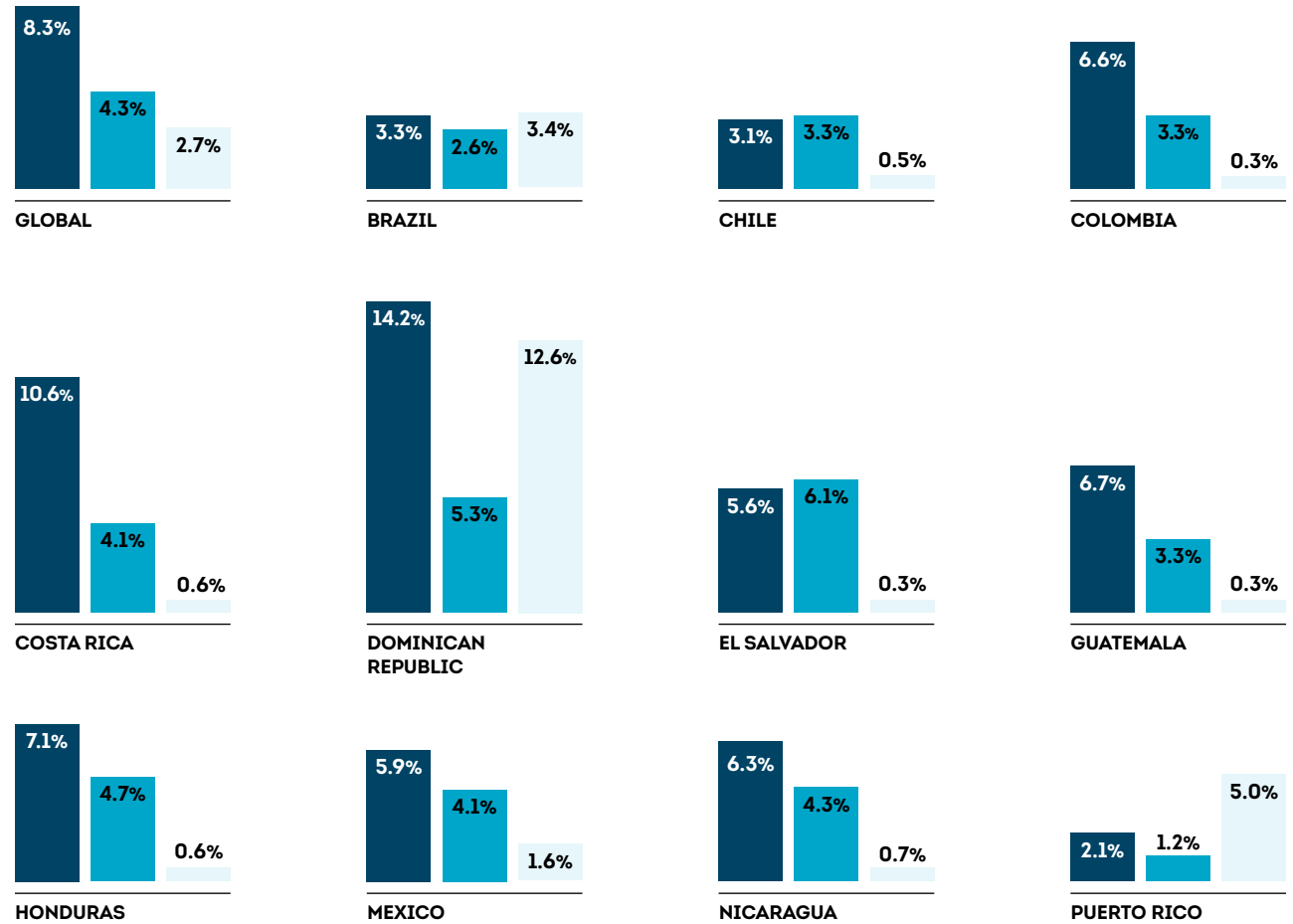
Account login: Login and failed login events

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

- Account creation
- Account login
- Financial transactions



Source: TransUnion global intelligence network



● CANADA

NORTH AMERICA

Canada Overview

Canadian business leaders are reporting rising losses, primarily from scams/authorised fraud, synthetic identity fraud and account takeover, while third-party fraud appears to be stabilising. 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 organisations improve detection accuracy, expand digital self-service and strike the right balance between security and convenience.

KEY TAKEAWAYS

Scam/authorised fraud and synthetic identity fraud drive major losses

29%

of fraud losses stem from scam/authorised 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

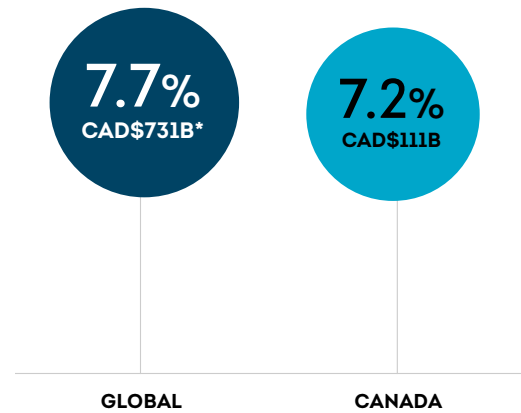
Fraud losses in Canada climb, with shifting causes

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/authorised 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 organisations must remain vigilant as the landscape evolves, balancing innovation with resilience in the face of increasingly sophisticated threats.

Total Cost of Fraud

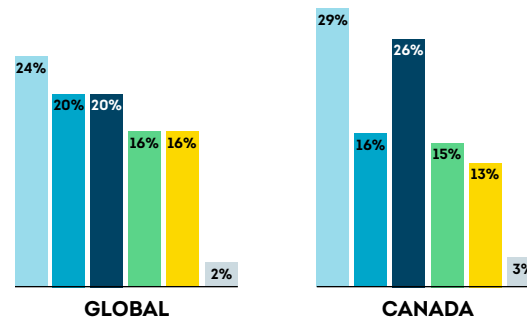
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding monetary amount total



*Based on currency exchange value on July 16, 2025

Source: TransUnion business survey

Most Prominent Cause of Fraud Losses



Source: TransUnion business survey

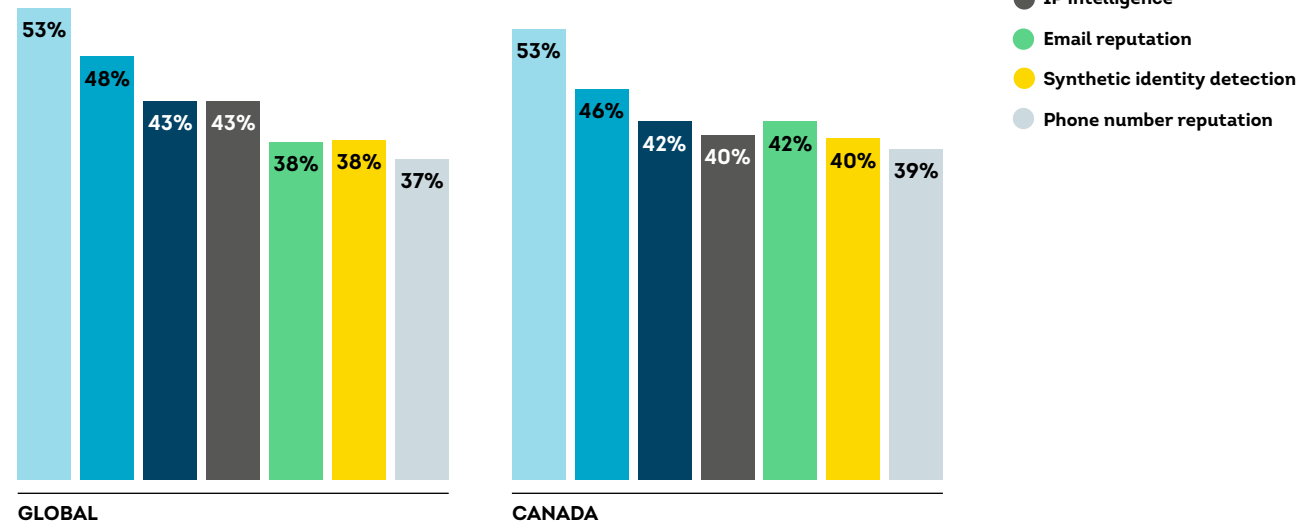
- **Scam/Authorised fraud**
Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Account takeover**
Unauthorised individuals taking over someone's online account (e.g., bank, social media, email) without their permission
- **Synthetic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

