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 21 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

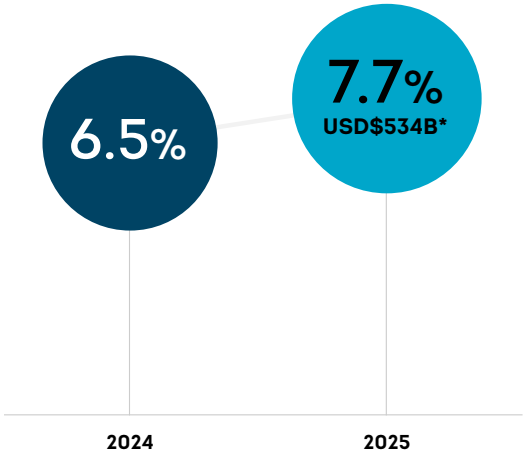
The cost of fraud rose globally

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

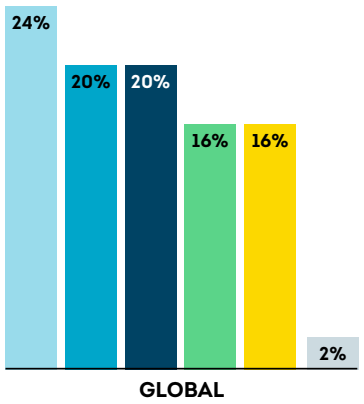
Business leaders stated percent of revenue their companies lost to fraud over the past year and the corresponding amount total among those surveyed globally



