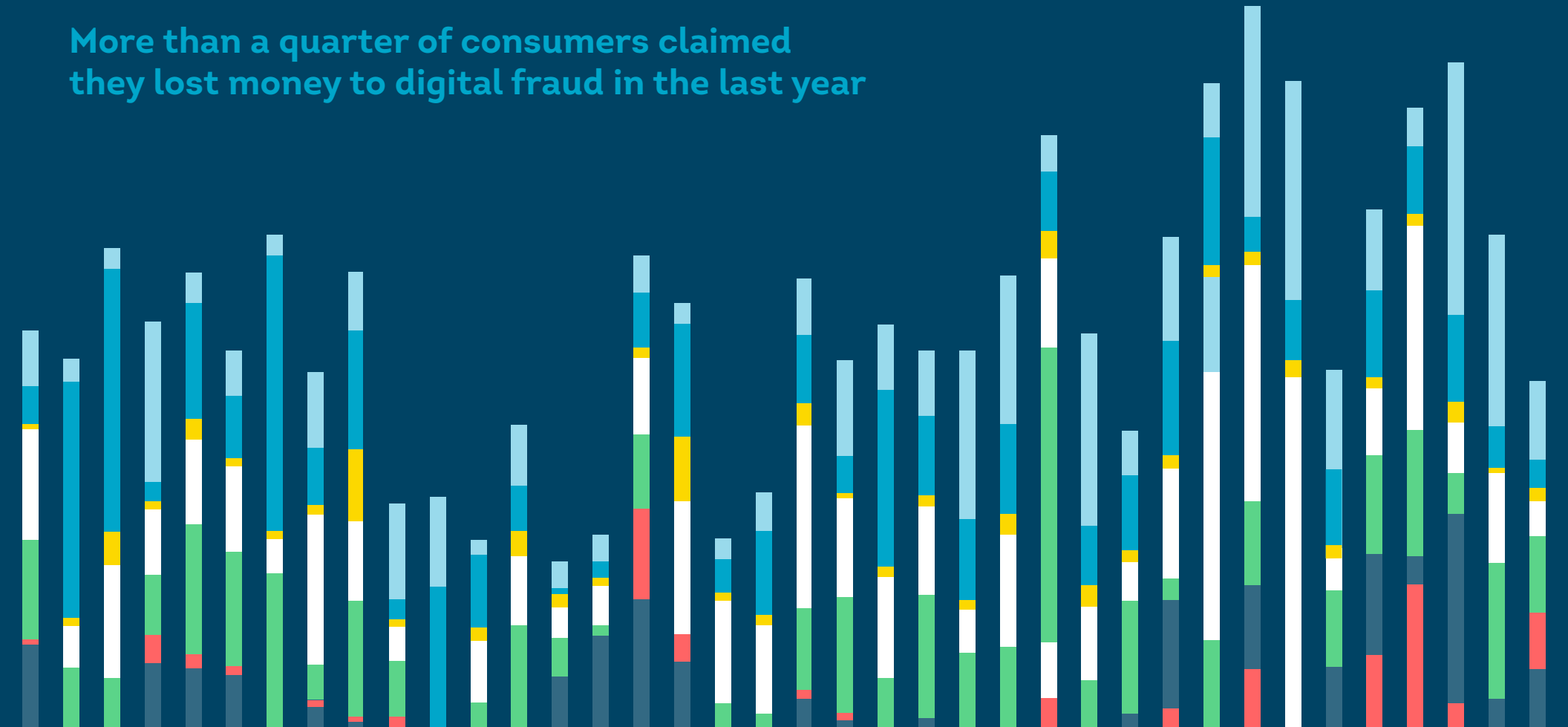
TransUnion

H1 2026 UPDATE: TOP FRAUD TRENDS

THE IMPERSONATION EPIDEMIC DRIVES COSTLY FRAUD ATTACKS

More than a quarter of consumers claimed they lost money to digital fraud in the last year



Executive Summary

Fraud has entered a new era where the primary battleground is identity. It's shifted from an operational expense to a strategic business risk — impacting revenue, growth and consumer trust. And consumers feel the pressure: in 2025, US consumers reported $99 billion in digital fraud losses, with 16% affected. Globally, a paradox emerged for organisations. While digital fraud rates declined to 3.8%, the severity and sophistication of identity-based attacks accelerated as criminals moved upstream to avoid detection. Account takeovers, for example, increased 37% to 3.14% of suspected digital fraud in 2025.

This shift reflects a broader impersonation epidemic. Fraudsters are exploiting data breaches, phishing and social engineering to shift from direct attacks to harder-to-spot identity compromise, synthetic identities and consent-based scams to bypass your detection systems. Meanwhile, consumers are demanding more protection than ever: Across markets, security of personal data is the top factor shaping where people choose to transact.

The fundamental question for organisations isn't how to block attacks but whether they can verify a person is real, legitimate and consistent across channels over time. Protecting growth now requires a unified, identity-centred approach to fraud prevention. Modern identity resolution — integrating device and behavioural intelligence with AI powered risk signals — strengthens trust, reduces friction and helps businesses stay ahead of rapidly evolving threats.

KEY TAKEAWAYS

Identity-based fraud impacts consumer trust – and wallets

26%
of consumers said they lost money from digital fraud in the last year.

77%
of consumers cited confidence their personal data is secure as the most important feature when choosing whom to transact with online.

Fraud risk persists at every stage of the consumer lifecycle

8.3%
rate of suspected digital fraud for account creation attempts in 2025, making it the highest risk stage across the consumer lifecycle.

37%
increase in the account takeover (ATO) suspected digital fraud rate from 2024 to 2025.

Compromised identities increase risk of sophisticated fraud attacks

33%
of consumers who reported being targeted by digital fraud said they experienced a phishing attack, the most of any scheme.

47%
increase in US data breach volume from 2024 to 2025.

TransUnion

About the Research

This report is intended to provide fraud, risk, identity and authentication leaders with current information to evaluate their fraud prevention tactics in the context of global fraud trends and adjust their fraud prevention strategies with confidence. It blends two sources of intelligence: insights from a global survey of 12,730 consumers in 18 countries and regions and those gained from billions of transactions within TransUnion's proprietary global intelligence network. Each lens tells a different part of the story, and together they provide a holistic view of today's fast-changing threat landscape.

How to apply these insights

Use this report as a strategic guide to:

- Benchmark your environment against global, regional and industry trends
- Identify vulnerabilities across the consumer lifecycle
- Assess your fraud stack's maturity in detecting evolving fraud attacks
- Align internal stakeholders around shared risks and consumer expectations
- Inform fraud detection investment decisions

See the full data sourcing methodology on page 25 for more detail.

Interpreting the data

Consumer survey findings

Consumer insights reflect experiences with digital fraud (online, email, phone and text messages) and attitudes and preferences about digital experiences. While they often align with actual attack patterns, they're still personal interpretations. Use them as indicators of sentiment, trust, behaviour shifts and expectations, not precise transactional measures.

Digital fraud metrics

All digital fraud data represents suspected digital fraud based on device risk indicators used by TransUnion clients. Because organisations continually adjust controls and risk appetite, fraud rates can shift over time or across industries and regions. Changes may reflect activity levels, transaction volumes or updated risk thresholds. Treat these figures as directional indicators of digital fraud activity.

Geographic comparisons: Digital fraud by geography is based on where a consumer was located during a transaction, not where a business operates. Regional fraud levels may shift from risk thresholds companies apply to certain geographies or transactions. Use these comparisons as directional indicators, not absolute measures of regional safety.

Industry benchmarks: Industry-level digital fraud rates represent fraud against companies in that sector, not fraud committed by or against consumers in that category specifically. Differences between industries often reflect how varied their risk tolerances, customer journeys and fraud prevention strategies are.

TransUnion

Contents

TransUnion

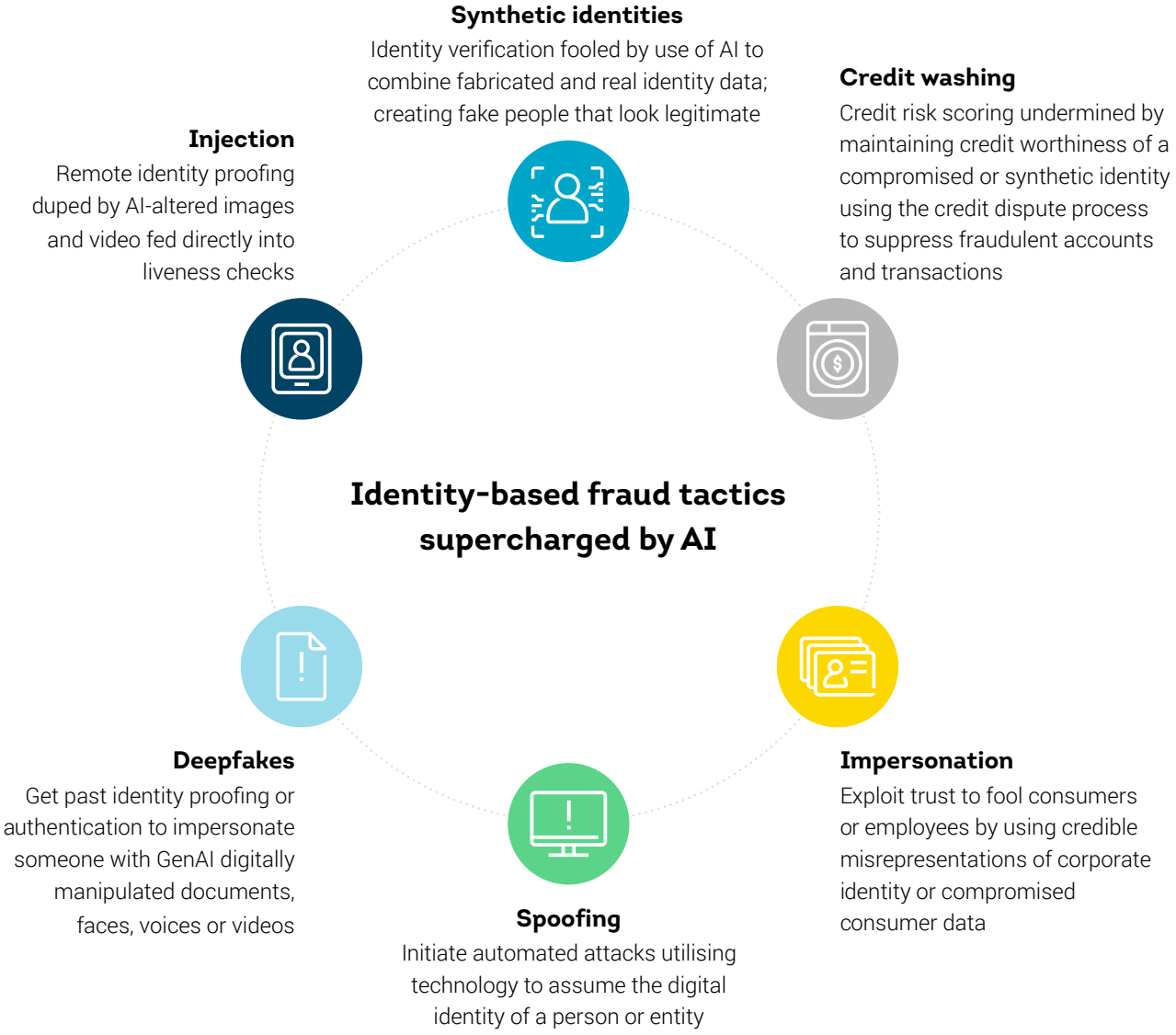
Are Your Customers Real?