Technology strengthens Canada's fraud defense 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 organisations also emphasise 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 digitising 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



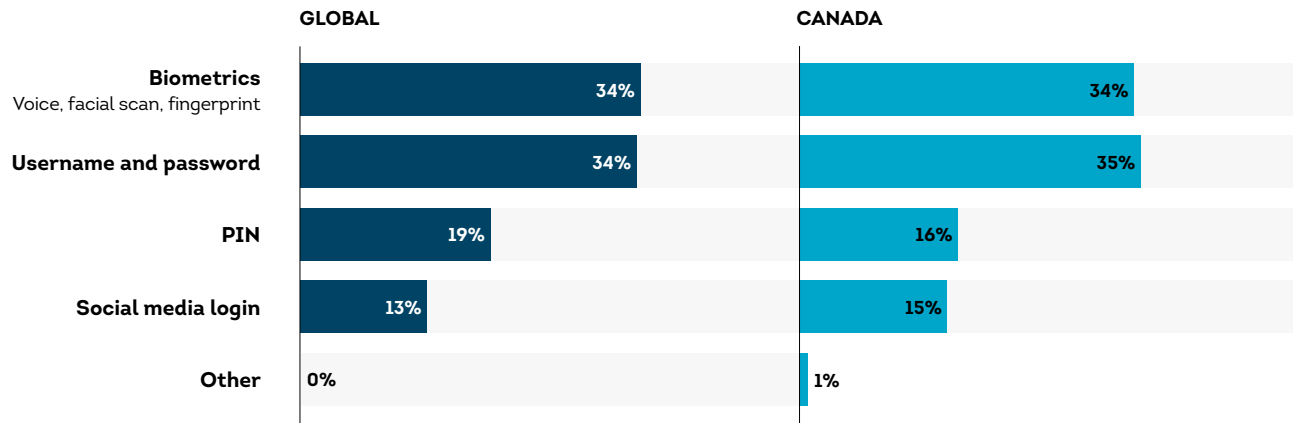
Source: TransUnion business survey

Evolving authentication practices reflect shifting fraud priorities

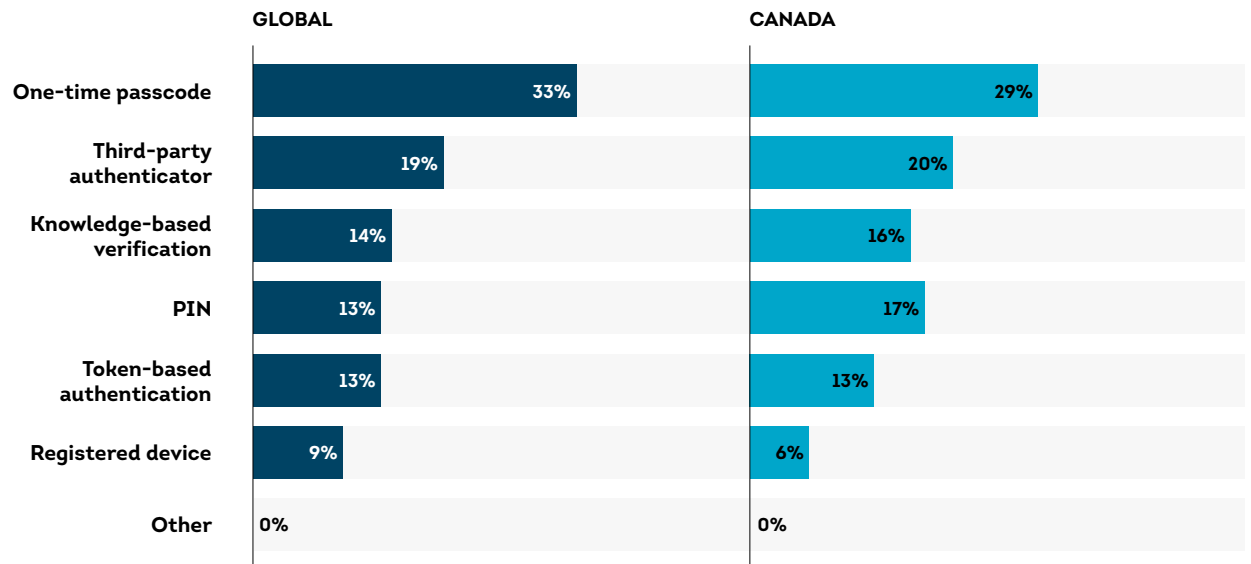
Authenticating consumers continues to be a vital part of fraud prevention strategies, especially as digital engagement grows. Despite its limitations, username and password remains the most widely used primary authentication method, according to Canadian business leaders. However, biometric authentication 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 modernise 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

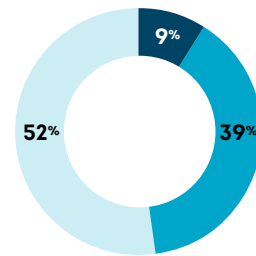
Consumers face emerging fraud threats

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 personalised, 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 victimisation rate is encouraging, the evolving nature of fraud highlights the need for continued awareness and education to help individuals recognise and respond to deceptive tactics with confidence.

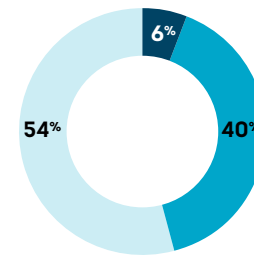
Consumers Targeted With Fraud

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.



GLOBAL

- Smishing



CANADA (TIE)