*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

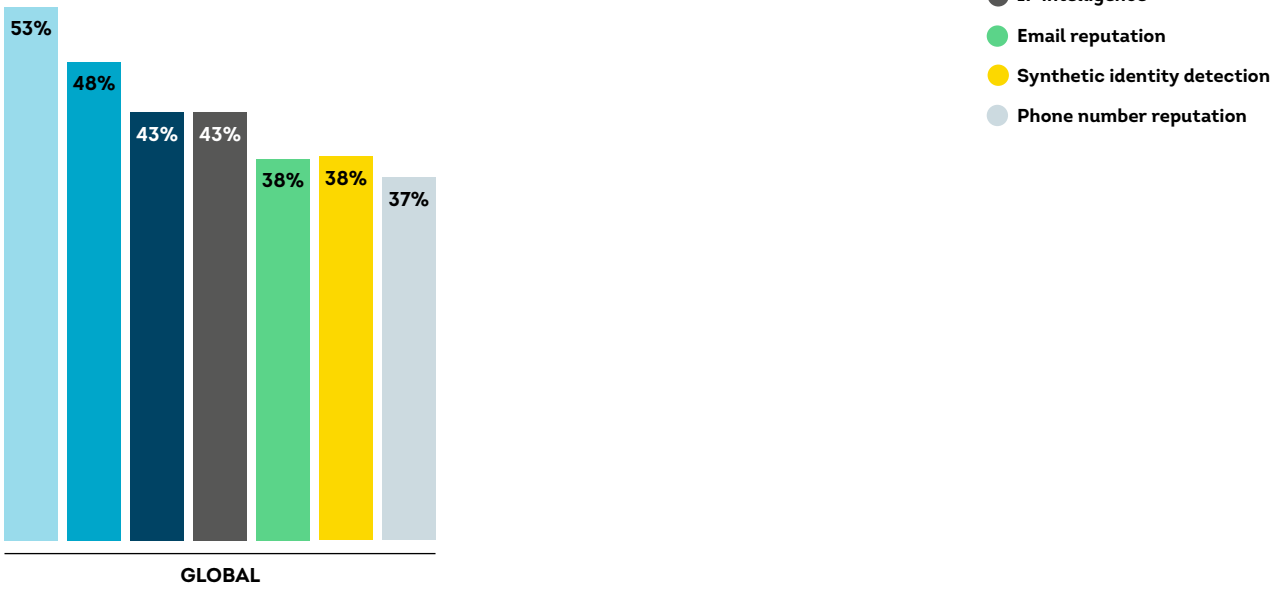
TransUnion

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

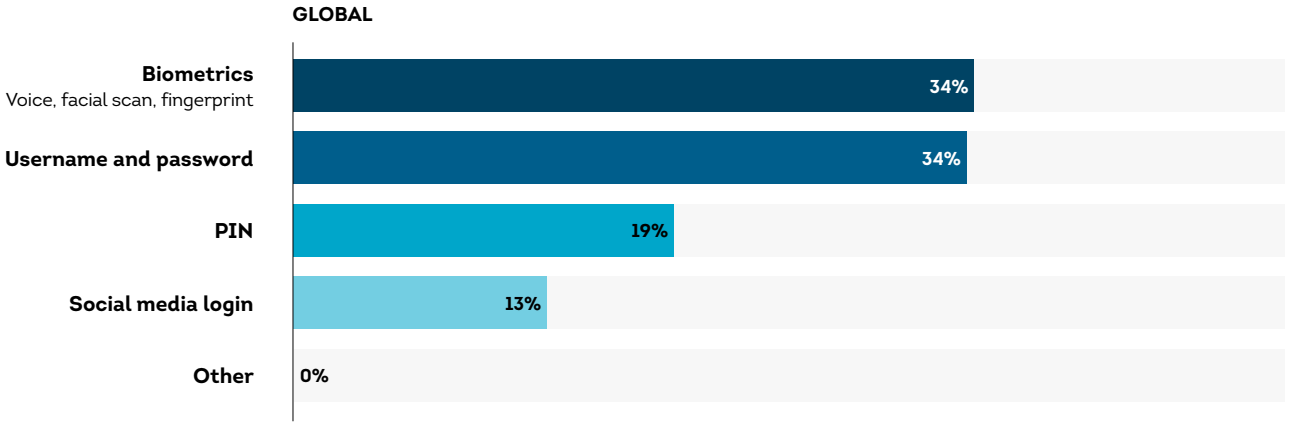
TransUnion

Dependence on passwords for customer authentication fading

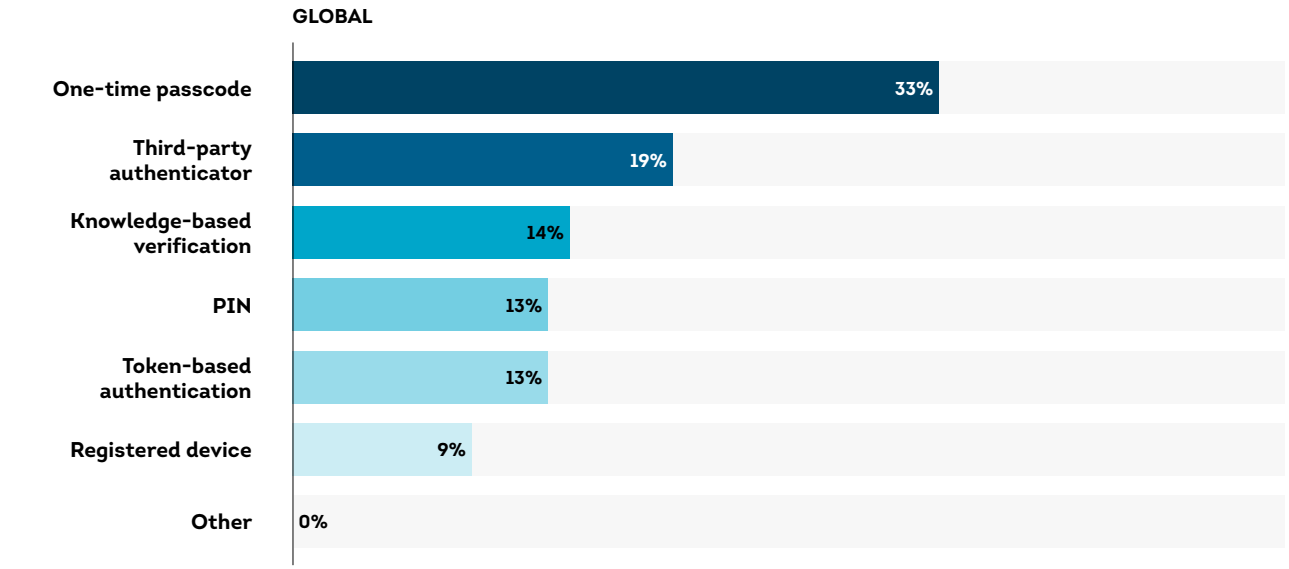
User accounts remain under threat from consumer scams and brand spoofing. Organisations appear to be shifting their approaches to embed a second factor into their authentication programs as standard practice. While more than a third (34%) of business leaders indicated they utilise usernames and passwords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

