TransUnion

H2 2025 UPDATE: TOP FRAUD TRENDS

DIGITAL IDENTITY RISK ACCELERATES FRAUD LOSSES

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

Executive Summary

Fraud is evolving fast and fraud-fighting teams are struggling to keep pace. A never-ending supply of compromised identity data threatens to overwhelm fraud detection systems — enabling bad actors to attack every customer touchpoint with ease. This was the sobering backdrop for the first half of 2025 fraud trends. Increased risk at new account opening from synthetic, stolen and altered identities is exposing your 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 24 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

TransUnion

Anatomy of Digital Identity Risk

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

Over the past year, we've seen this supply chain become very 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

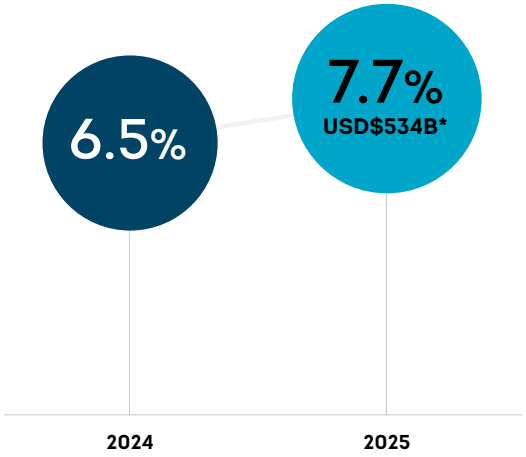
The cost of fraud rose globally

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

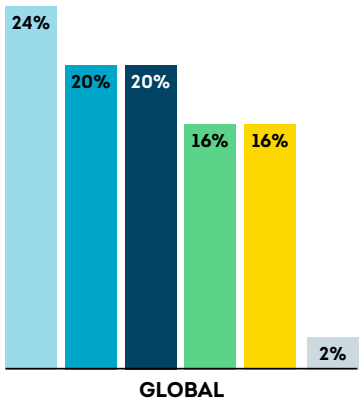
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding amount total among those surveyed globally



*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



- **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**

Source: TransUnion business survey

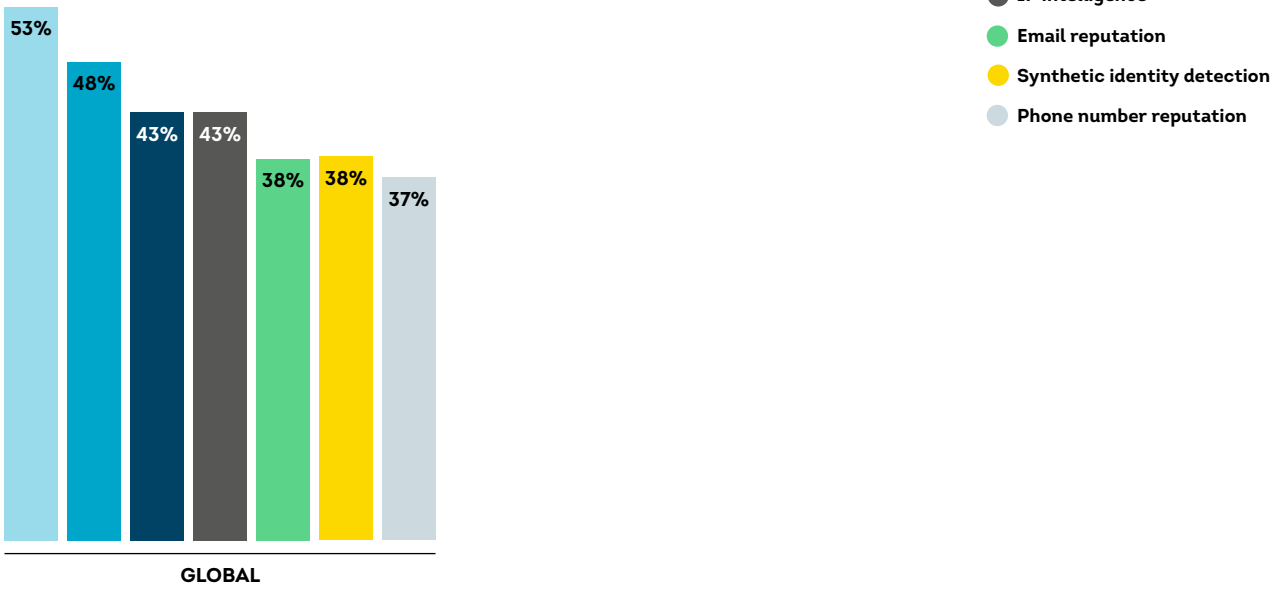
TransUnion

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.