- Phishing
- Vishing

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

Source: TransUnion consumer survey

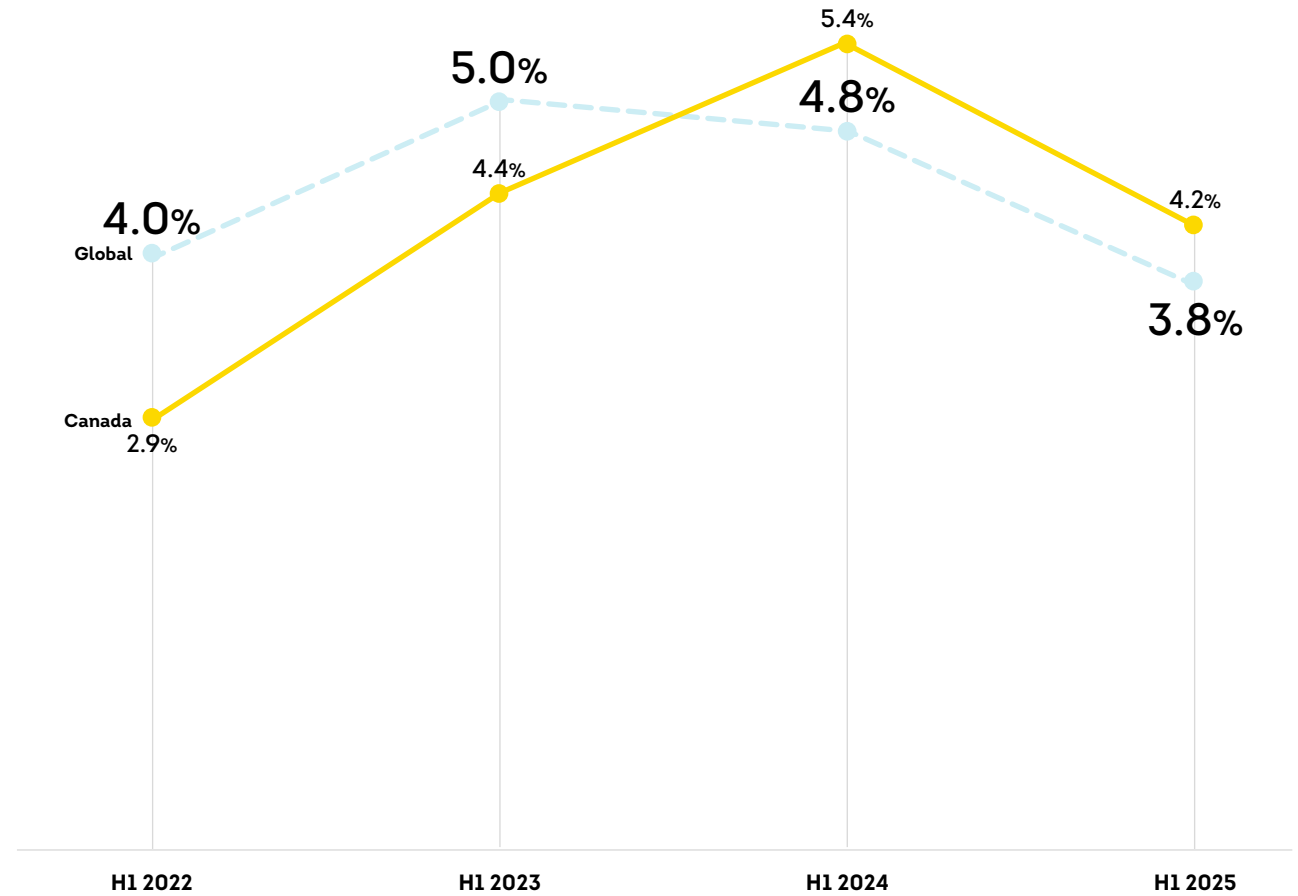
Digital Fraud Trends

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

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 analysed, 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 organisations, 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

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

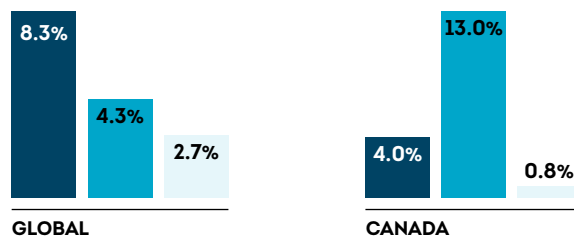
Account creation: Account signup, registration and loan origination

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

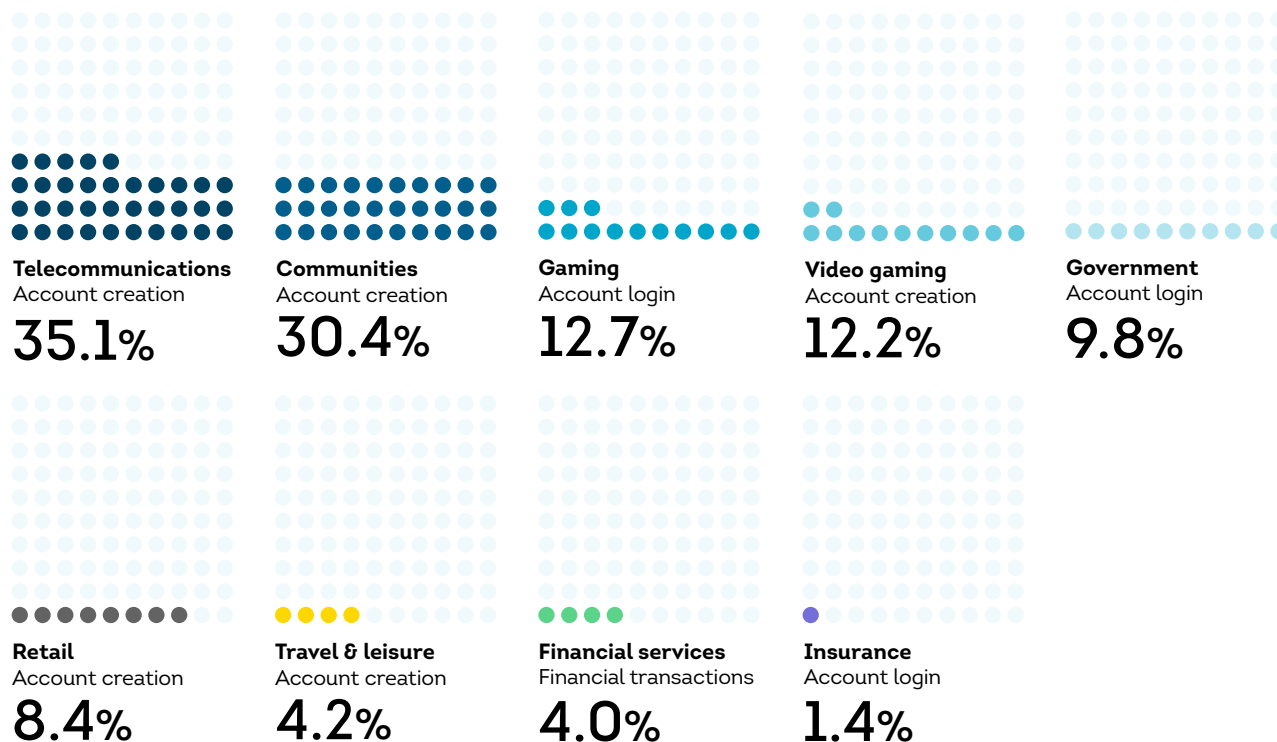


Source: TransUnion global intelligence network

- Account creation
- Account login
- Financial transactions

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



● UNITED STATES

NORTH AMERICA

United States Overview

Fraud schemes are getting more sophisticated, and the US is a target-rich environment for bad actors. US fraud prevention leaders recognise 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 organisations

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

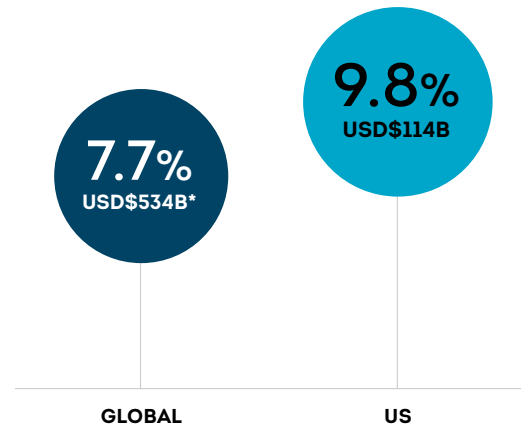
The cost of fraud rising

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/authorised fraud (23%).

Total Cost of Fraud

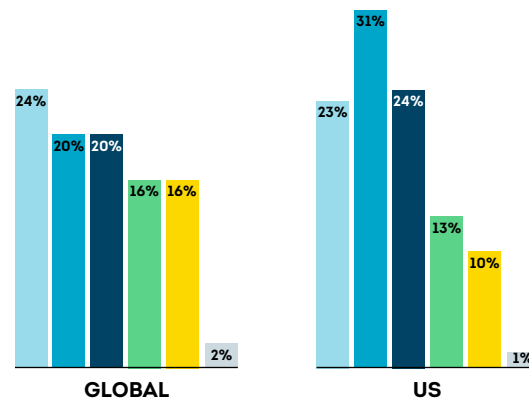
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding monetary amount total