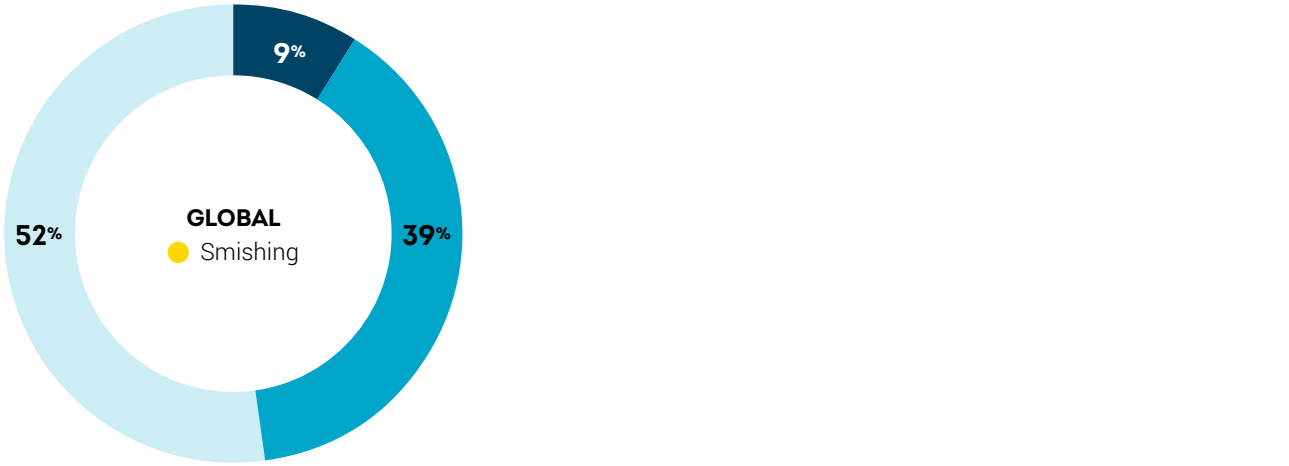
TransUnion

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

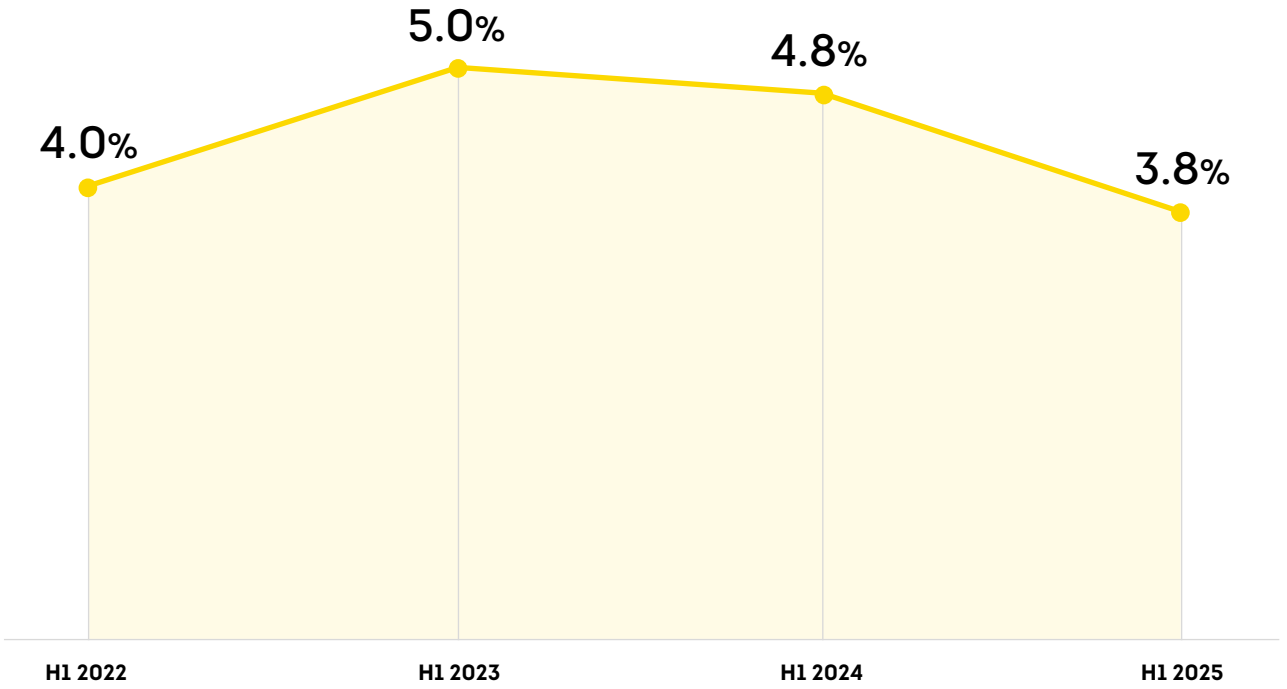
TransUnion

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