Source: TransUnion business survey

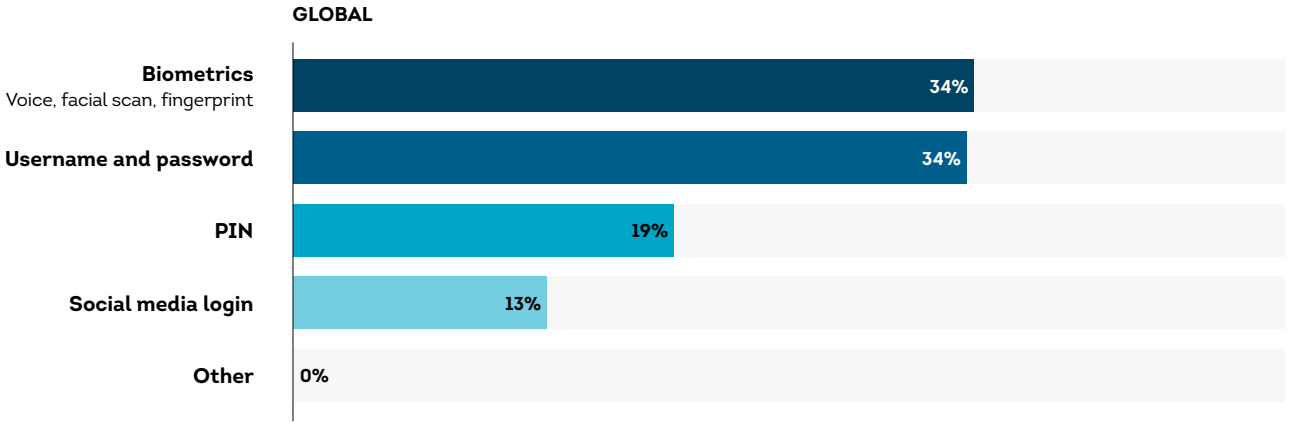
TransUnion

Dependence on passwords for customer authentication fading

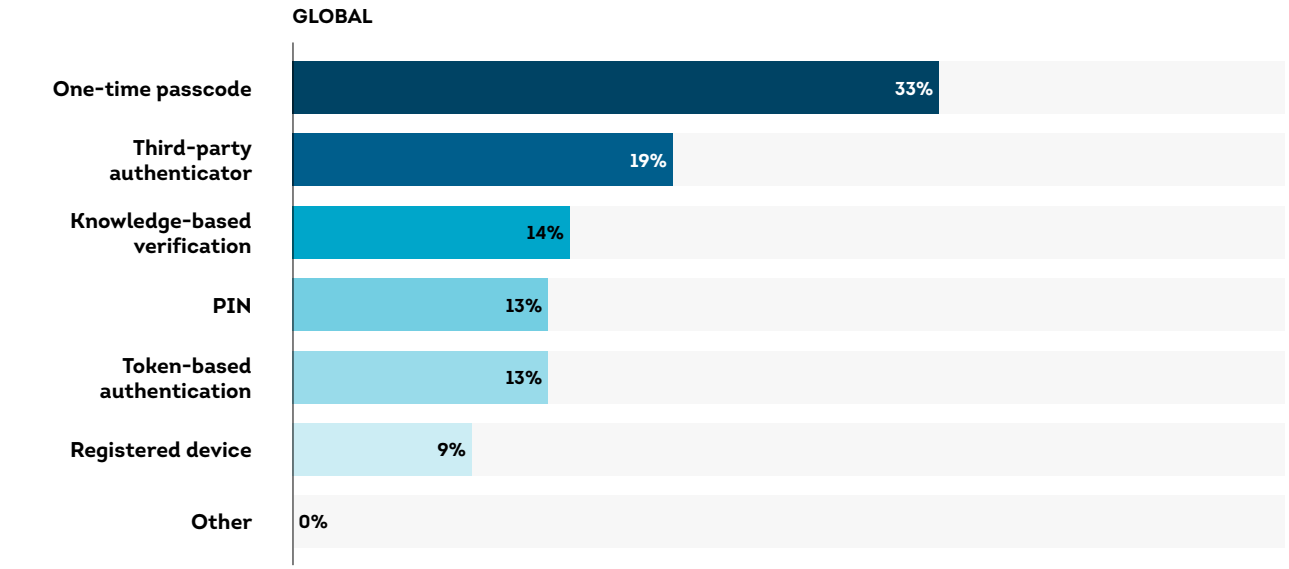
User accounts remain under threat from consumer scams and brand spoofing. Organisations appear to be shifting their approaches to embed a second factor into their authentication programs as standard practice. While more than a third (34%) of business leaders indicated they utilise usernames and passwords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