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

Source: TransUnion business survey

Most Prominent Cause of Fraud Losses



Source: TransUnion business survey

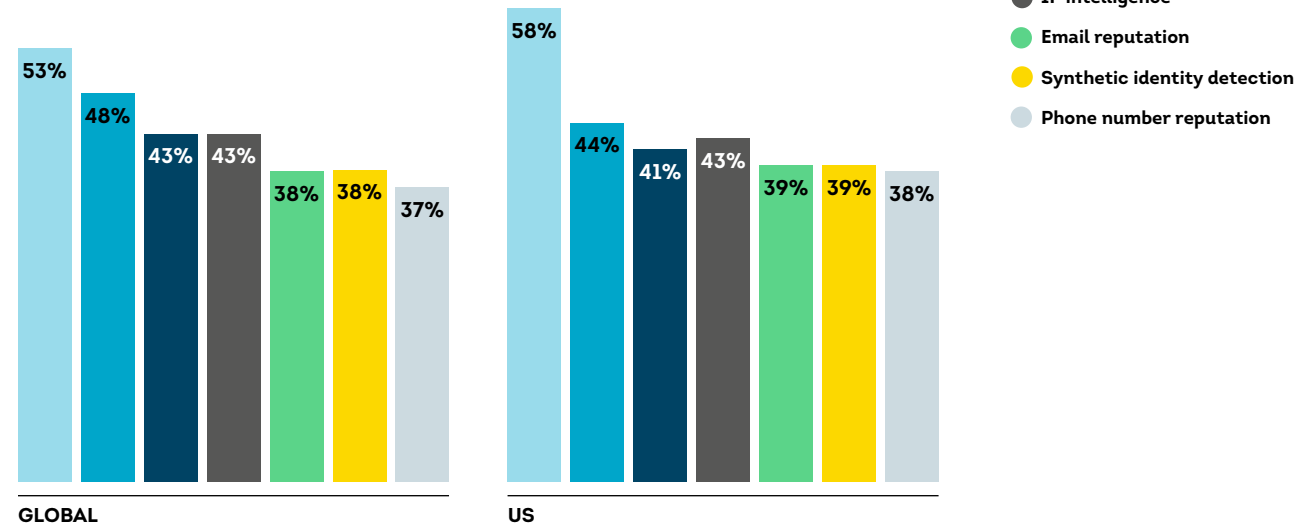
- **Scam/Authorised fraud**
Dishonest scheme intended to trick a person into giving up something of value (e.g., account access, money, information)
- **Account takeover**
Unauthorised individuals taking over someone's online account (e.g., bank, social media, email) without their permission
- **Synthetic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

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



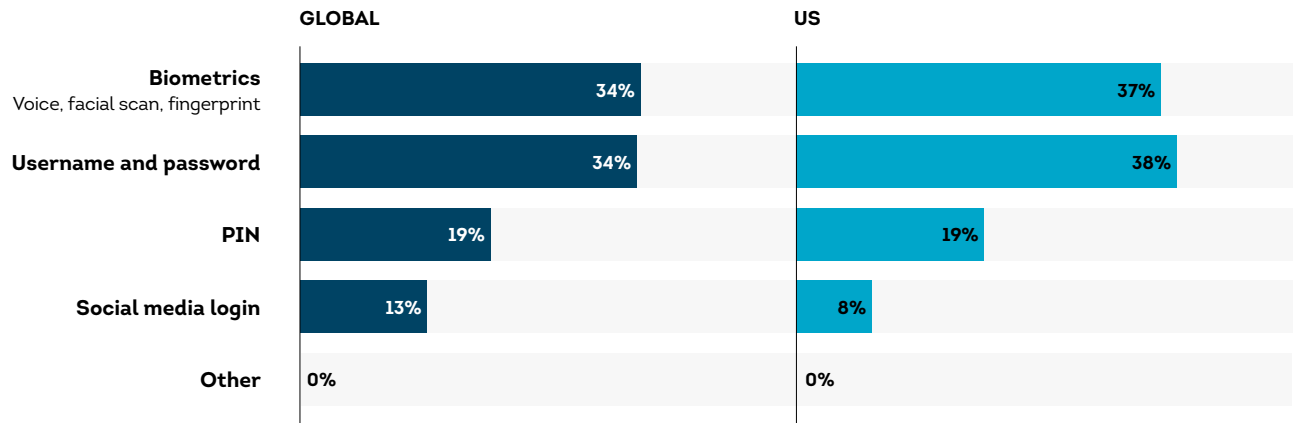
Source: TransUnion business survey

Biometrics catch up with passwords as primary authentication method

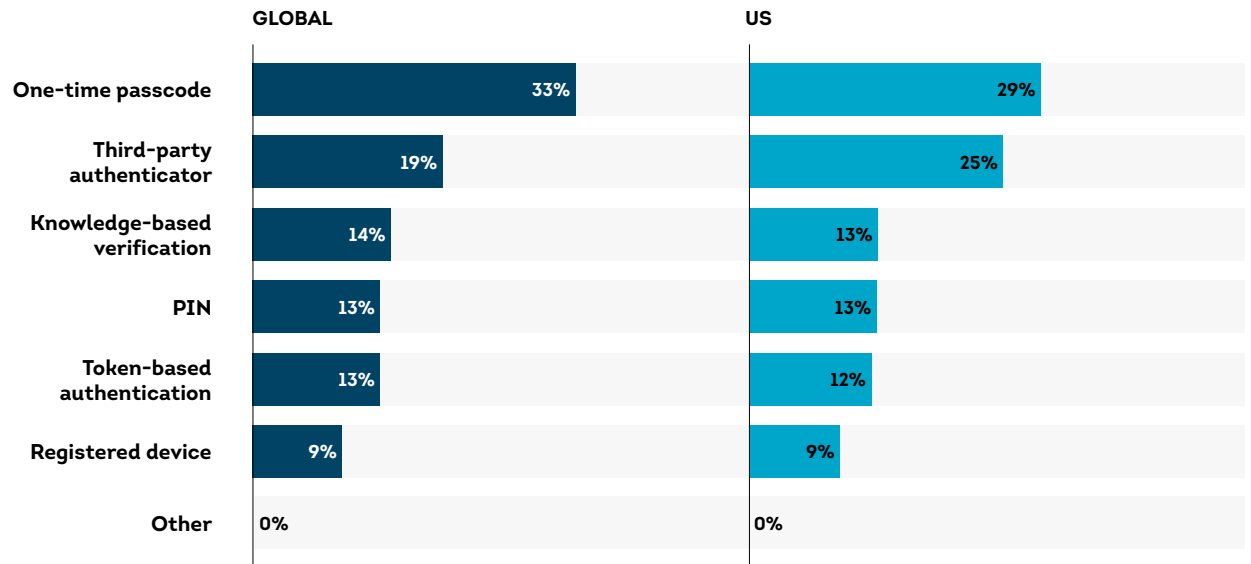
User credentials remain under threat from consumer scams and data breaches. It's no wonder US business leaders reported ATO as the primary reason behind fraud losses. To stem the tide, US business leaders appear to be moving away from simple username and password authentication to embedding biometric verification into their authentication programs. While more than a third (38%) of US business leaders said they still utilise 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 utilise 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

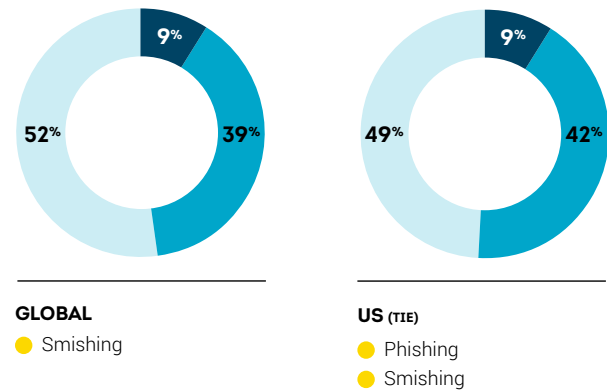
Phishing and smishing tied for most common consumer-reported fraud scheme

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 recognise 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