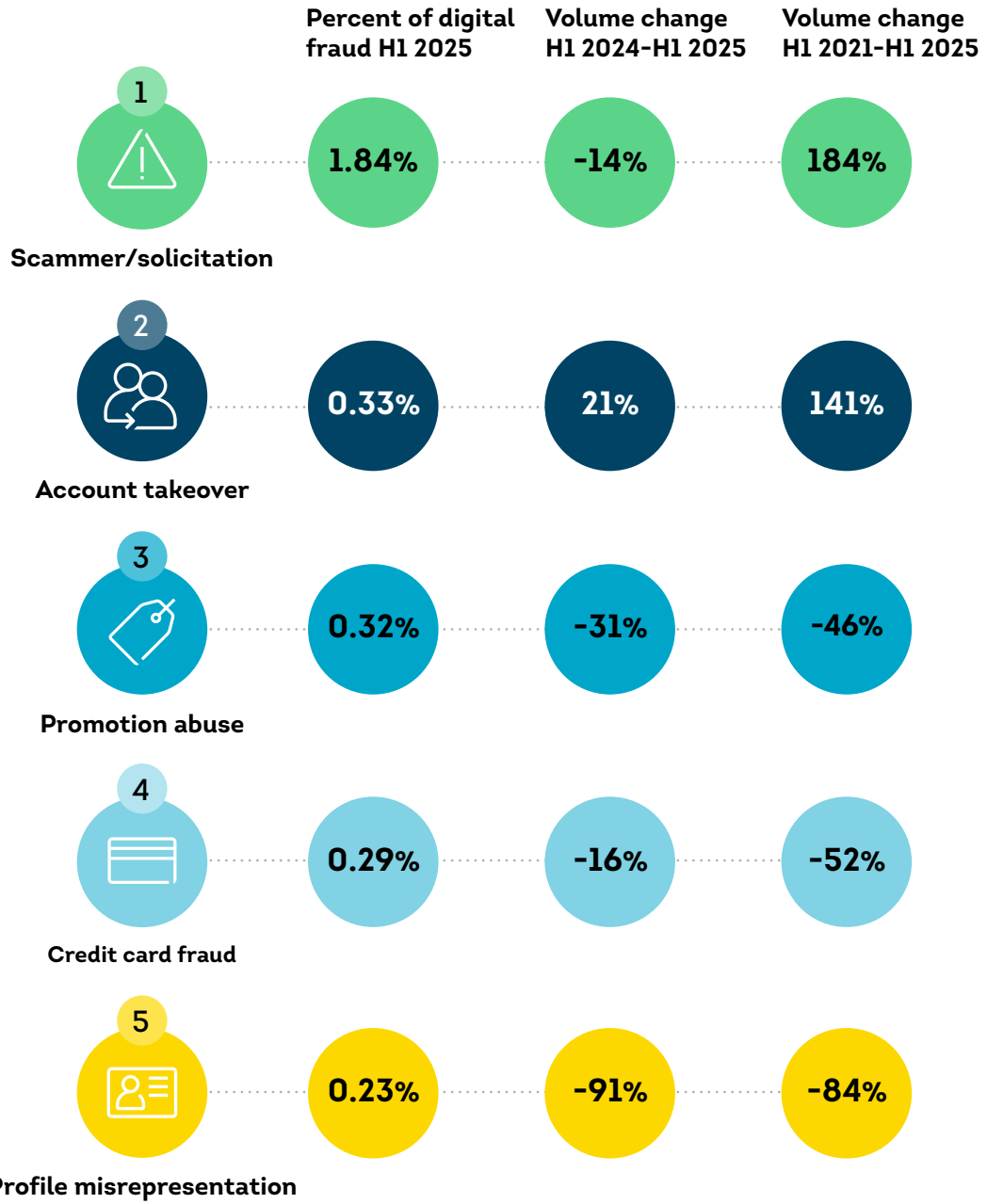


Source: TransUnion global intelligence network

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

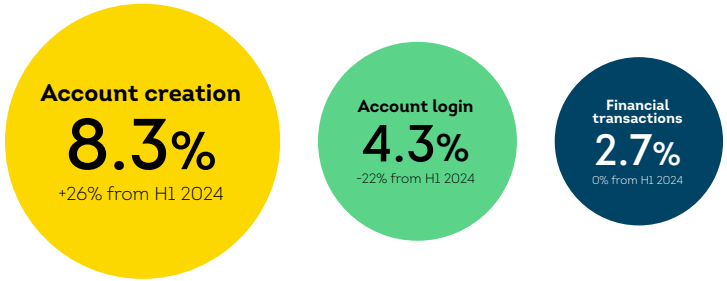
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