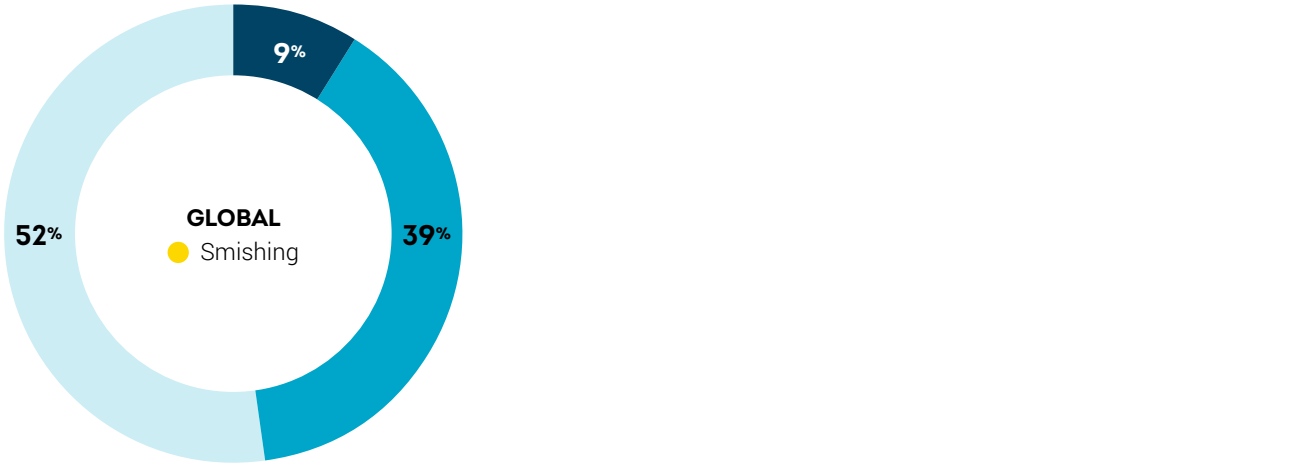
TransUnion

Consumers reported scams as most frequently experienced fraud

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

Consumers Targeted With Fraud

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



Source: TransUnion consumer survey

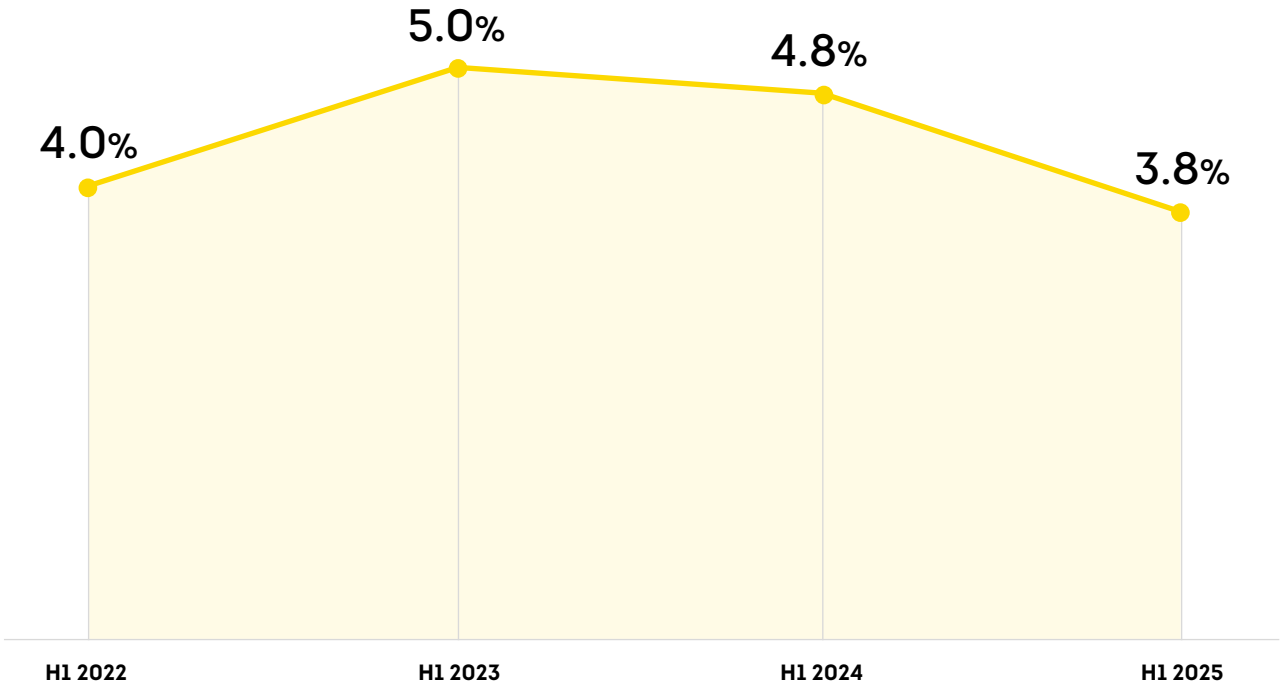
TransUnion

Digital Fraud Trends

Digital fraud rates fell for the second year in a row

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

Rate of Suspected Digital Fraud Globally

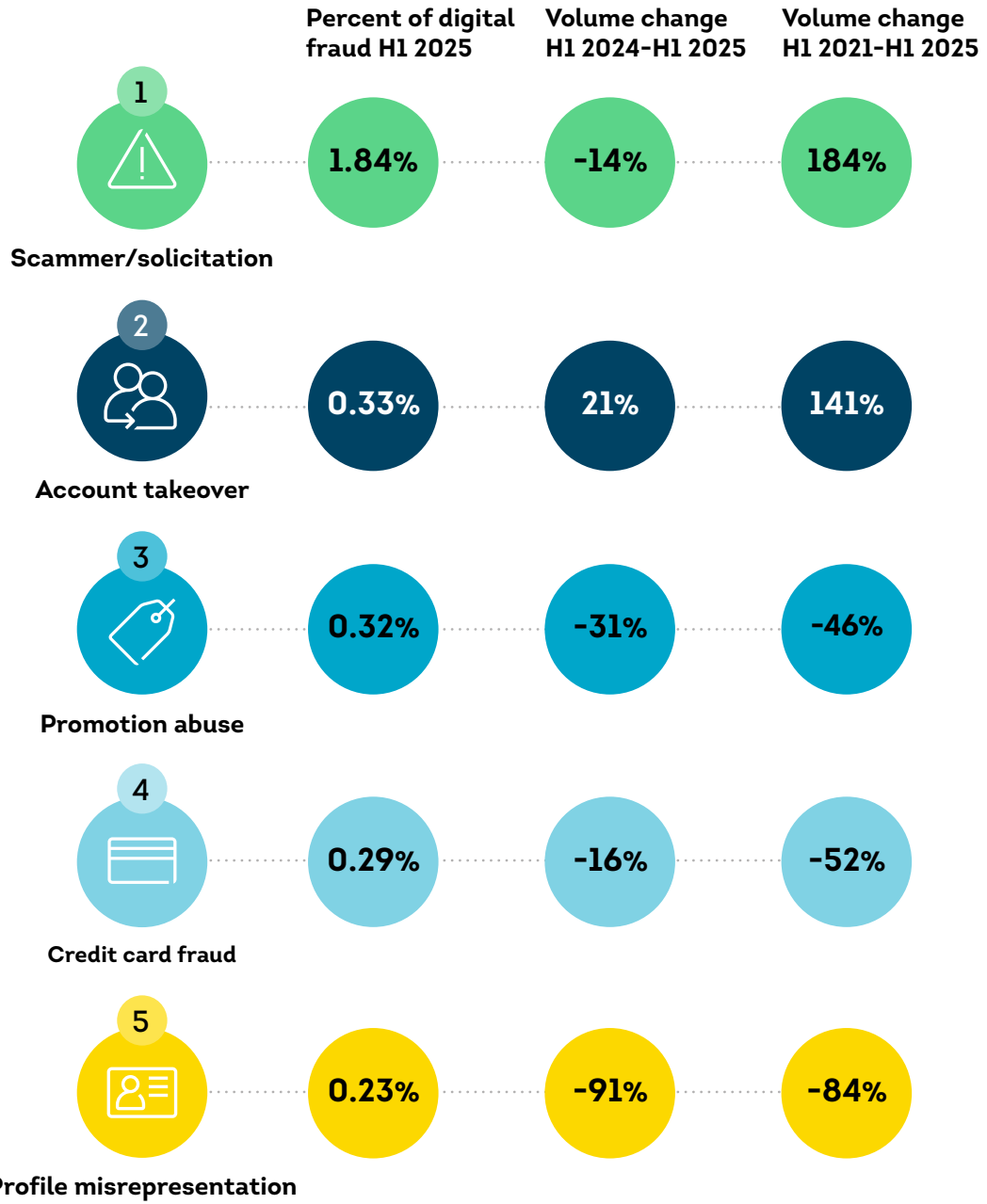


Source: TransUnion global intelligence network

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

TransUnion

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

The video gaming industry, which includes online and mobile games, experienced the largest percentage (13.5%) of suspected digital fraud attempts globally among sectors 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**

Video gaming

H1 2025
13.5%
Scammer/solicitation

H1 2024-H1 2025
+3%

Communities
(online dating, forums, etc.)