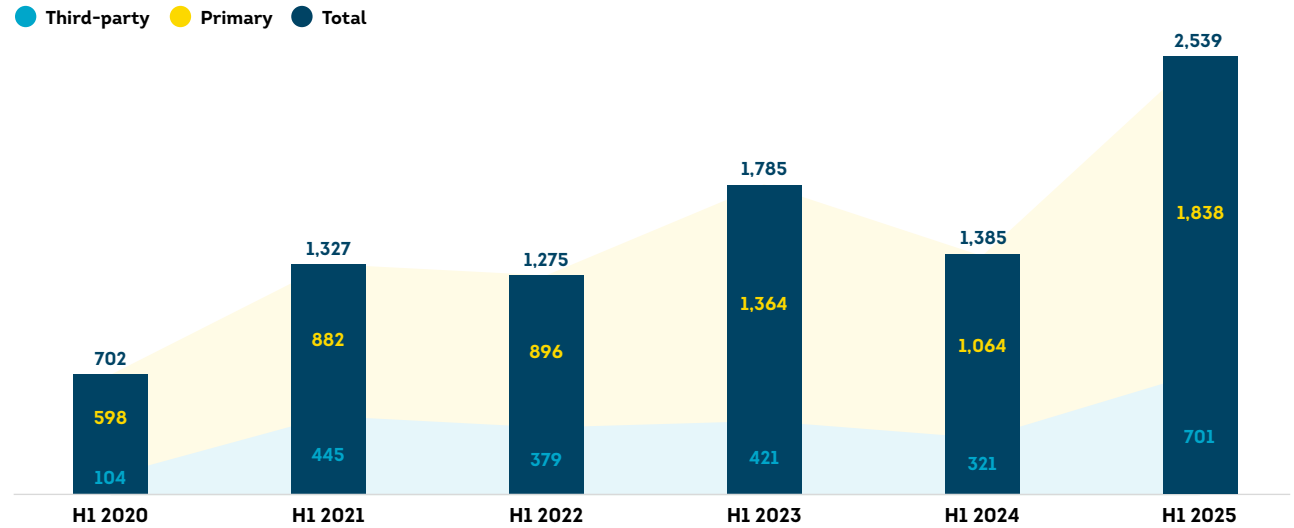
Identity Data Exposure Trends

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.

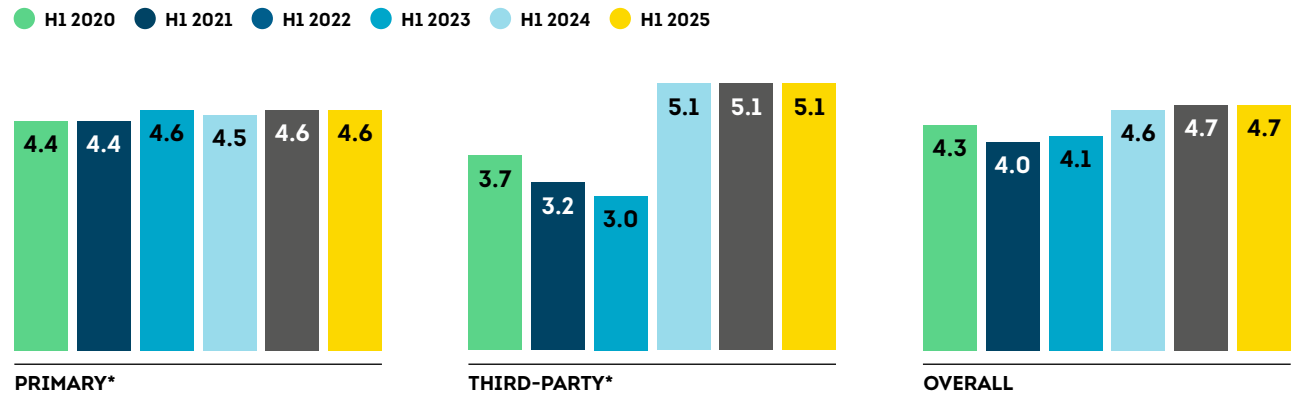
Due to the targeting of high-risk credentials like Social Security numbers, average breach severity (the ability of a breach to enable identity fraud) as measured by TransUnion TruEmpower™ Breach Risk Score (BRS) – a leading indicator of future fraud – remained at the highest level in the period examined.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

US Data Breach Volume



Source: TransUnion global intelligence network

Average Breach Risk Score for US Data Breaches



Source: TransUnion global intelligence network

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

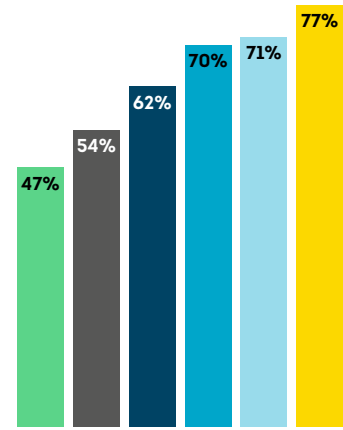
High-value identity credentials prioritised by criminals

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.

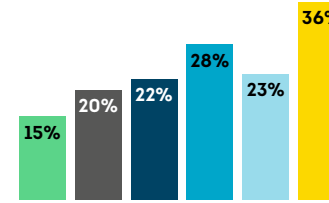
Top 10 Exposed Identity Credentials in US Data Breaches H1 2025

Percentage of credentials exposed in a data breach

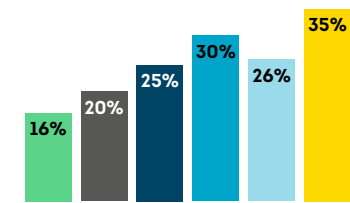
● H1 2020 ● H1 2021 ● H1 2022 ● H1 2023 ● H1 2024 ● H1 2025



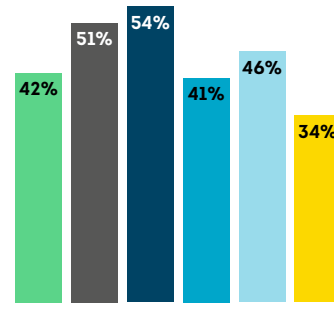
FULL SOCIAL SECURITY NUMBER



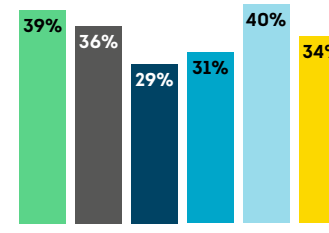
CHECKING OR SAVINGS ACCOUNT NUMBER



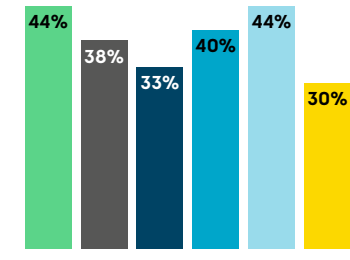
DRIVER'S LICENSE OR OTHER STATE ID



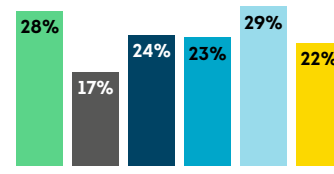
DATE OF BIRTH



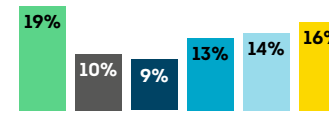
MEDICAL HISTORY



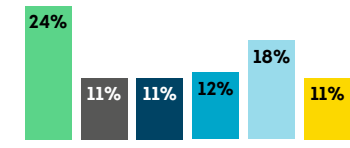
HOME ADDRESS



HEALTHCARE INSURANCE ACCOUNT NUMBER



FULL CREDIT OR DEBIT CARD NUMBER



HEALTHCARE PROVIDER ACCOUNT NUMBER

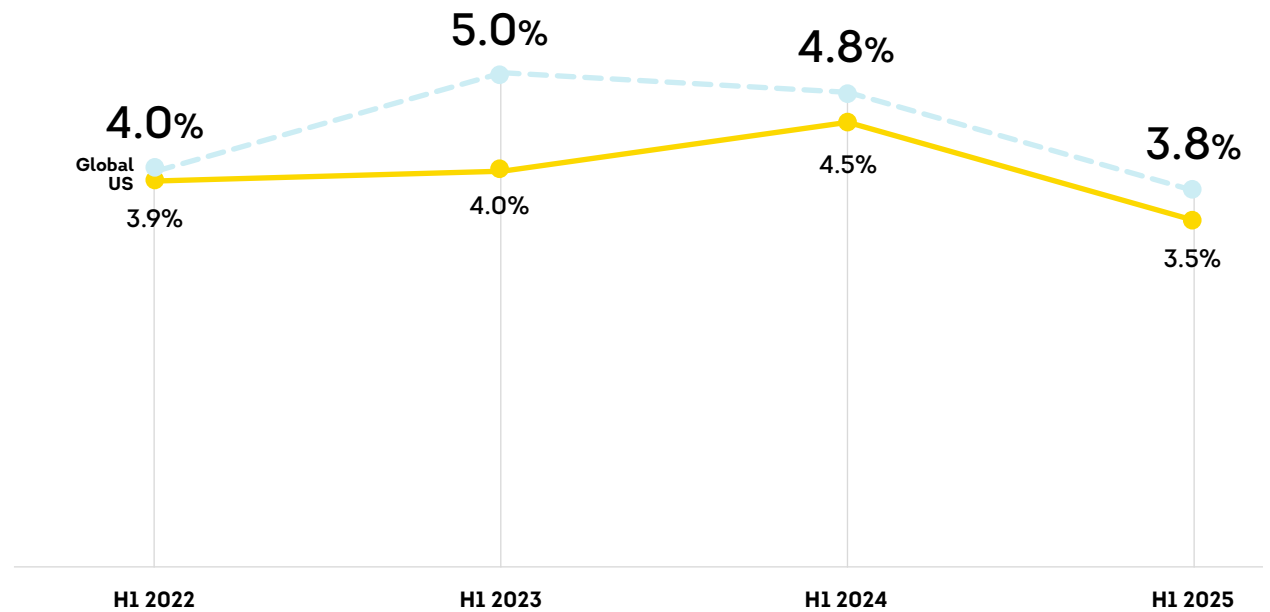
Source: TransUnion global intelligence network