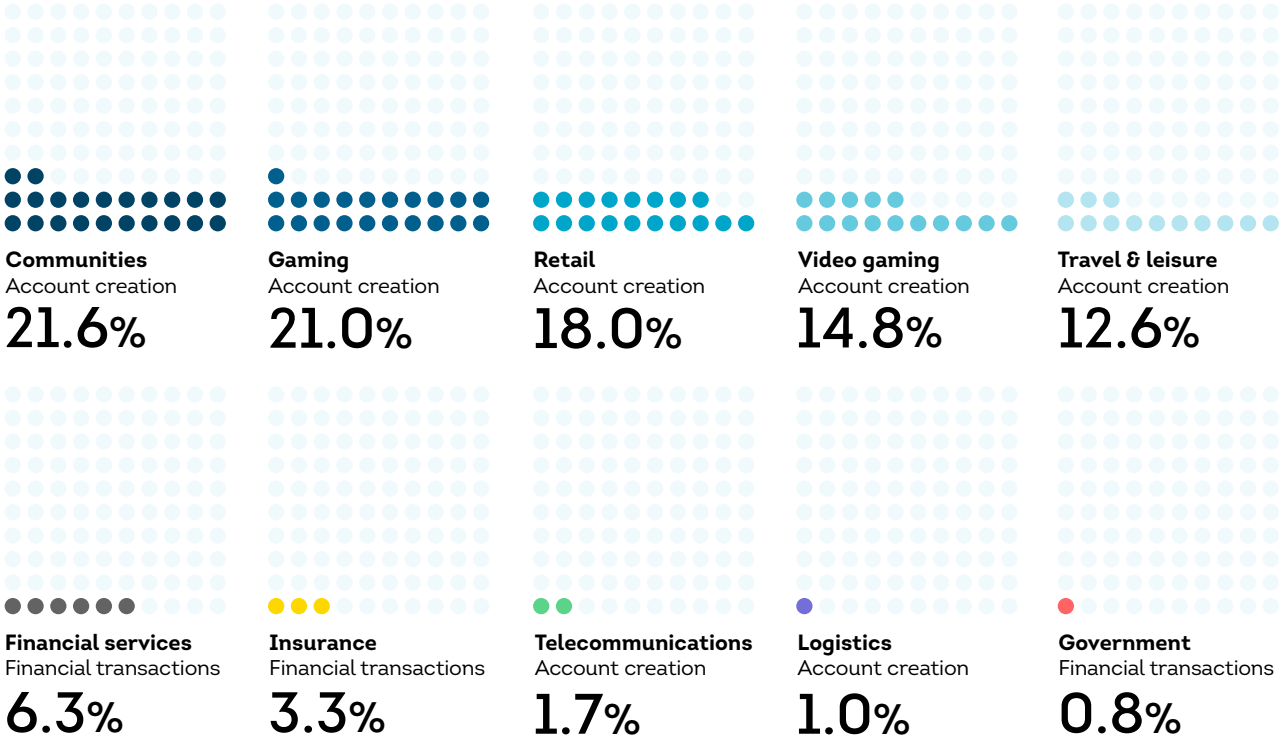
Percentage of each attempted transaction type suspected to be digital fraud globally in H1 2025



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

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

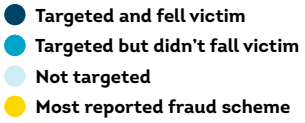
Consumer-reported email, online, phone call and text messaging fraud is widespread across nearly every African country TransUnion recently surveyed. Despite high targeting rates, only between 6% to 13% reported actually falling victim. This suggests education and defences are gaining traction.

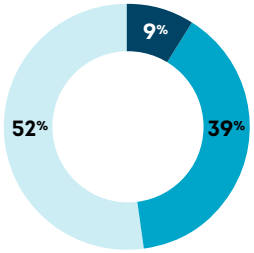
Trends over time show encouraging signs. Kenya's consumer reported fraud victimisation rate dropped from 11% in late last year to 10% in Q2 2025. Namibia also declined during this period. This pattern suggests fraud attempts are common — but more consumers are spotting and stopping them. It's a sign 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.

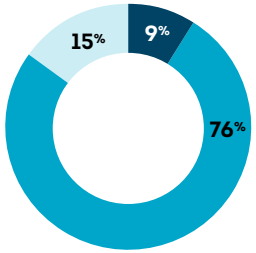
Consumers Targeted With Fraud

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.