H1 2025
8.3%
Profile misrepresentation

H1 2024-H1 2025
-33%

Gaming
(online sports betting, poker, etc.)

H1 2025
6.8%
Promotion abuse

H1 2024-H1 2025
+24%

Telecommunications

H1 2025
4.4%
Scammer/solicitation

H1 2024-H1 2025
+74%

Financial services

H1 2025
3.3%
Account takeover

H1 2024-H1 2025
-20%

Retail

H1 2025
2.6%
Credit card fraud

H1 2024-H1 2025
-64%

Government

H1 2025
2.3%
Credit card fraud

H1 2024-H1 2025
+52%

Logistics

H1 2025
2.3%
Shipping fraud

H1 2024-H1 2025
-42%

Insurance

H1 2025
1.2%
First-party application fraud

H1 2024-H1 2025
-47%

Travel & leisure

H1 2025
0.2%
Credit card fraud

H1 2024-H1 2025
-56%

Source: TransUnion global intelligence network

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

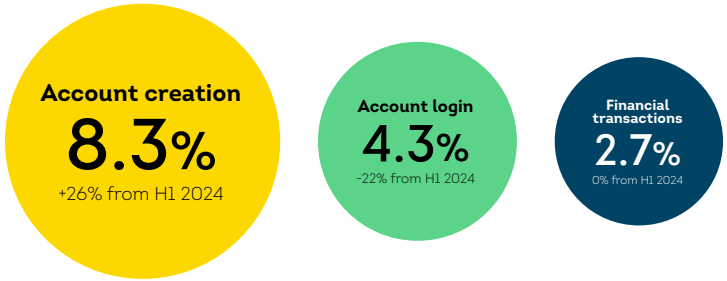
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

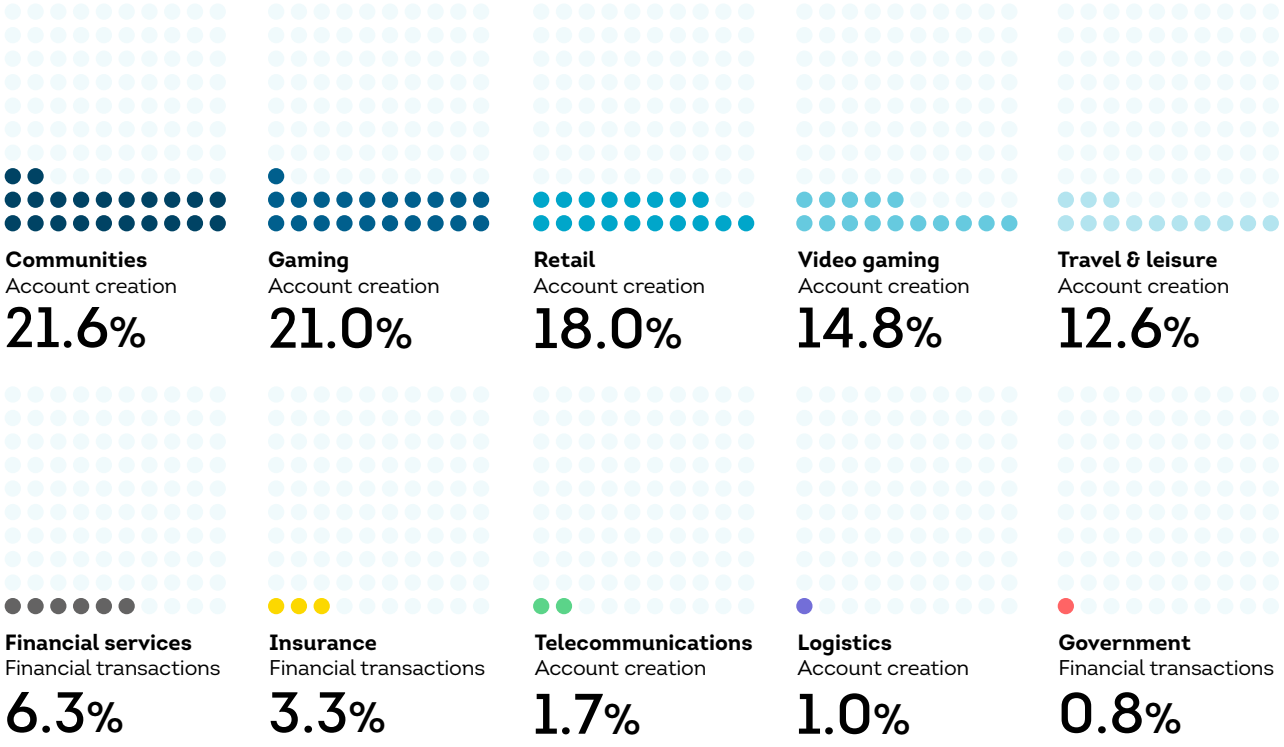
Percentage of each attempted transaction type suspected to be digital fraud globally in H1 2025