The future of AI-supercharged fraud

If identity is the new frontline of fraud, AI is the ultimate tool for fraudsters and fraud fighters alike. Fraud isn't being reinvented by AI; it just lowers the barrier to entry and is easier to scale and more efficient. Think about it: The fraud ring that required 10 people to coordinate loan applications using altered identity information can now be done by a single person using AI-generated synthetic identities and a form-filling AI agent.

You see where this is going. AI will make it harder to tell the difference between real people and fraudsters at every stage of the consumer lifecycle. AI will enable effortless ATO using compromised identity credentials and new account fraud with synthetic or altered identities, deepfake documents and liveness biometrics. It will also make it easier for fraudsters to impersonate organisations' staff and spoof their digital channels to perpetrate consumer scams.

To level the playing field, you need to develop a plan for combating identity-based fraud with AI at the centre to improve detection without adding undue friction. Identity resolution is critical to support risk assessments across the lifecycle and channels over time. Look to add AI-powered detection enabled by machine learning models that leverage diverse risk signals, including device intelligence, behavioural and consortium insights.



TransUnion

GLOBAL FRAUD TRENDS

Consumer Fraud Experiences

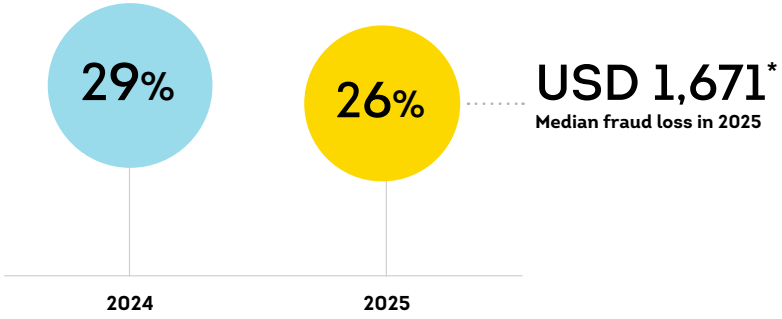
Gen Z most susceptible to losses from trust-based fraud schemes

Among consumers surveyed in 18 countries and regions, 26% said they lost money from digital fraud in the last year, costing them a median amount of USD 1,671. The youngest consumers were more likely to lose money to fraud than the overall population; 39% of Gen Z said they lost money due to digital fraud in the last year, the highest of any generation.

Broad use of social platforms, gaming platforms and cryptocurrency may play a role in the higher likelihood Gen Z would lose money. Of the types of fraud Gen Z reported losing money to, trust-based fraud — third-party seller scams on legitimate ecommerce sites (27%) and money mule scams (26%) — topped the list. That's compared to 24% for both overall, which was also the highest. Closely following, 23% of consumers overall reported losing money to vishing scams (fraudulent phone calls that induce consumers to reveal personal information), possibly the result of impersonation of legitimate businesses or government organisations.

Consumer-Reported Fraud Loss

The percent of consumers in 18 countries and regions who said they lost money to digital fraud in the last year — and the median amount they reported losing

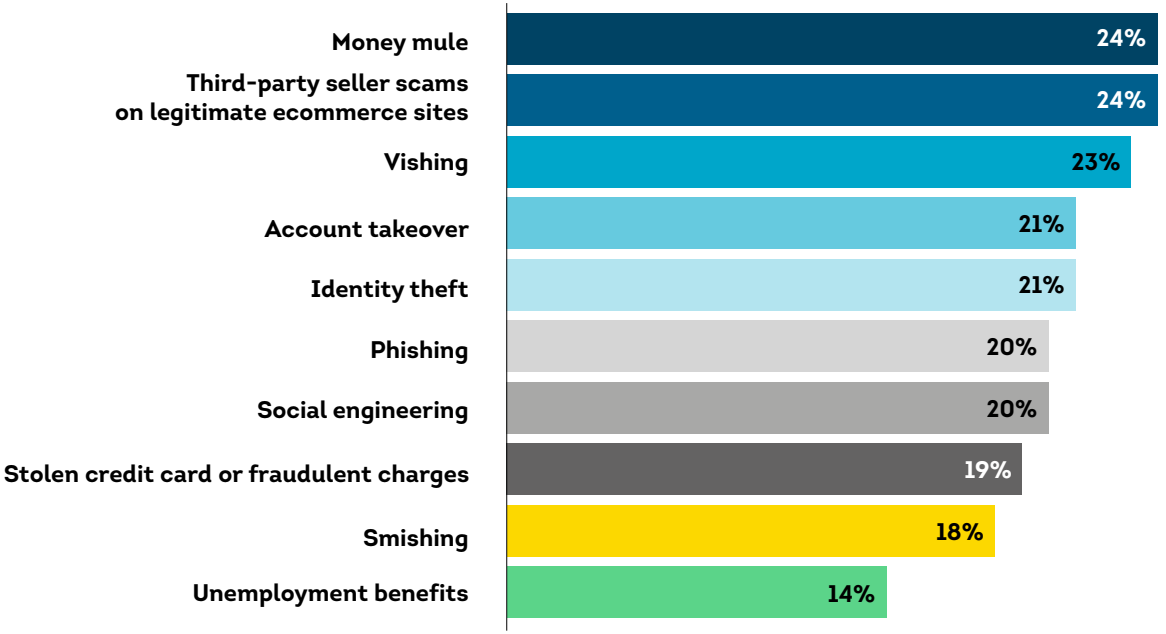


*USD conversion based on currency exchange value on Dec. 29, 2025

Source: TransUnion consumer survey

Most Prominent Cause of Fraud Loss

Percentage reporting losing money to these schemes among consumers who said they lost funds from digital fraud in the last year fraud



Source: TransUnion consumer survey

TransUnion

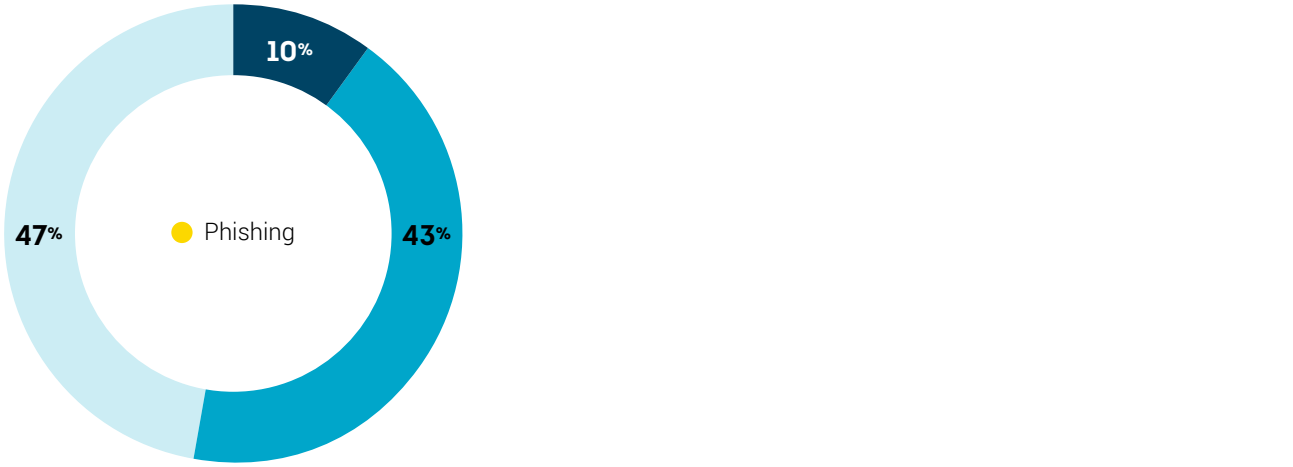
Identity-exposing scams dominate consumer reported fraud

Over half (53%) of consumers reported being targeted by digital fraud schemes from August to December 2025, and 10% said they fell victim. Still, a significant portion (47%) of those surveyed said they were unaware of being targeted.

Among those who said they were targeted, the leading types of fraud consumers reported were meant to expose identities: phishing (33%), smishing (28%) and vishing (27%).

Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with digital fraud attempts from August to December 2025, and the most frequent scheme by which they reported being attacked



Source: TransUnion consumer survey

TransUnion

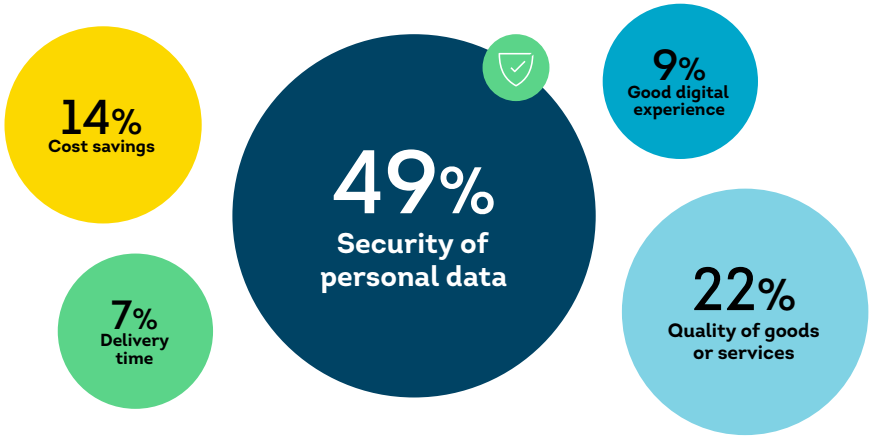
Safe and seamless online transactions drive consumer brand preference

With more consumers relying on organisations' digital services, their preferences for safety and security are critical to future business growth. Over a third (37%) of consumers said they conducted more than half of their retail and business transactions online (34% the prior year) and 39% said they conducted more than half of their account management activities online (38% the prior year). More importantly for brands, around half of high-income households reported using online channels for commerce and account management, 55% and 50%, respectively.

Expectations for safe, secure and convenient online experiences from the brands consumers choose to spend money with are high. More than half (56%) of consumers said they're likely to switch companies to get a better digital experience. When asked which digital experiences would cause you not to return to a website, the top answer was fraud concerns at 65%.

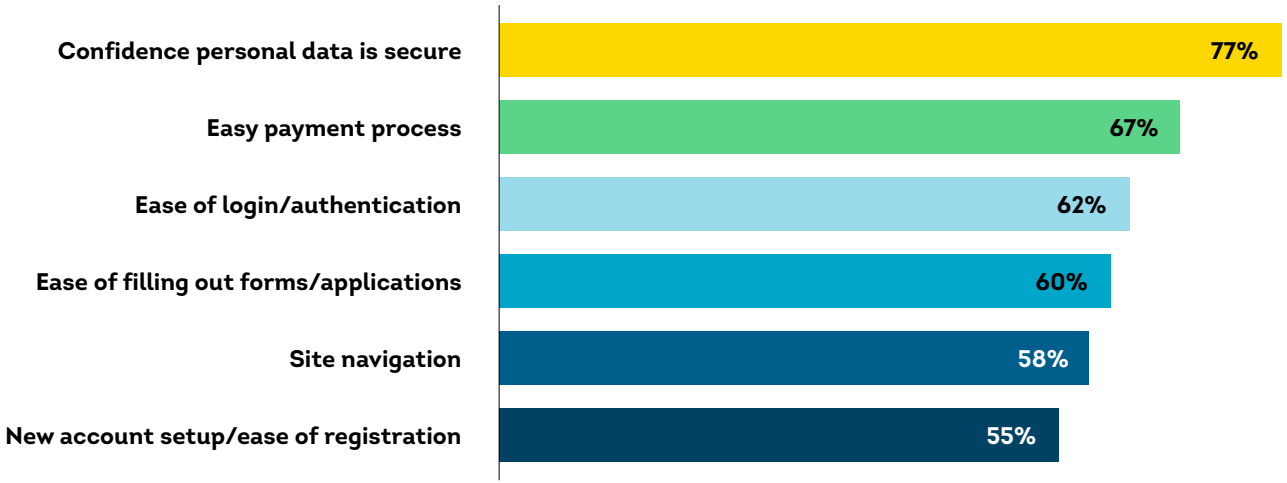
To gain more customers, organisations need to demonstrate trust when it comes to consumer data. About half (49%) of consumers ranked personal data security as the highest expectation or quality in preferred online companies. Not only that, over three-quarters (77%) said confidence their personal data will not be compromised is very important when choosing with whom to transact online. Both were the top answers for their respective questions.

Ranked Expectations/Qualities in Preferred Online Companies
Top answer chosen



Source: TransUnion consumer survey

Stated Important Features When Choosing Whom to Transact With Online
Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

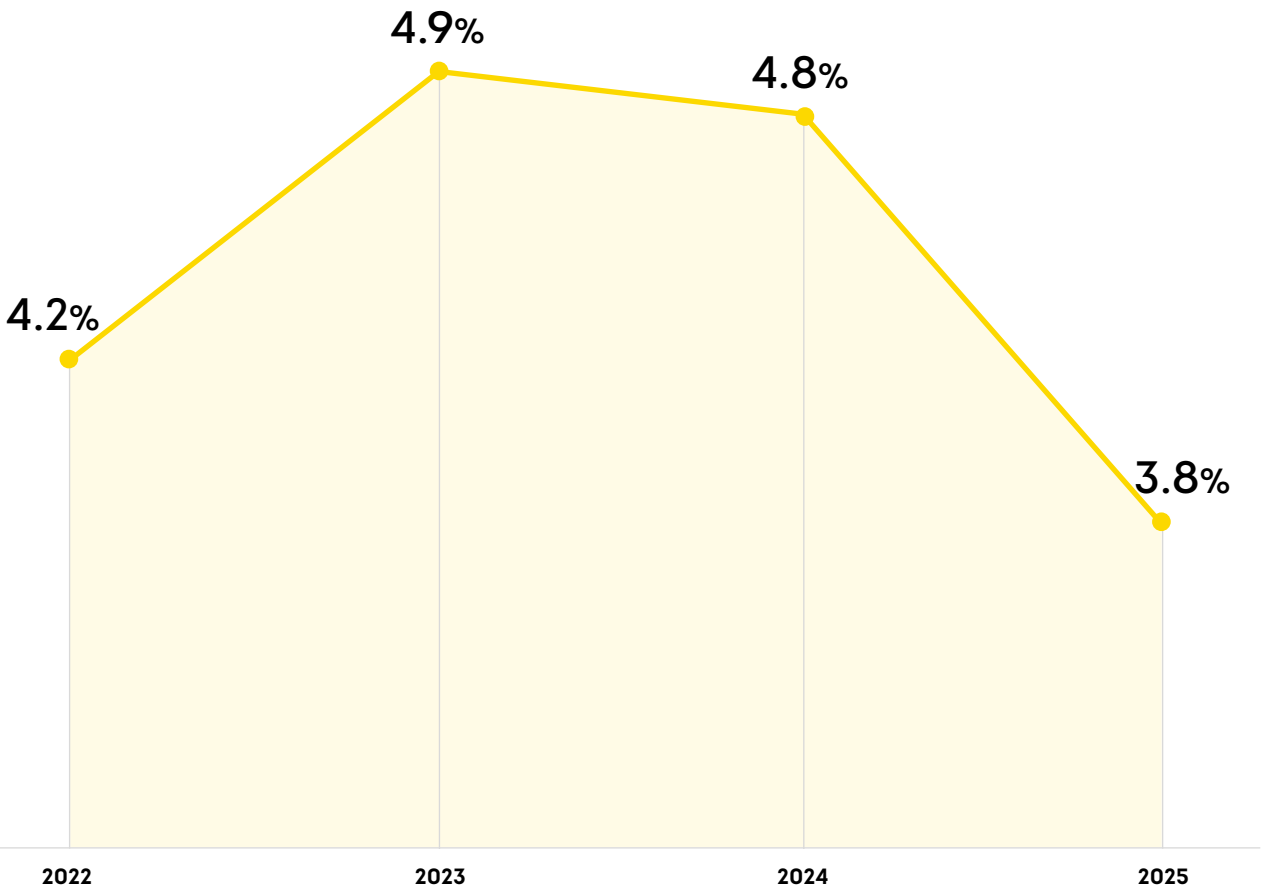
Digital Fraud Trends

Suspected digital fraud rate lower overall

The rate of suspected digital fraud attempts globally among TransUnion® clients was 3.8% in 2025; the lowest rate in our analysis dating back to 2022. What's behind this trend? Organisations may be reporting a lower percentage of fraud due to increased digital transaction volume. As such, their detection systems may be tuned to catch larger fraud risks, letting more medium-risk transactions flow. Bad actors may also be subverting existing fraud detection and authentication tools with the use of synthetic, stolen or socially engineered consumer credentials to gain access to existing accounts or open new ones. Criminals are also avoiding organisations' fraud detection tools by successfully targeting consumers directly.

While the overall rate fell, differences by region and industry tell a more nuanced story. For example, regionally for the select countries we analysed, Asia (5.9%) had the highest rate of suspected digital fraud, while Europe (2.1%) had the lowest.