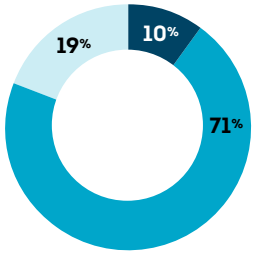




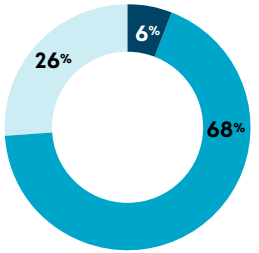
GLOBAL
Smishing



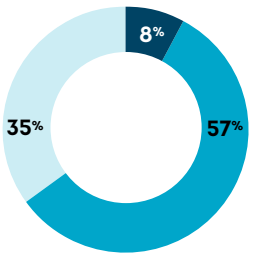
ZAMBIA
Money/gift card



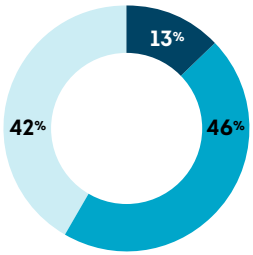
KENYA
Vishing



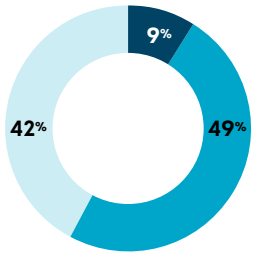
BOTSWANA
Money/gift card



NAMIBIA
Money/gift card



SOUTH AFRICA
Money/gift card



RWANDA
Money/gift card

Source: TransUnion consumer survey

TransUnion

Digital Fraud Trends

Declining suspected digital fraud in African markets

The share of digital transactions flagged as potentially fraudulent among TransUnion fraud solution customers 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.

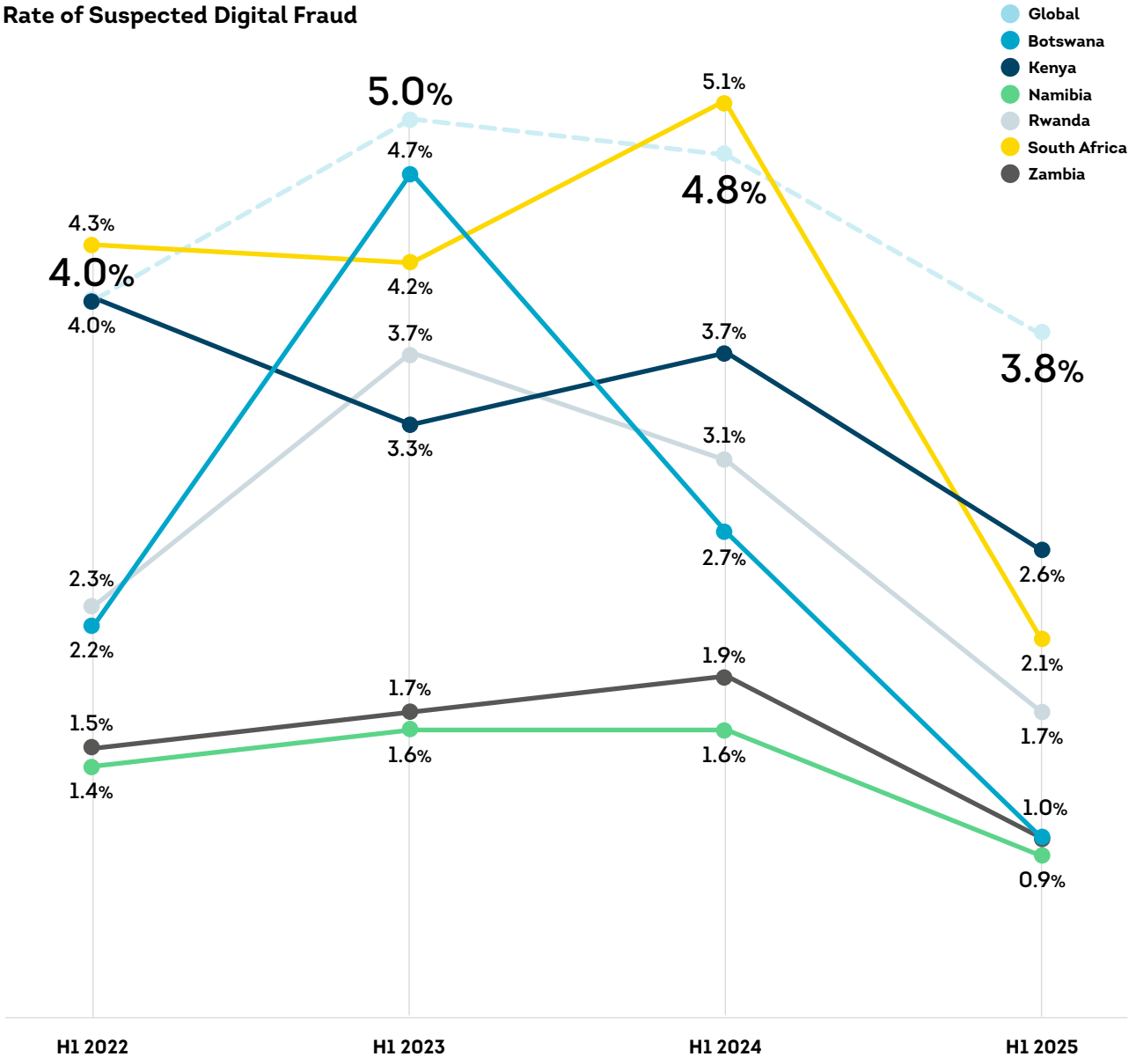
Kenya fell from 4.0% to 2.6% in the same period. This decline reflects the country's leadership in mobile finance and tightening fraud measures.