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

TransUnion


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

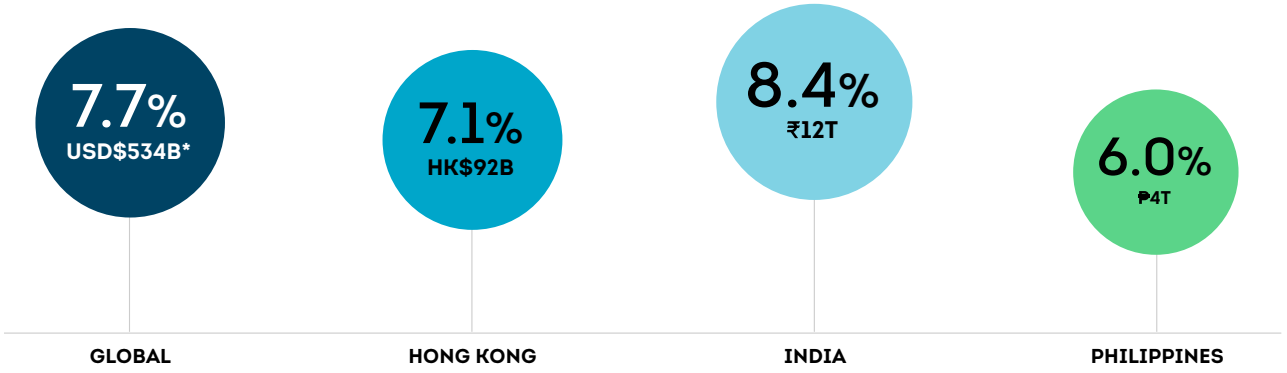
Hong Kong business leaders claim their companies lost the equivalent of 7.1% of their revenues in the past year due to fraud, representing HK$92B among the 200 business leaders surveyed. According to them, the most prominent cause of fraud losses this year was third-party fraud — followed by account 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.

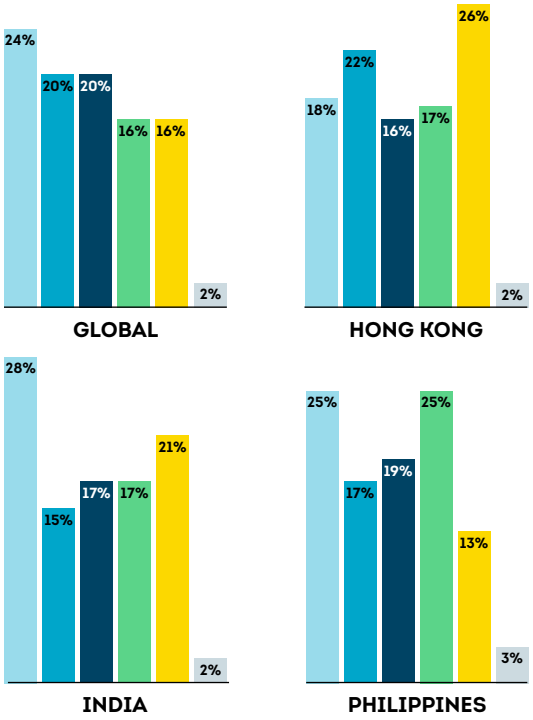
Total Cost of Fraud

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**

Source: TransUnion business survey

TransUnion

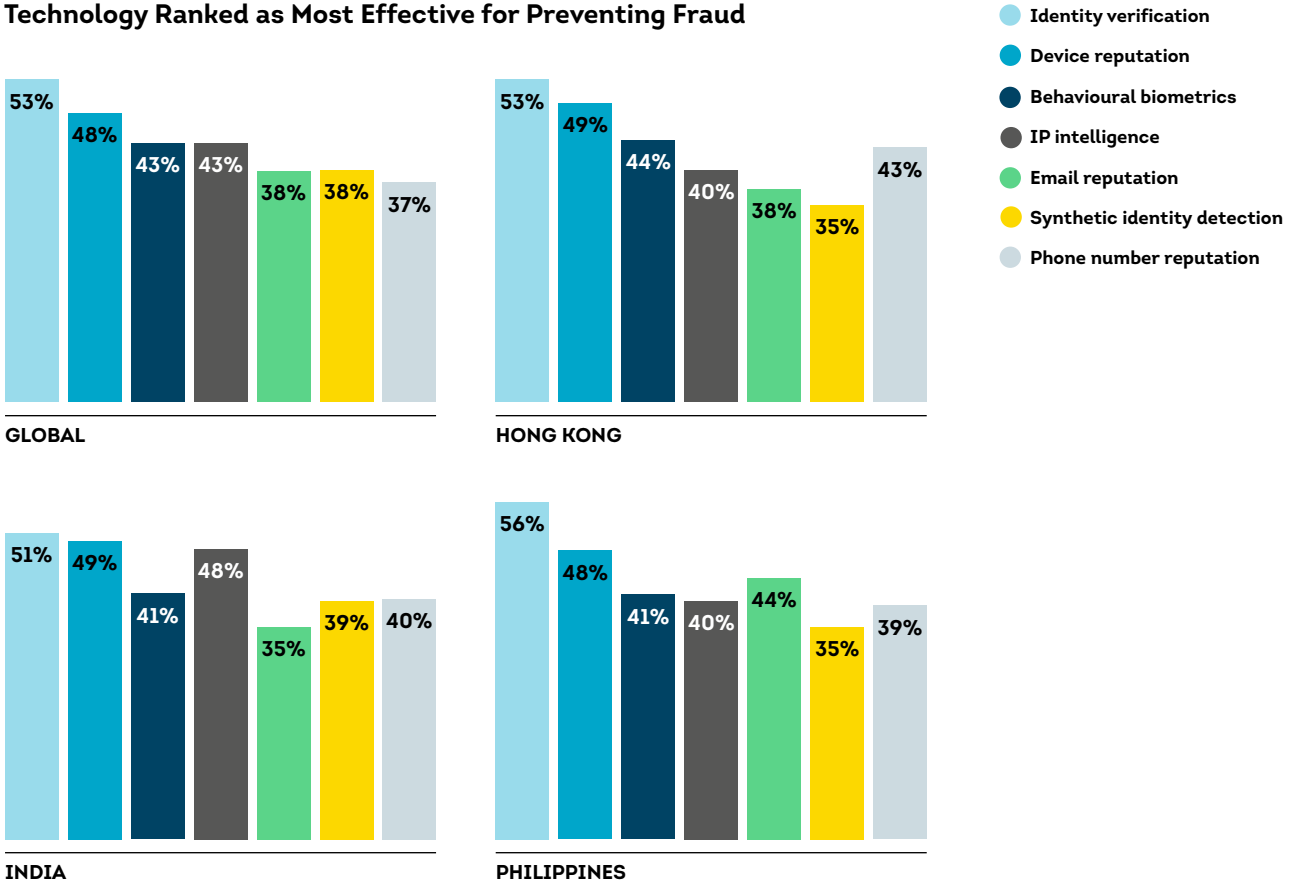
Identity verification seen as most effective across all markets