Rate of Suspected Digital Fraud Globally



Source: TransUnion global intelligence network

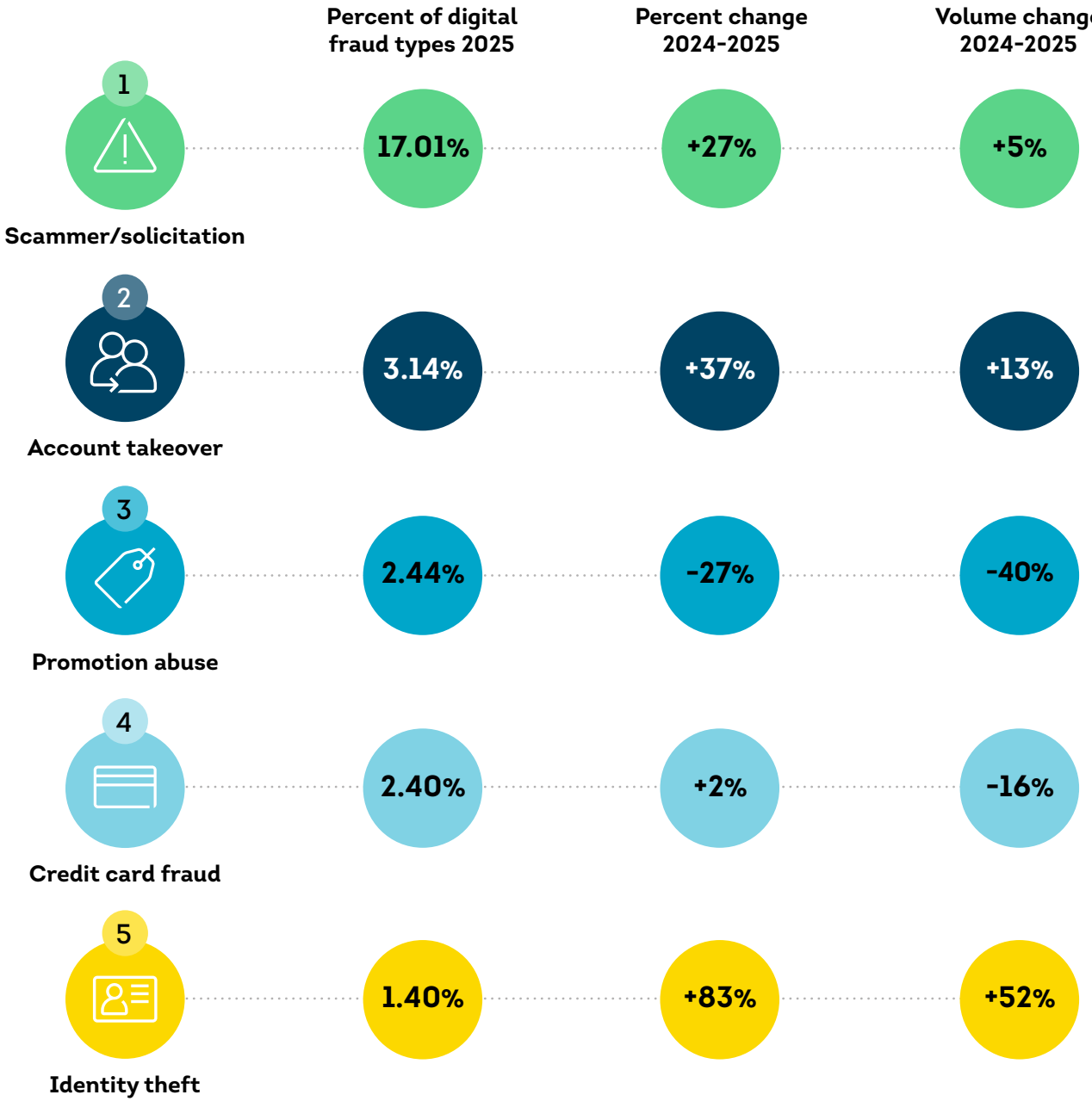
TransUnion

ATO attacks grow in frequency and volume

Consumer accounts continued to be under attack, with ATO rising to 3.14% of digital fraud reported to TransUnion in 2025, up from 2.3% in 2024. Not only did the rate grow 37% in 2025, but the volume of digital transactions reported as ATO also grew 13%.

Making up 17.01% of all suspected digital fraud reported to TransUnion in 2025, scammer/solicitation fraud (promoting unauthorised services and products, often to steal account credentials) was again the top type of digital fraud, increasing 27% since 2024. ATO and scammer/solicitation are closely linked as solicitation scams often lead directly or indirectly to ATO attempts.

Top Digital Fraud Types and Their Growth



Source: TransUnion global intelligence network

TransUnion

Entertainment industries are the most susceptible to digital fraud risk

The video gaming industry experienced the highest percentage (12.8%) of suspected digital fraud attempts globally in 2025 among industries analysed, a 7% increase in volume over 2024. This was followed by communities at 8.1%. The top fraud type reported by TransUnion clients in these industries was scammer/solicitation.

Why is video gaming a ripe target for fraud? This isn't primarily an issue of a 14-year-old on a gaming console. Based on a global survey by the Entertainment Software Association, the average age of a video gamer is 41, with the largest gamer segment age range between 25–36. And, more than half of gamers said their preferred gaming device is a mobile phone. With fictitious screen names the norm for attention economy platforms, fraudsters have a perfect environment in which to engage unsuspecting members.

Bad actors taking advantage of entertainment and social-oriented site engagement, including video gaming and communities, create fake user profiles to target consumers with scams and solicitations. Sometimes, they use this method to defraud consumers directly, but more often, they do so to secure personal information to perpetrate ATO or new account creation fraud down the line.

Digital Fraud Attempts by Industry

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

Video gaming

2025
12.8%
Scammer/solicitation

2024-2025
+7%

Communities
(online dating, forums, etc.)

2025
8.1%
Scammer/solicitation

2024-2025
-36%

Gaming
(online sports betting, poker, etc.)

2025
7.7%
Promotion abuse

2024-2025
+27%

Telecommunications

2025
4.2%
Scammer/solicitation

2024-2025
+66%

Financial services

2025
3.2%
Account takeover

2024-2025
-21%

Retail

2025
2.8%
Account takeover

2024-2025
-60%

Government

2025
2.2%
Credit card fraud

2024-2025
+28%

Logistics

2025
1.6%
Shipping fraud

2024-2025
-55%

Insurance

2025
1.3%
Suspected ghost broker

2024-2025
-39%

Travel & leisure

2025
0.2%
Credit card fraud

2024-2025
-58%

Source: TransUnion global intelligence network

Digital Fraud Across the Consumer Lifecycle

Account creation is highest risk stage of the consumer lifecycle

Bad actors using altered, stolen, fake or synthetic identities targeted the digital new account creation process in 2025, with 8.3% of all these transactions suspected of digital fraud. This was by far the riskiest consumer lifecycle stage, followed by account login (4.3%).

Account creation was the riskiest consumer lifecycle stage for most industries analysed in 2025, except for financial services, insurance, telecommunications and government where financial transactions were the riskiest. The communities and retail industries had the highest rates of suspected digital fraud during account creation among sectors analysed at 22.5% and 22.3%, respectively.

Consumer Lifecycle Stage Examples

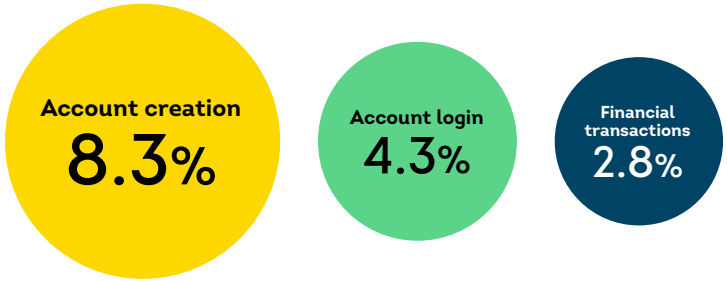
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

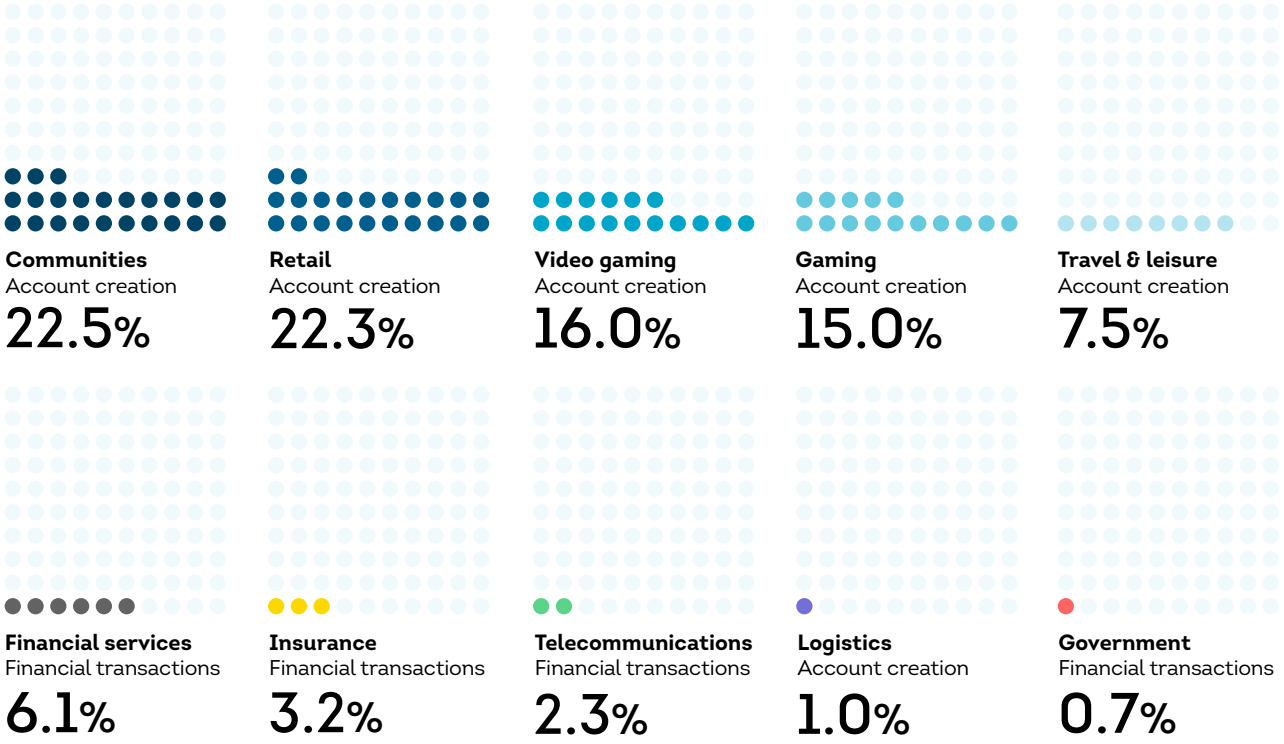
Percentage of each attempted transaction type suspected to be digital fraud in 2025



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 the corresponding percentage for that stage in 2025



Source: TransUnion global intelligence network

TransUnion

AFRICA

Africa Overview

Digital fraud across Africa continues to evolve as consumers and businesses deepen their reliance on mobile-first, digitally connected ecosystems. While the region shares common pressures, each market reflects a distinct blend of behaviour and attacker focus — with Kenya and Zambia facing heavy messaging-based social engineering, Namibia seeing more voice-driven impersonation, Rwanda contending with identity misuse and mule activity, and South Africa navigating sophisticated marketplace and cross-channel scams.