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

TransUnion

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.

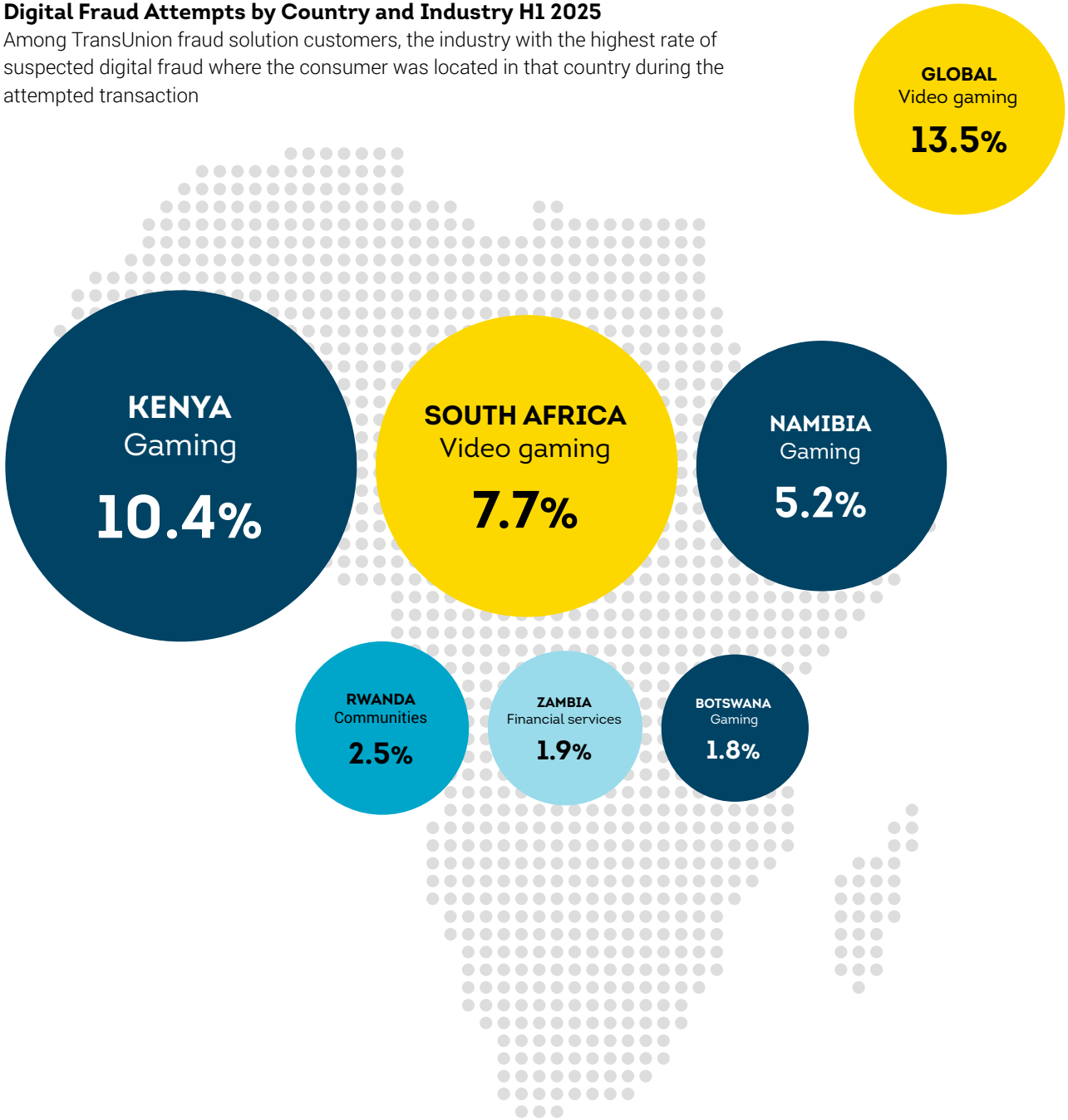
In H1 2025, there was a tendency for both gaming (online sports betting, poker, etc.) and video gaming to attract suspected fraudsters in Africa. Of transactions where the consumer was in Kenya, Namibia and Botswana, the rate of suspected digital fraud in gaming was the highest among those industries 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