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



Source: TransUnion business survey

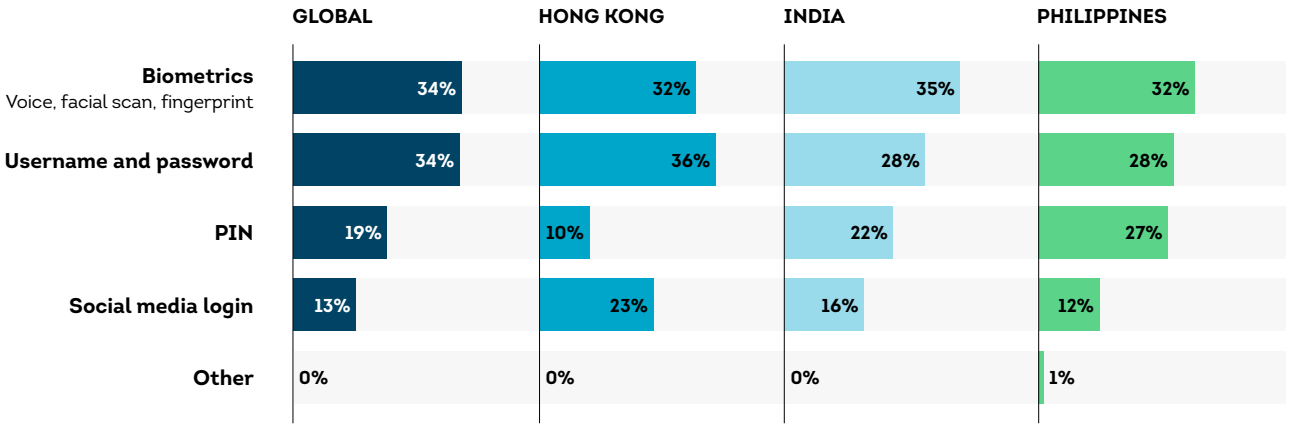
TransUnion

Authentication practices dominated by biometrics

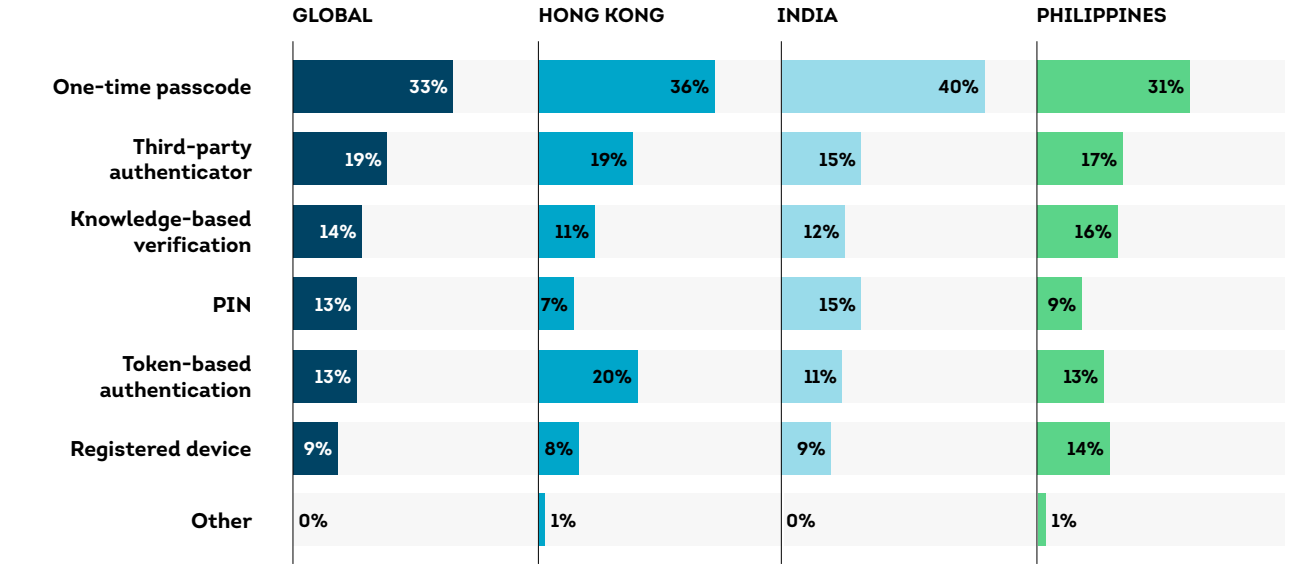
According to business leaders surveyed in Hong Kong, in order to authenticate consumers, they rely most on username/password (36%) — followed by biometrics (32%) and social media login (23%). PIN usage was relatively low (10%). India business leaders reported relying most on biometrics (35%) — followed 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