Ecommerce deception, ATO attempts and organised money mule recruitment points to rising coordination among fraud networks. At the same time, improved detection across several markets is shifting criminal focus toward early consumer lifecycle points, such as new account creation, where identity gaps and synthetic identity activity remain persistent challenges.

Across all countries, consumers expect strong data protection, visible safeguards and seamless digital experiences. As fraud tactics diversify, strengthening identity assurance, applying friction-right authentication and expanding cross-industry intelligence will be essential to protecting trust and enabling secure digital growth across the continent.

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 Kenya, Namibia, Rwanda, South Africa and Zambia.

KEY TAKEAWAYS

Consumers report significant fraud losses

USD 580
median consumer-reported fraud loss among Africans who said they lost money to digital fraud in the last year.

33%
of African consumers who said they lost money to fraud in the last year reporting doing so to third-party seller scams on legitimate ecommerce sites, the most common answer on the continent.

Security top consumer online priority

50%
of Africans said the security of personal data is their top expectation when deciding what online company to do business with, the most popular answer in the region.

86%
of Africans said confidence their personal data will not be compromised is the most important feature when choosing whom to transact with online, the top answer in the region.

South Africa had the highest suspected digital fraud rate in the region

3.0%
suspected digital fraud rate for attempted transactions where the consumer was in South Africa in 2025, the highest for countries analysed in the region.

2.6%
suspected digital fraud rate for attempted transactions where the consumer was in Botswana, Kenya, Namibia, Rwanda, South Africa and Zambia in 2025.

Consumer Fraud Experiences

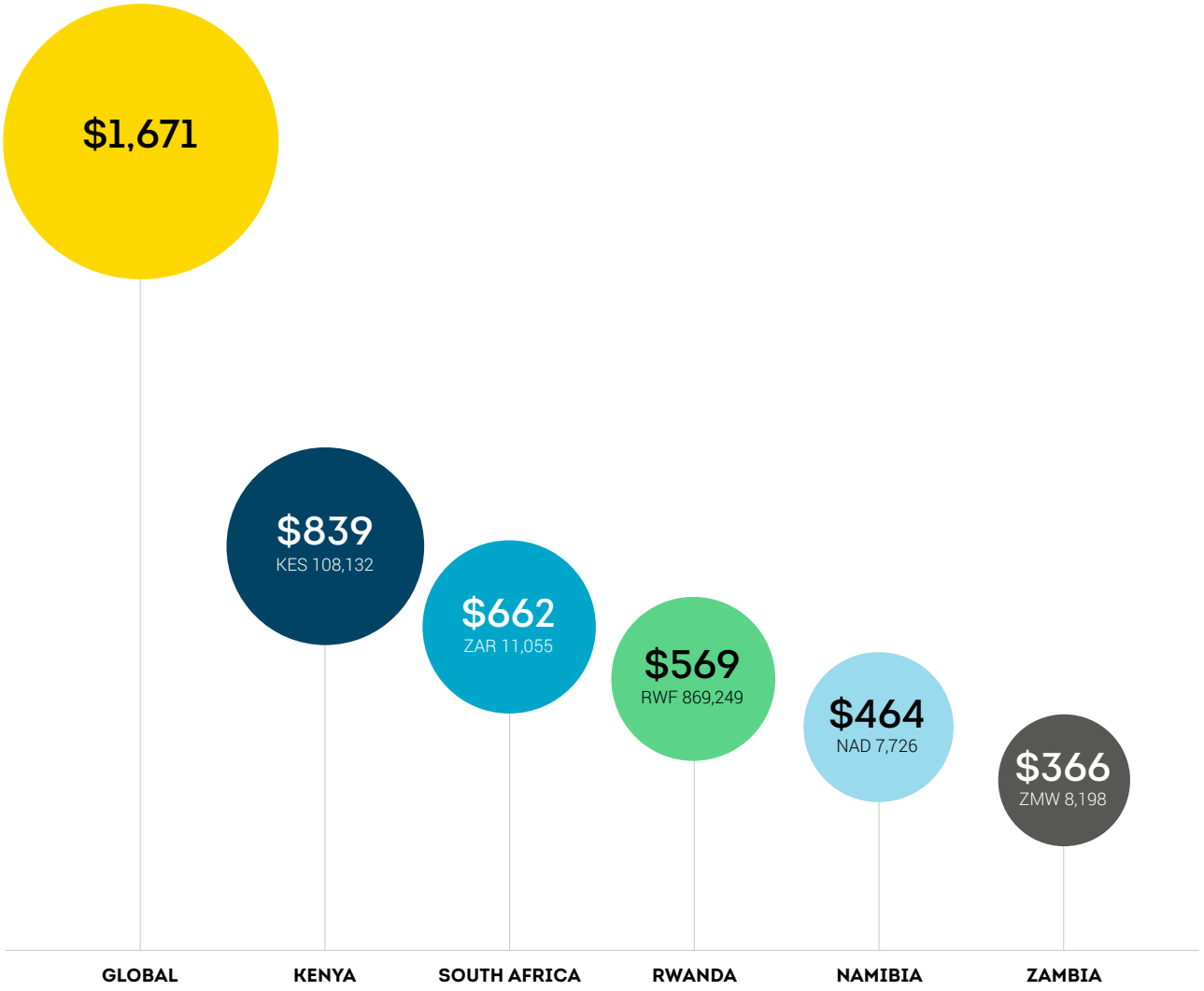
African fraud losses lower than global average but still significant

Even though fraud losses among consumers who said they lost money in the last year due to digital fraud across Africa was well below the global median of USD 1,671, the financial impact on consumers is still significant. Kenyan consumers reported the highest losses in the region at USD 839 (KES 108,132) — followed by South Africa at USD 662 (ZAR 11,055) and Rwanda at USD 569 (RWF 869,249). Namibia (USD 464 or NAD 7,726) and Zambia (USD 366 or ZMW 8,198) reported smaller losses, but that doesn't mean people there were targeted any less. Instead, it reflects different levels of digital adoption and fraud-prevention maturity across the region.

What's clear is fraud — whether through email, online platforms, phone calls or text messages — continues to hit African consumers in very real ways. As digital activity expands, so does the need for stronger security measures, friction-right solutions and ongoing awareness to help people spot threats before they cause financial loss.

Consumer-Reported Fraud Loss

Median reported fraud loss (in USD) among consumers who said they lost funds from digital fraud in the last year



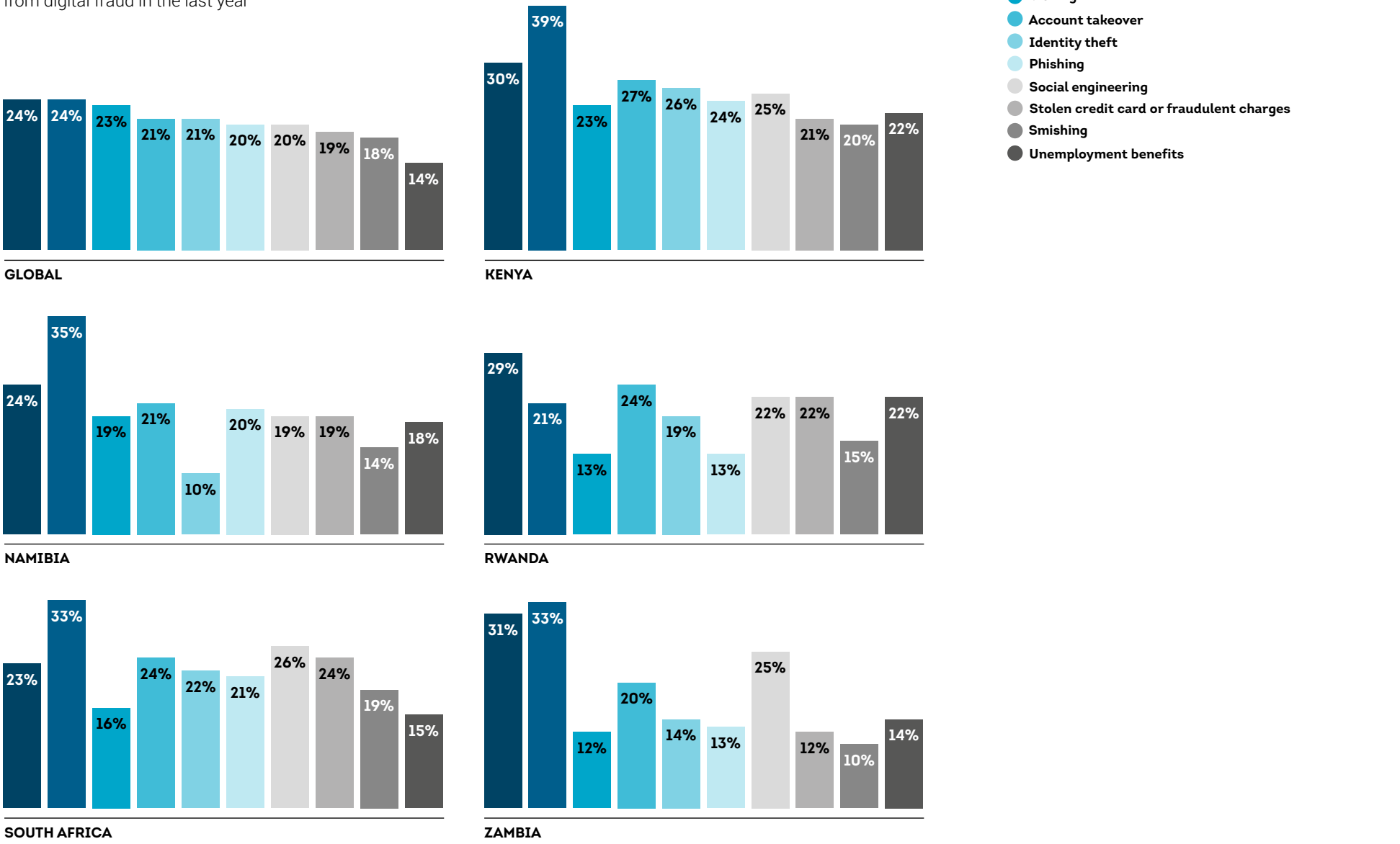
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