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 organisations 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 organisation.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

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 organisations 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

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%

Financial services

H1 2025

3.4%

H1 2024-H1 2025

-18%

Logistics

H1 2025

1.9%

H1 2024-H1 2025

-70%

Communities

(online dating, forums, etc.)

H1 2025

13.7%

H1 2024-H1 2025

+64%

Retail

H1 2025

3.5%

H1 2024-H1 2025

-46%

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

Call Centre Fraud Trends

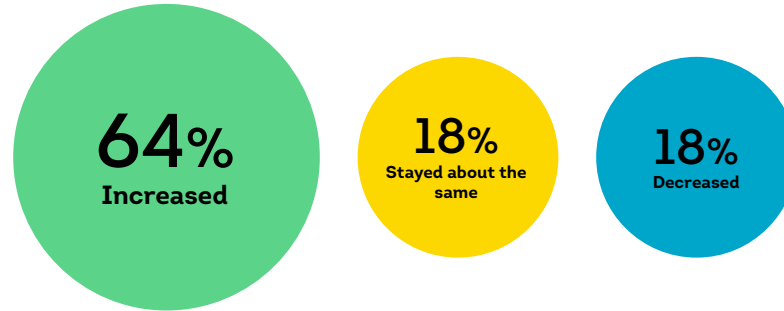
Inbound calls are risky because of the vital role call centres play in the customer experience – representing a high-trust touchpoint for consumers. Among US business leaders surveyed, 64% indicated fraudsters increased their attacks on call centres in the past year, up from 44% from 2024. More than 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.

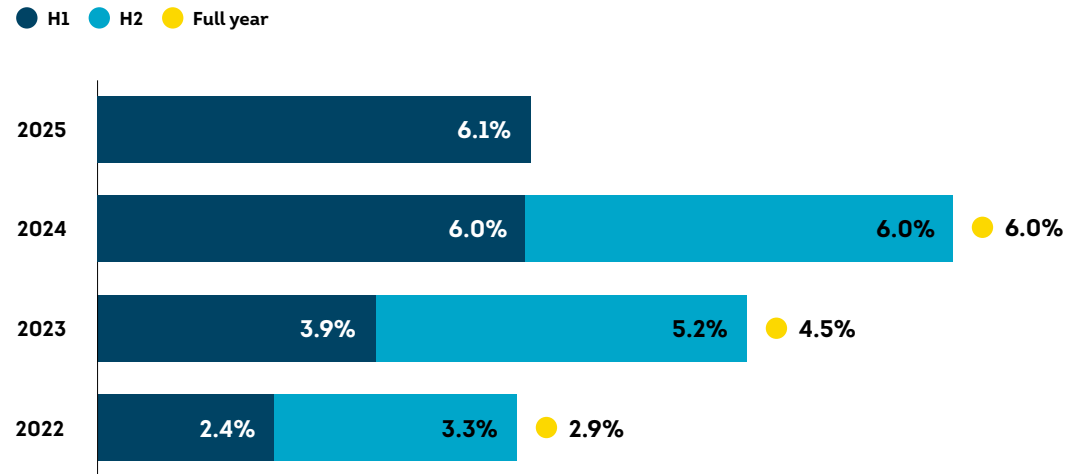
Increased Frequency of Call Centre Fraud Attacks

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

High-Risk Calls Into Call Centres



Source: TransUnion global intelligence network. See page 69 for further information.

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

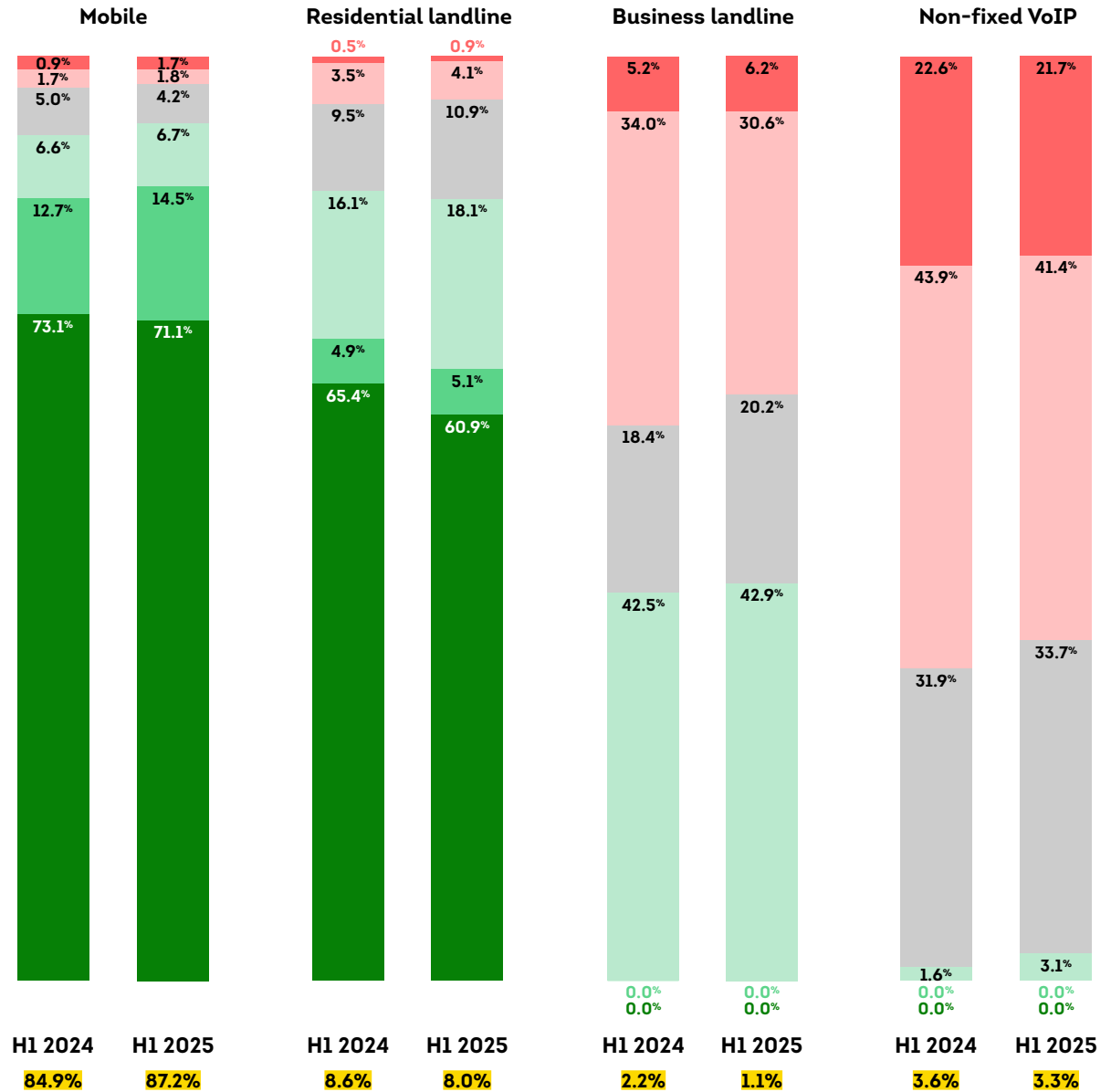
TransUnion documented the vast majority (87.2%) of calls received by its US call centre customers in H1 2025 were from mobile phones, and these calls are getting riskier. While just 3.5% of mobile calls were identified as being the highest risk for fraud, that's a 35% increase from 2.6% in H1 2024. The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