TransUnion

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

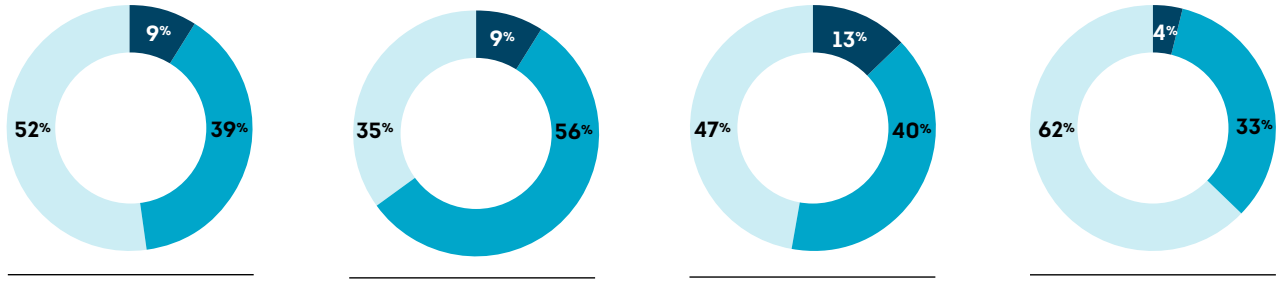
More than half (53%) of consumers reported being targeted by fraud schemes and of those, 13% said they had fallen victim, indicating a high conversion rate from targeting to actual loss. Both numbers are higher than the global average of 48% targeted and 9% fallen victim. The most reported fraud scheme 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