Source: TransUnion consumer survey

TransUnion

Most Prominent Cause of Fraud Loss

Percentage reporting losing money to these schemes among consumers who said they lost funds from digital fraud in the last year



Source: TransUnion consumer survey

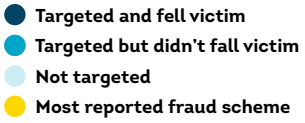
Fraud attempts target majority of African consumers, with smishing most common

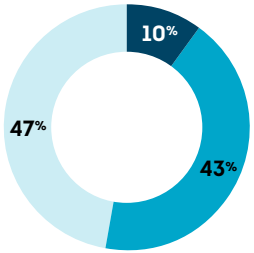
In Africa, a large share of consumers said they faced frequent fraud attempts, with most reporting they were targeted by digital fraud attempts from August to December 2025 but avoided falling victim. Kenyan and Zambian consumers reported the highest rates of being targeted but not falling victim in the region at 72% and 68%, respectively. Namibians (55%), Rwandans (60%) and South Africans (50%) also reported high levels of attempted scams, demonstrating broad regional exposure.

While most consumers reported not falling victim, 12%–14% still said they did, showing persistent attempts often break through. The most common attack types reported by those who said they were targeted vary by market. Smishing was the most reported type of attack in Kenya and Zambia, vishing in Namibia, phishing in Rwanda, and third-party seller scams on legitimate ecommerce sites in South Africa. Together, these patterns reflect a diverse and evolving fraud landscape that continues to challenge consumers across the region.

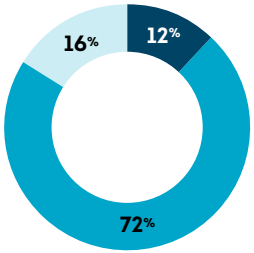
Consumers Targeted With Fraud

Percentage of consumers who said fraudsters targeted them with digital fraud attempts from August to December 2025, and the most frequent scheme by which they reported being attacked

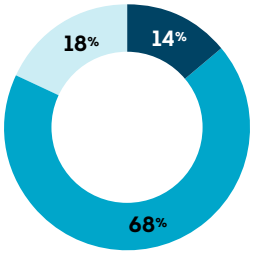




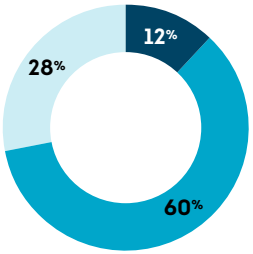
GLOBAL
Phishing



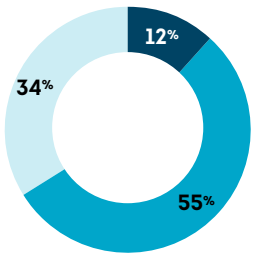
KENYA
Smishing



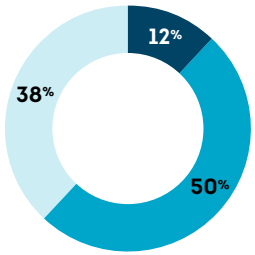
ZAMBIA
Smishing



RWANDA
Phishing



NAMIBIA
Vishing



SOUTH AFRICA
Third-party seller scams on legitimate ecommerce sites

Source: TransUnion consumer survey

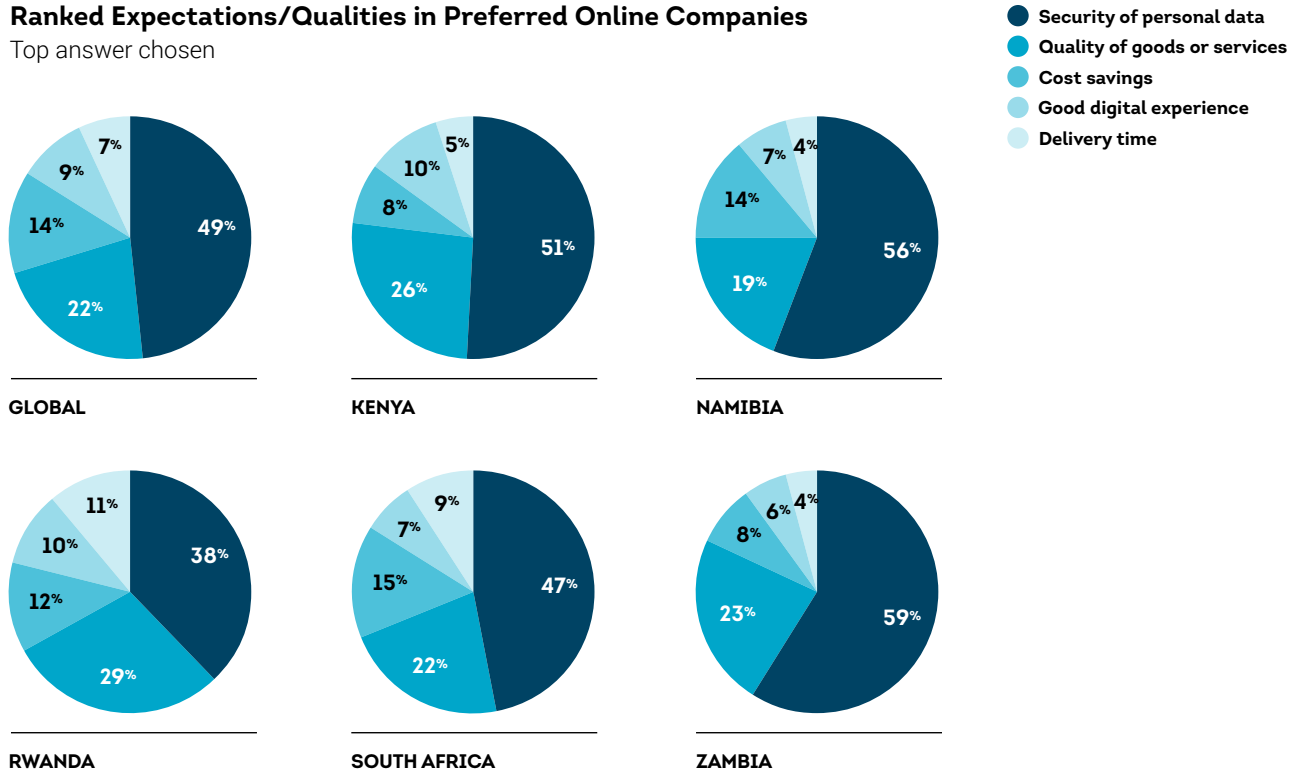
TransUnion

Security and product quality drive African consumers' online preferences

In the African markets, consumers place the strongest emphasis on the security of their personal data when choosing which online companies to trust. When asked for their top expectation when deciding what online company to do business with, Zambians were most likely to say security of personal data at 59% — followed by Namibians (56%), Kenyans (51%), South Africans (47%) and Rwandans (38%). Quality of goods and services also ranked highly, especially in Rwanda (29%) and Kenya (26%).

While cost savings and delivery time matter, they play a smaller role compared to trust and product confidence. A good digital experience shows moderate influence, with Kenya and Rwanda leading at 10% when consumers were asked for their top expectation when deciding what online company to do business with. Overall, the data shows African consumers are increasingly selective, prioritising platforms that make them feel safe and deliver consistently strong value.