Among TransUnion fraud solution customers, 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

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

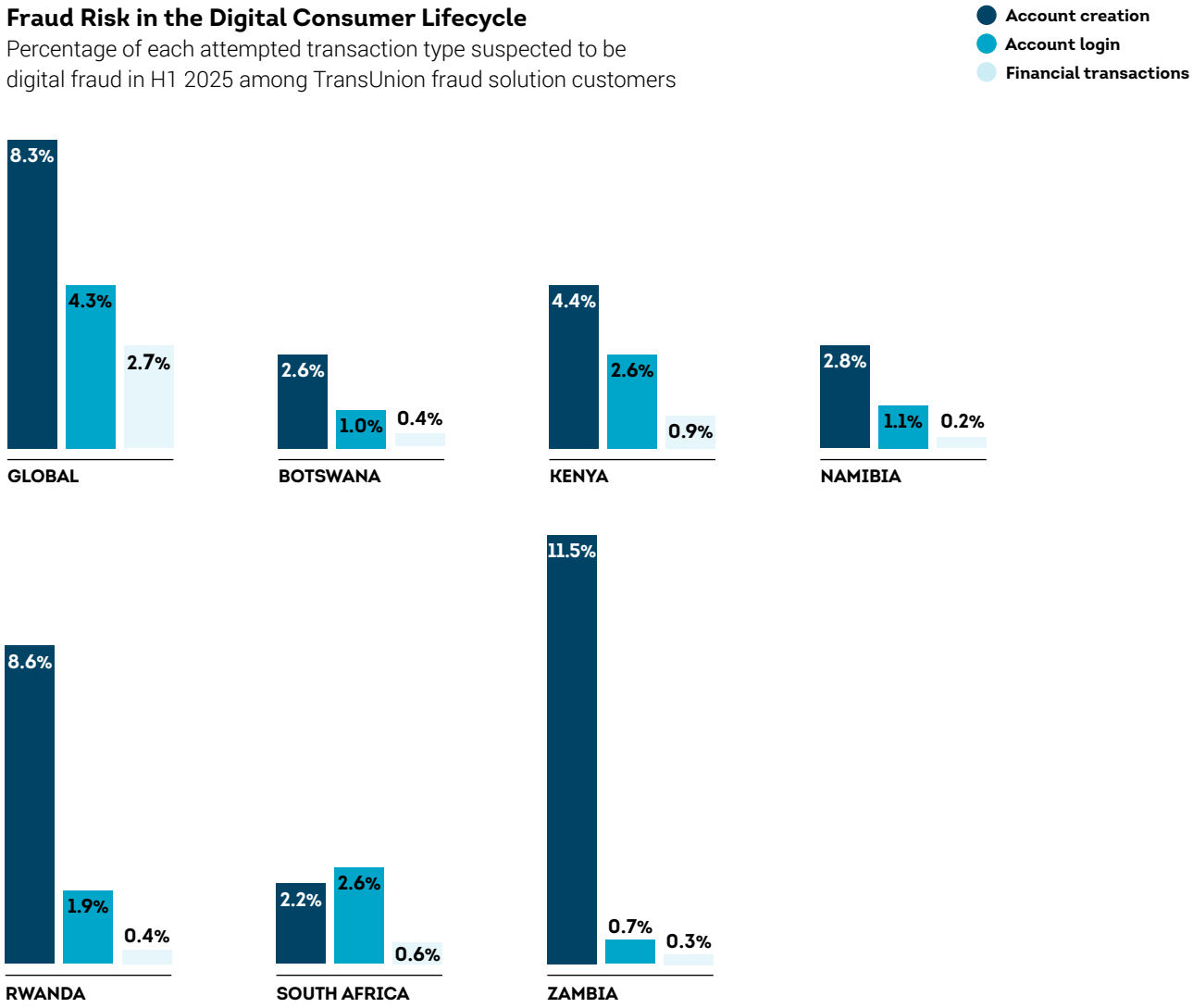
Account creation: Account signup, registration and loan origination

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 among TransUnion fraud solution customers



Source: TransUnion global intelligence network

TransUnion

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. To learn more about TransUnion fraud prevention solutions in **South Africa** and **Africa Regions**, get in touch today.

TransUnion