● >500 ● 400 ● 300 ● 200 ● 100 ● 0 ● 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

Risky identities impact all stages of the consumer lifecycle

Not every digital customer interaction presents the same risk to organisations. 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

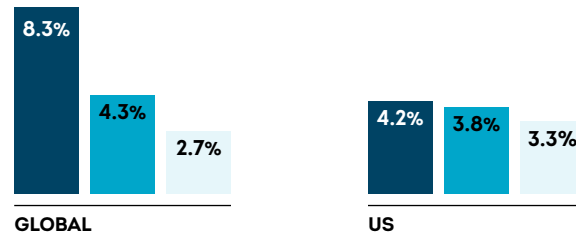
Account login: Login and failed login events

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

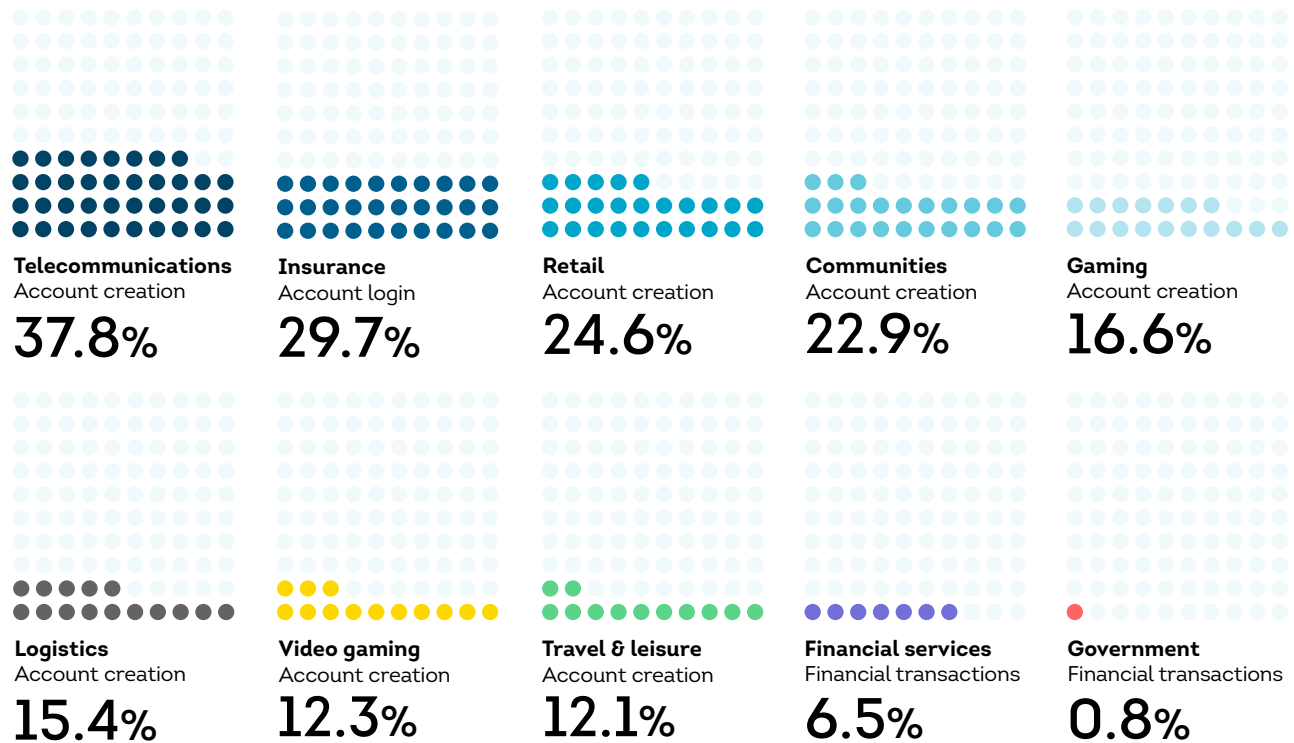
- Account creation
- Account login
- Financial transactions



Source: TransUnion global intelligence network

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

Synthetic identity lending exposure illustrated new account origination risk

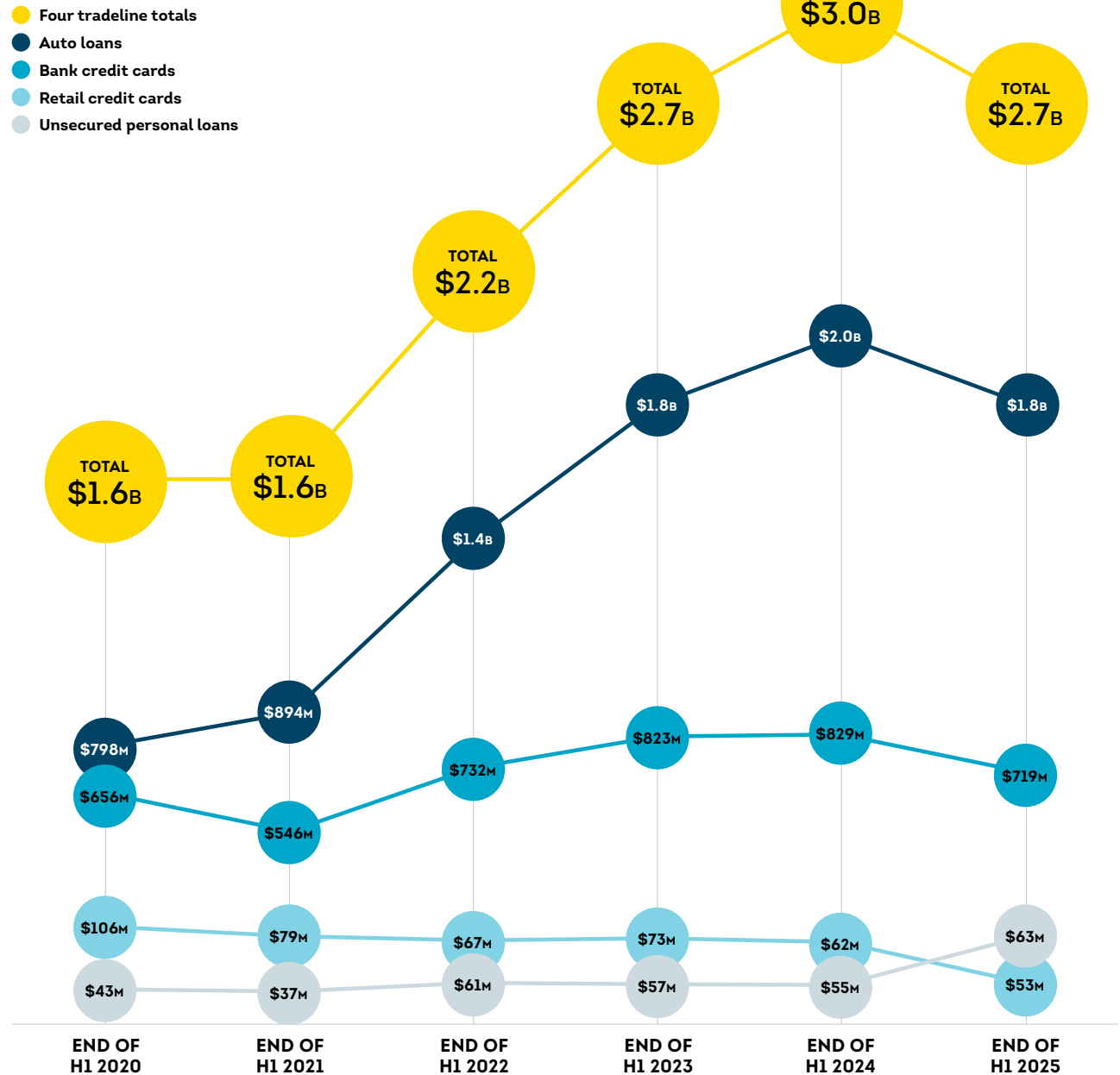
With a wealth of stolen identity credentials combined with GenAI, synthetic identity fraud is a persistent threat. Nearly a quarter (24%) of US business leaders surveyed by TransUnion stated synthetic identity fraud was the leading source of fraud losses for their organisations.