Ranked Expectations/Qualities in Preferred Online Companies
Top answer chosen

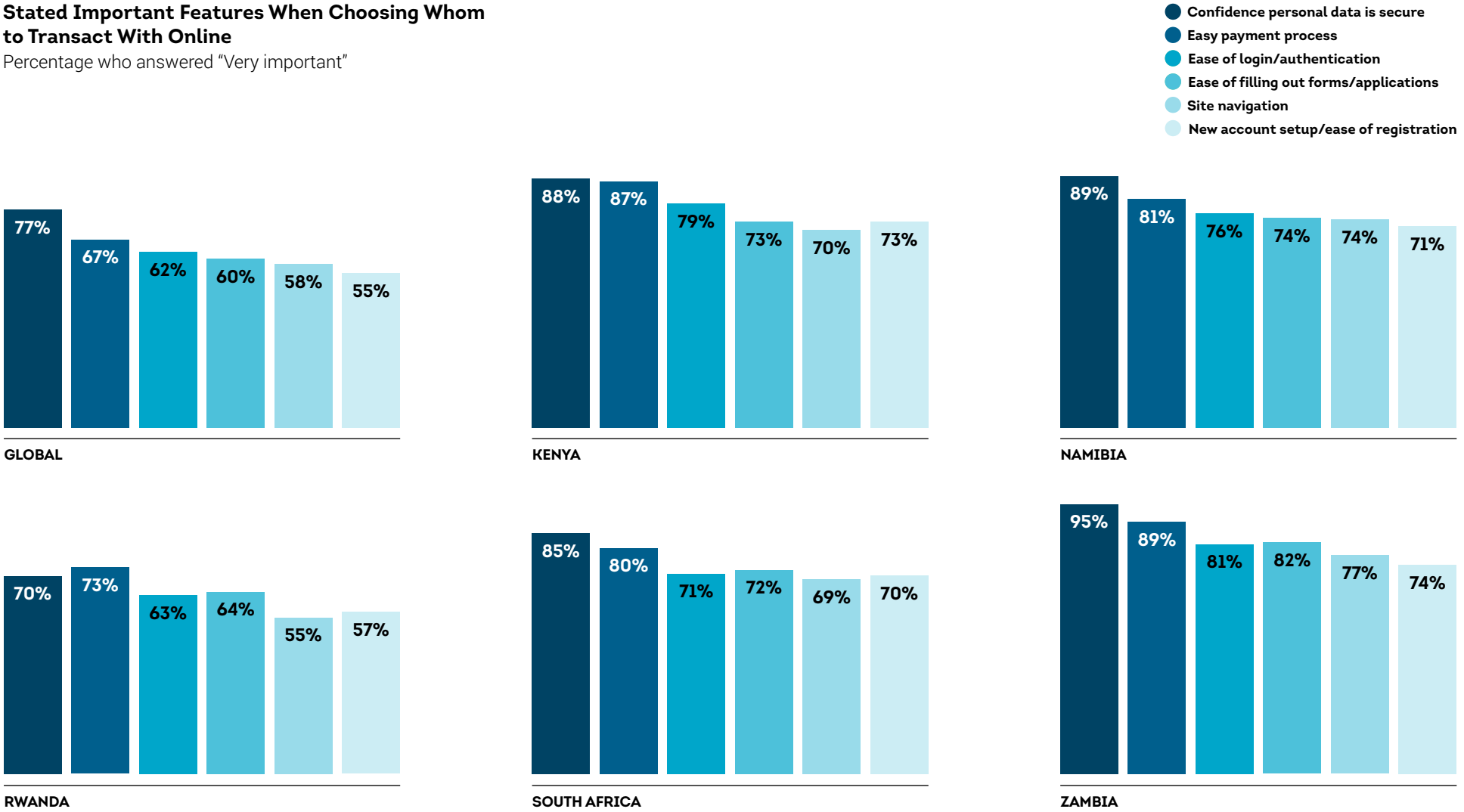


Source: TransUnion consumer survey

TransUnion

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

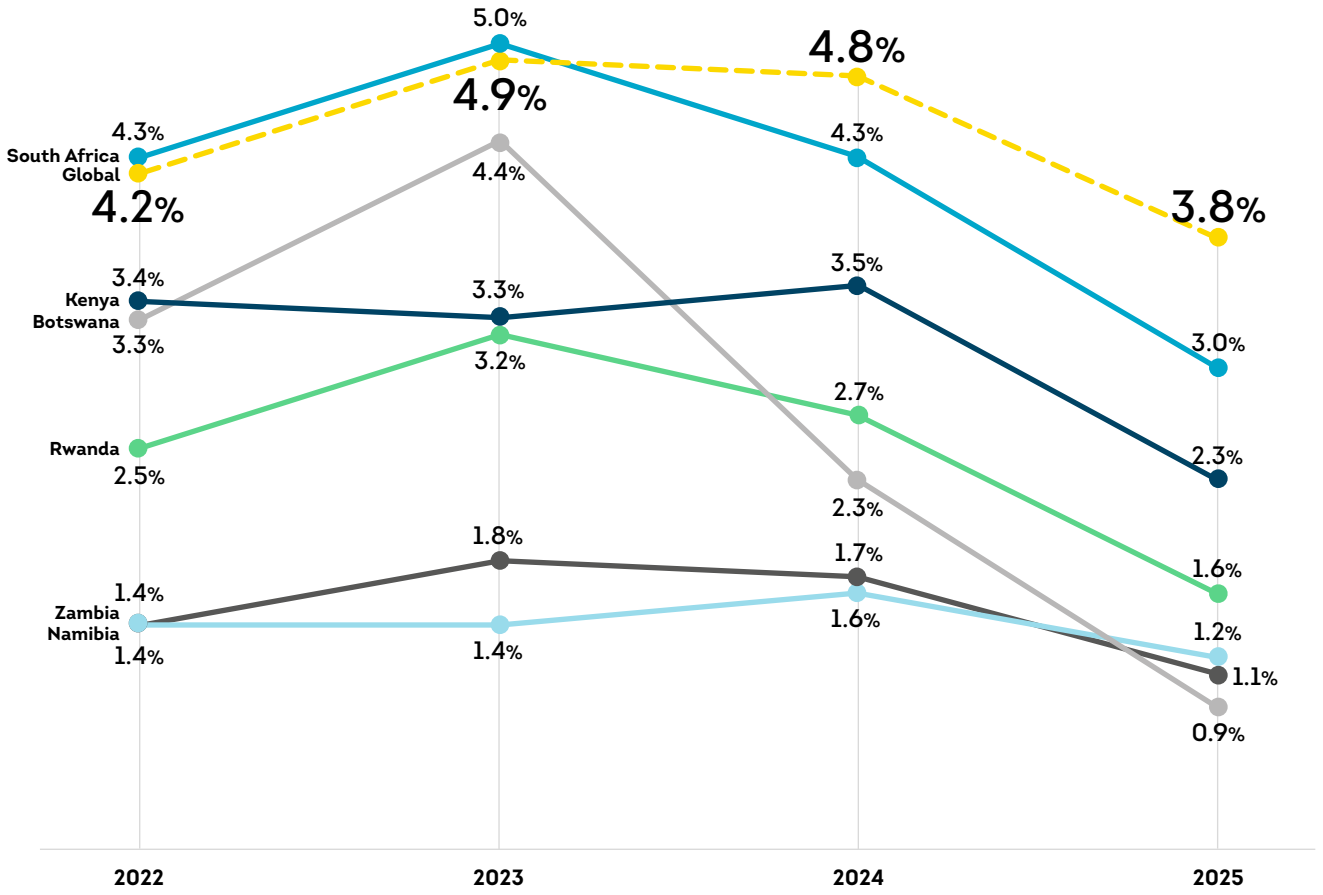
Digital Fraud Trends

Despite dropping digital fraud rates, specific investments required

Suspected digital fraud attempt rates in the African countries analysed declined from 2022 to 2025, signalling improvements in detection and prevention, but the region remains vulnerable. For attempted transactions where the consumer is in the respective country, South Africa consistently reports the highest rates, dropping from 4.3% in 2022 to 3.0% in 2025, close to the global average. Kenya showed a similar downward trend, falling from 3.4% to 2.3%, while Rwanda declined from 2.5% to 1.6% over the same period. Namibia, Zambia and Botswana maintained the lowest levels in the region, ending 2025 at 1.2%, 1.1% and 0.9%, respectively.

Although the downward trend is encouraging, the data reflects an evolving fraud landscape where fraudsters continuously adapt their methods. Steady investment in authentication, user education and real-time monitoring will be essential to sustaining progress and reducing future risks.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

TransUnion

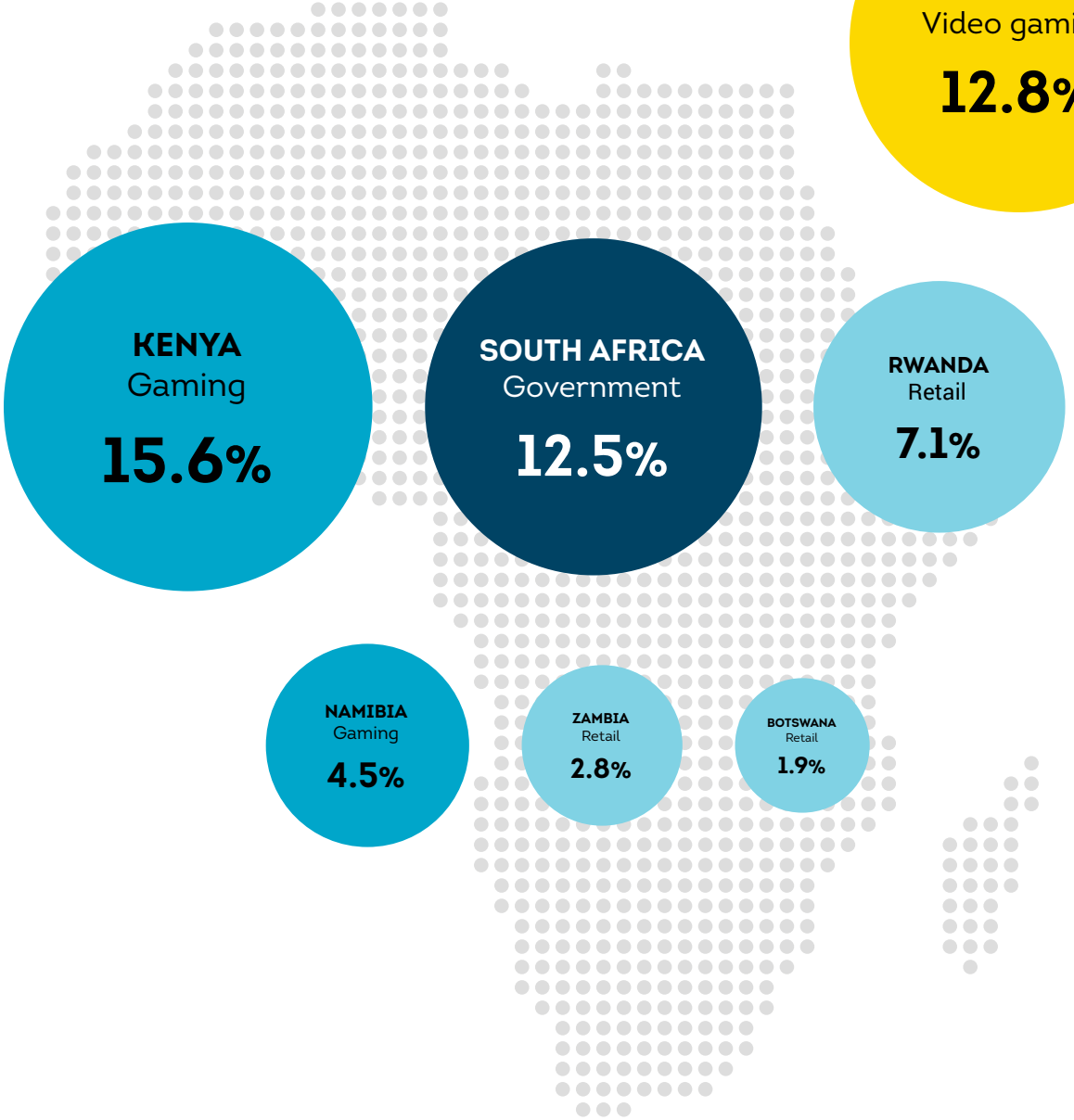
Industries targeted by fraud vary widely across Africa