TransUnion

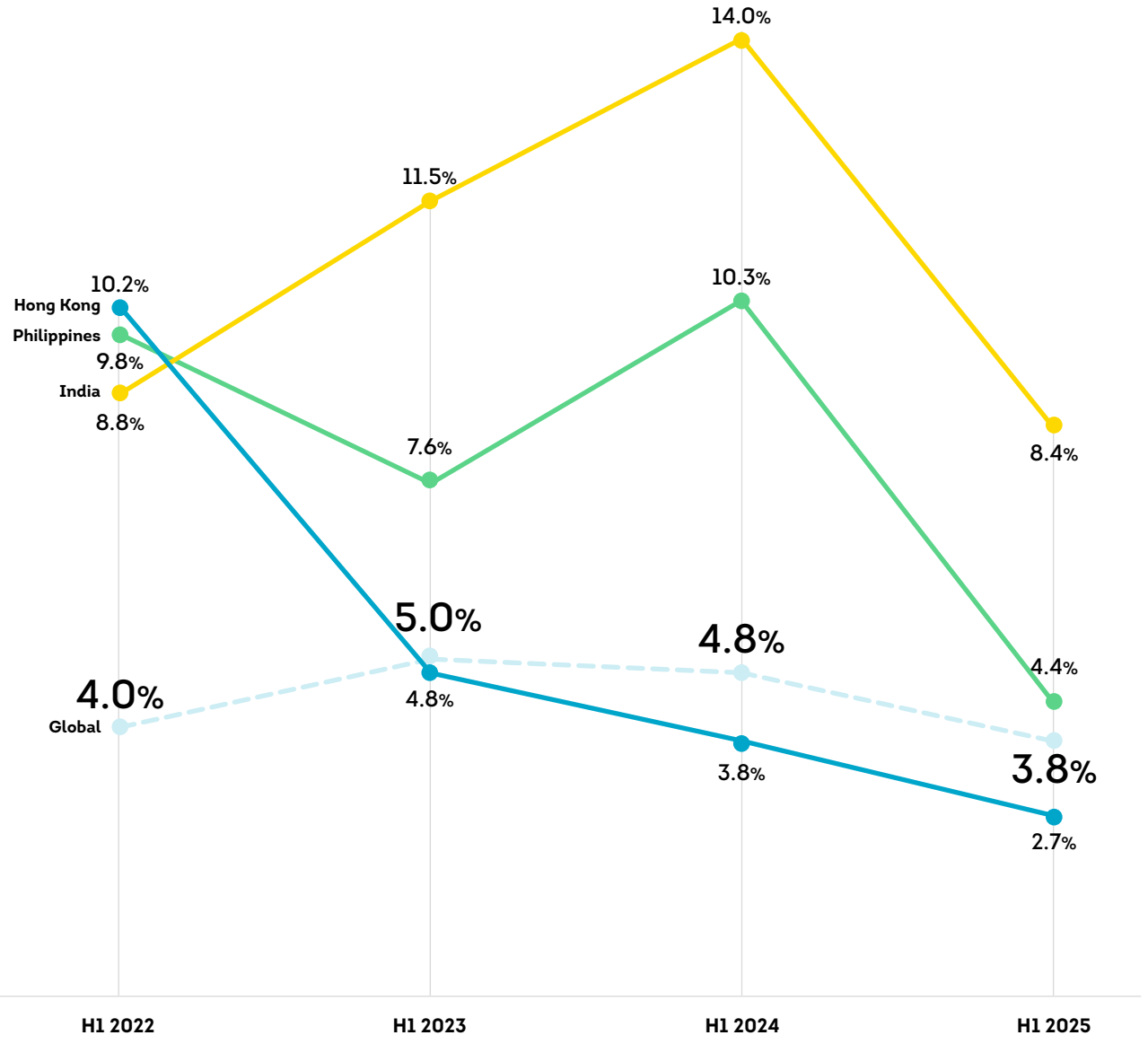
Digital Fraud Trends

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

TransUnion

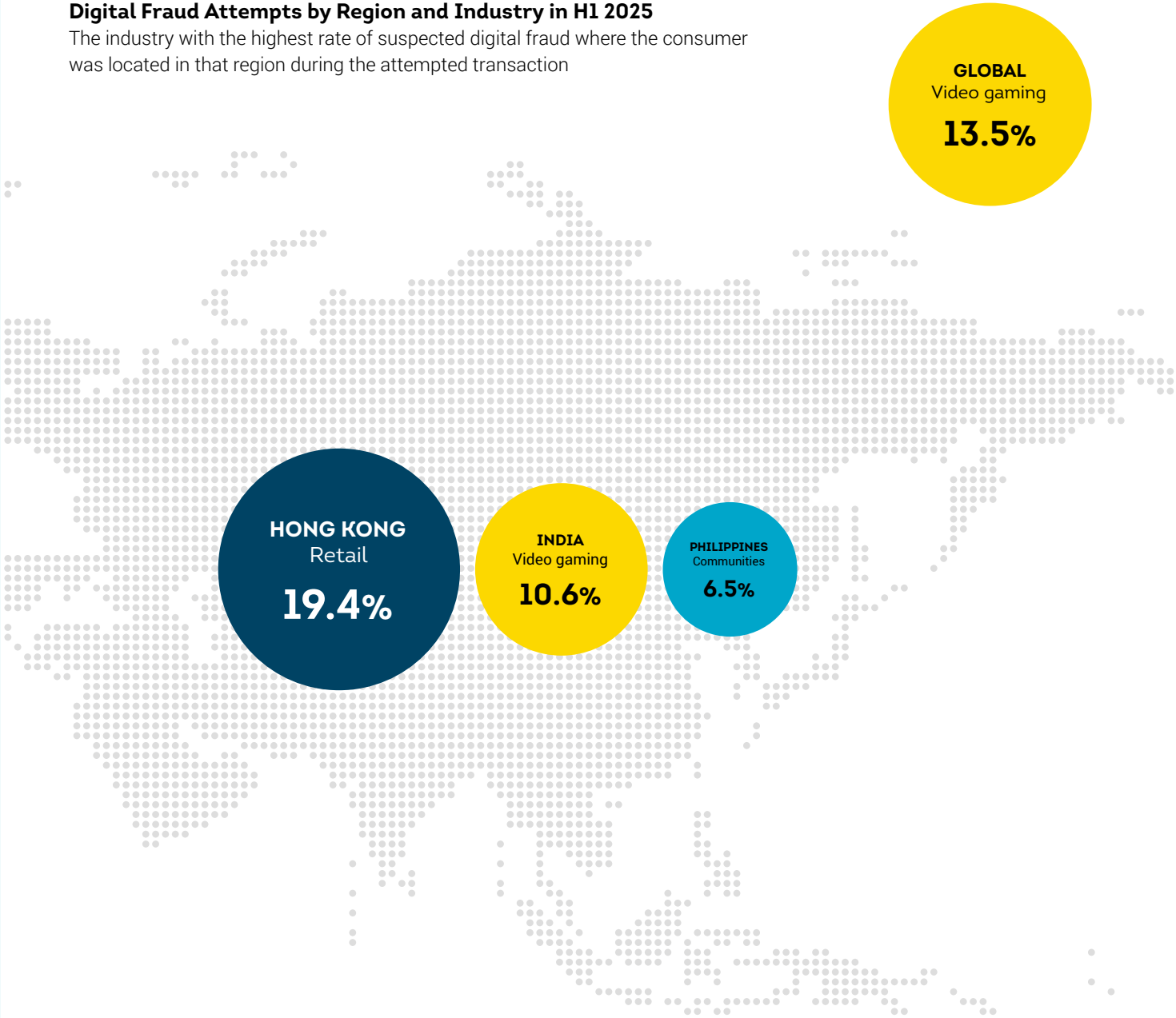
Regional fraud trends vary by industry

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

TransUnion

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

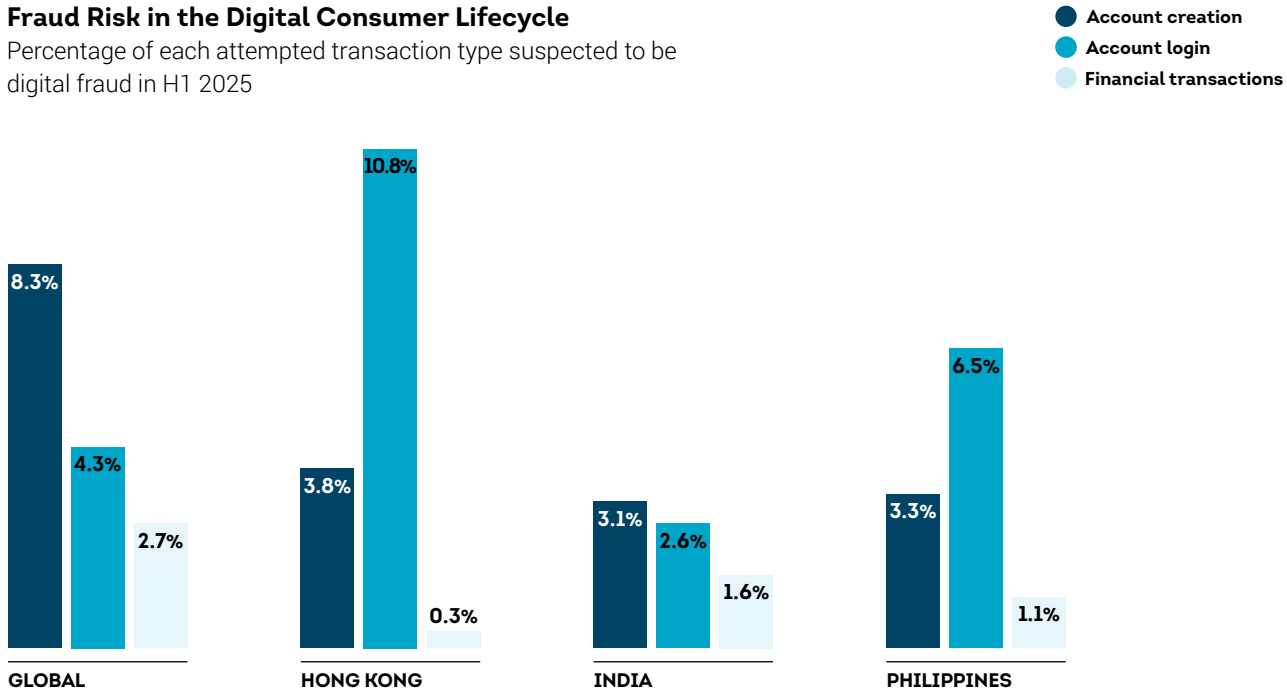
The suspected digital fraud rate in H1 2025 for account login attempts where the consumer was in India when transacting was 2.6%. Fraud during this stage could reflect widespread social engineering, phishing and smishing attacks. For account creation attempts from India, the rate was 3.1%. This shows 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

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.

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.

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.

ABOUT TRANSUNION (NYSE: TRU)

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

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

TransUnion