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



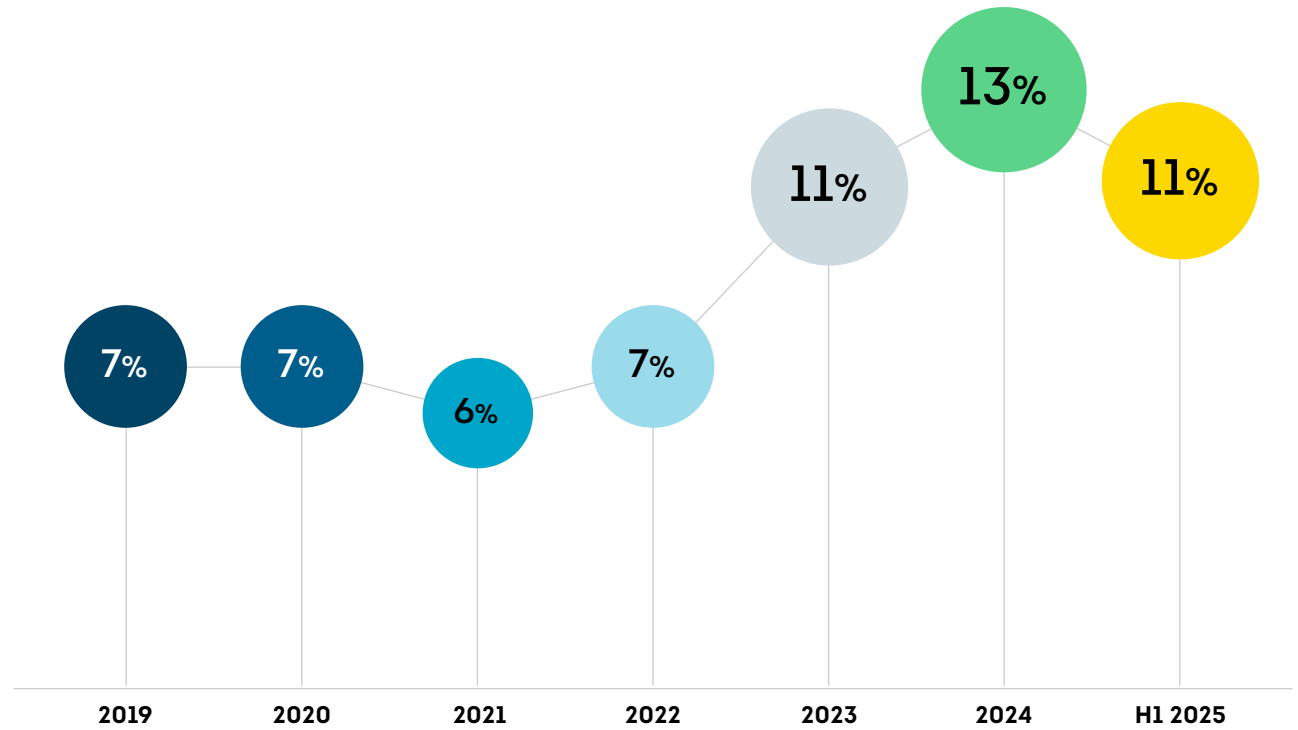
Source: TransUnion global intelligence network

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 unauthorised transactions on a consumer's legitimate credit account.

Consumers in the US (or their authorised 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

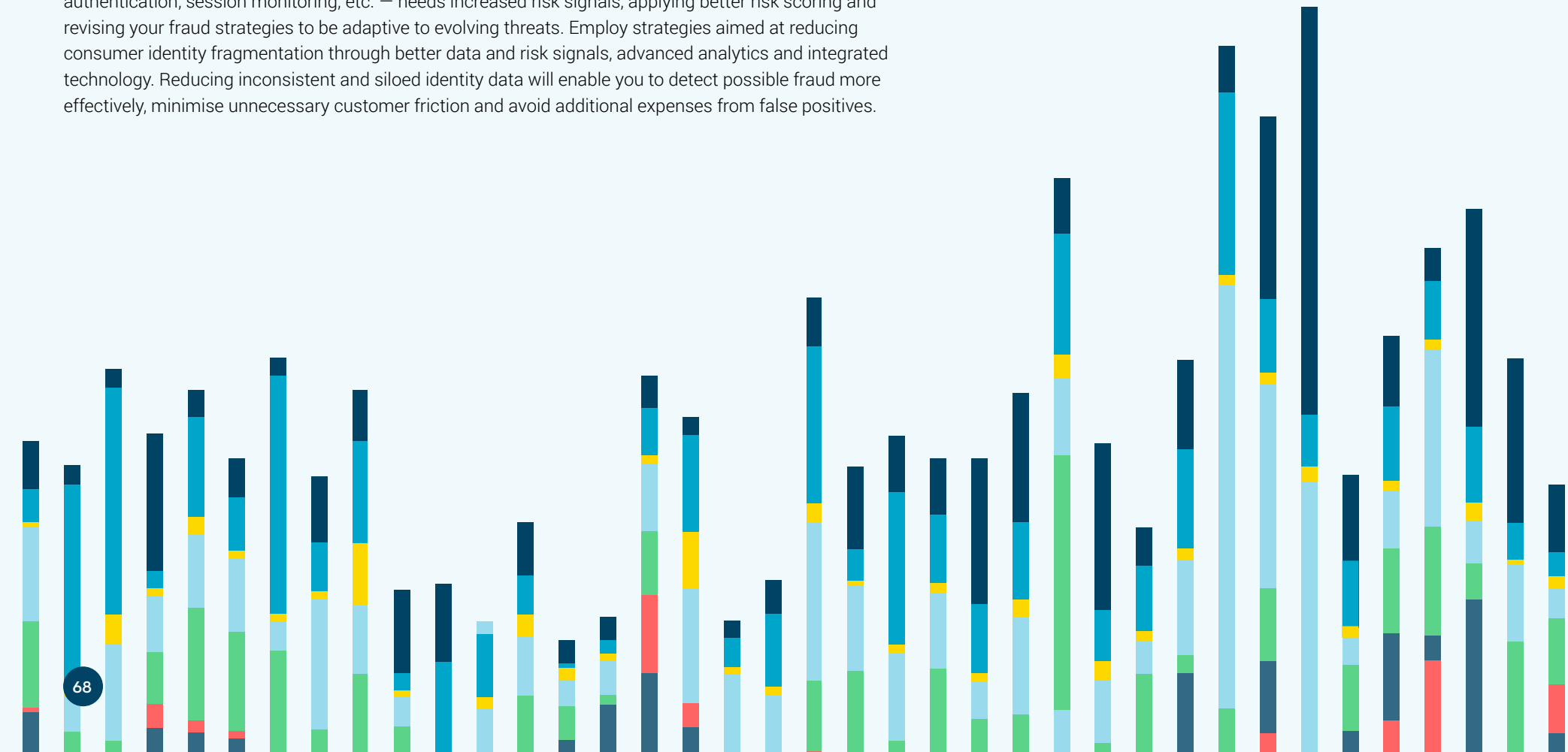


Source: TransUnion global intelligence network

Conclusion

No matter where you are in the world, rising fraud risk and monetary losses are growing concerns for organisations of all sizes and in all industries. For the remainder of 2025 and beyond, threats for consumers and organisations alike will continue as serious data breaches and scams lead to more compromised identities and credentials. Protecting your organisation and customers is non-negotiable. You must assume a security posture that all identity data and credentials presented to your organisation 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 prioritise 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, minimise 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.

transunion.co.uk/solution/truvalidate