Suspected digital fraud attempts across Africa in 2025 showed fraudsters focusing on very different industries depending on the country, reflecting local digital behaviours and opportunity points. Attempted transactions where the consumer was in Kenya had the highest suspected digital fraud rate for an industry in the region in 2025, with gaming targeted at a significant 15.6%, indicating strong exposure in the fast-growing digital entertainment channel. Following closely was South Africa where government faced a 12.5% fraud rate, highlighting risks tied to public-sector digitalisation. Rwanda also showed notable exposure, with retail experiencing a 7.1% suspected digital fraud rate as online shopping expands. Namibia and Zambia saw comparatively lower fraud pressure; gaming (4.5%) dominated in Namibia and retail (2.8%) in Zambia.

These differences reveal an evolving landscape where fraudsters tailor their tactics to each country's digital footprint, exploiting whichever industries show the most consumer activity and trust.

Digital Fraud Attempts by Country and Industry in 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

TransUnion

Account creation was the riskiest stage in the digital consumer lifecycle in Africa

Fraud risk varies significantly across different stages of the digital consumer lifecycle, with account creation standing out as the most vulnerable point. Zambia showed the highest exposure by far with 13.7% of account creation attempts when the consumer was in that country suspected to be digital fraud in 2025, well above all other markets. Rwanda followed at 7.7%, indicating fraudsters often target early onboarding steps where identity verification may be weaker. Kenya also faced elevated risk at 4.5% during account creation compared to much lower suspected digital fraud rates during login (2.3%) or financial transactions (0.9%).

In contrast, South Africa saw a different pattern. Login attempts where the consumer was in that country had a higher suspected digital fraud rate (3.0%) than account creation (2.4%), suggesting attackers are increasingly trying to compromise existing accounts. Namibia showed consistently low fraud levels, with financial transactions presenting the lowest risk (0.2%).

Overall, the data revealed while attackers use varied tactics across the region, initial stages of digital engagement, especially new account setup, are a key focus for fraudsters.

Consumer Lifecycle Stage Examples

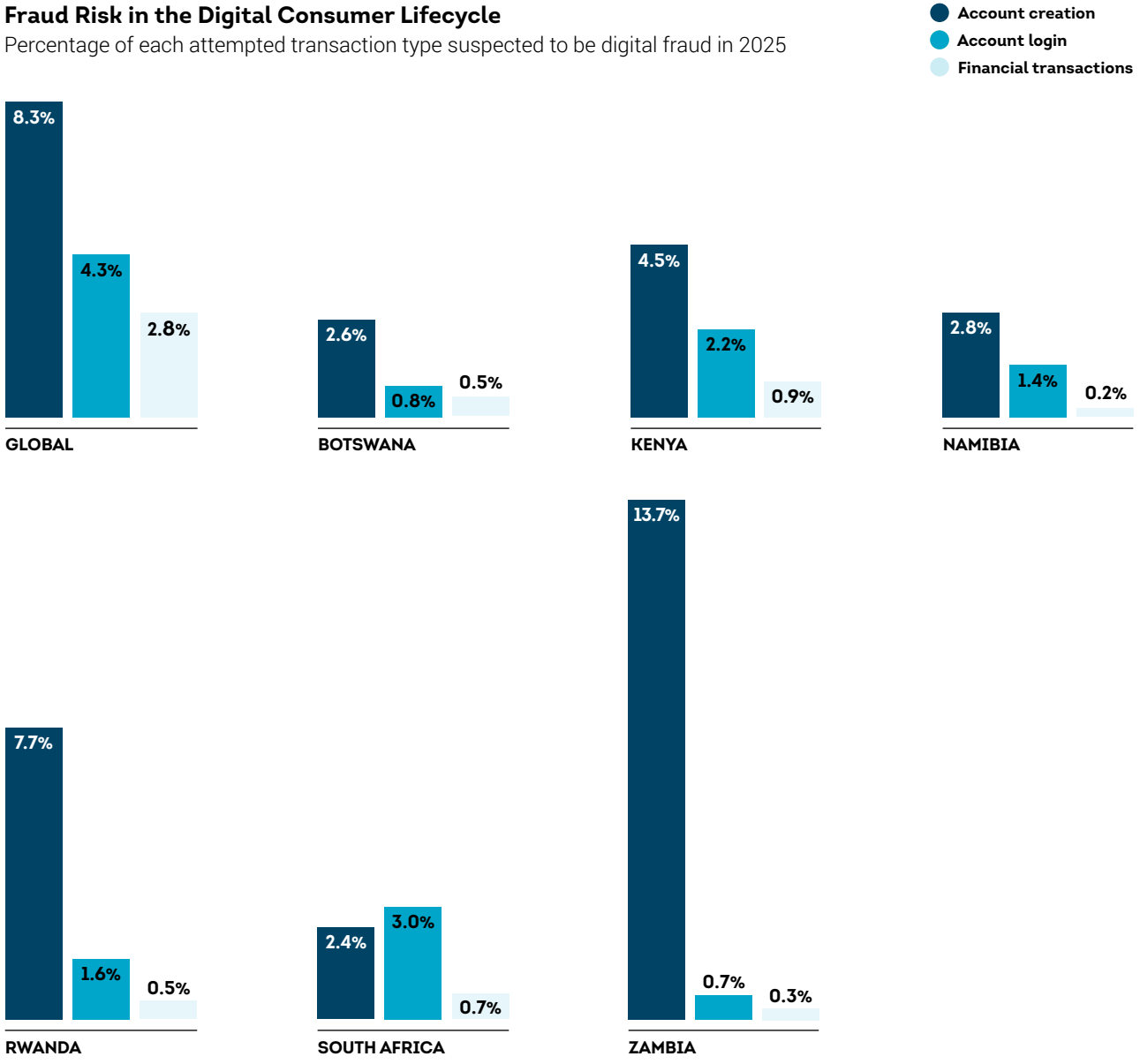
Account creation: Account signup, registration and loan origination

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 2025



Source: TransUnion global intelligence network

TransUnion

Conclusion

Fraud is becoming a bigger challenge for organisations of all sizes and industries. As we look ahead in 2026 and beyond, risks will grow as fraudsters work to avoid or fool your defences. Data breaches and scams will continue to compromise identities, making it essential to protect your organisation and consumers. The reality is you have to instil trust in consumers while trusting no one — all without compromising a seamless customer experience.

With digital identity risks throughout the consumer lifecycle, investing in smarter fraud detection is no longer a nice-to-have, it's a must. This means taking a holistic, enterprise-wide approach to fraud prevention. Fragmented systems are easier for fraudsters to exploit, so it's time to break down those silos and strengthen every layer of your defences. From identity and document verification to authentication and session monitoring, each layer needs to be smarter, more adaptive and equipped with better risk signals and scoring.

AI should be front and centre. As threats evolve, your strategies need to evolve too. Focus on reducing fragmented identity data by leveraging advanced analytics, better risk signals and integrated technology. In doing so, you'll not only detect fraud more effectively but also reduce unnecessary friction for consumers — while avoiding the extra costs of false positives. It's all about staying ahead of fraudsters and protecting what matters most. TransUnion can partner with you to show you how to do so utilising its learnings from 20 years of successfully applying AI to generate integrated, data-driven insights for its clients.

Data Sourcing Methodology

This report blends proprietary data from TransUnion's global intelligence network and a specially commissioned consumer survey.

Consumer survey

This online survey was conducted Nov. 20–Dec. 9, 2025 in Brazil (1000 respondents), Canada (999), Chile (499), Colombia (853), the Dominican Republic (415), Hong Kong (1000), India (950), Kenya (495), Mexico (500), Namibia (308), the Philippines (821), Puerto Rico (218), Rwanda (308), South Africa (1000), Spain (999), the UK (1000) and US (1000), and Zambia (365) by TransUnion in partnership with third-party research provider, Dynata. Adults 18 years of age and older were surveyed using an online research panel method across a combination of desktop, mobile and tablet devices. Survey questions were administered in Chinese (Hong Kong), English, French (Canada), Portuguese (Brazil) and Spanish (Colombia, the Dominican Republic, Mexico, Puerto Rico and Spain). To ensure 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. Suspected digital fraud attempts reflects those which TransUnion clients determined met one of the following conditions based on device risk indicators: 1) denial in real time due to fraudulent indicators, 2) denial in real time for corporate policy violations, 3) fraudulent upon client investigation, or 4) a corporate policy violation upon client investigation. 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