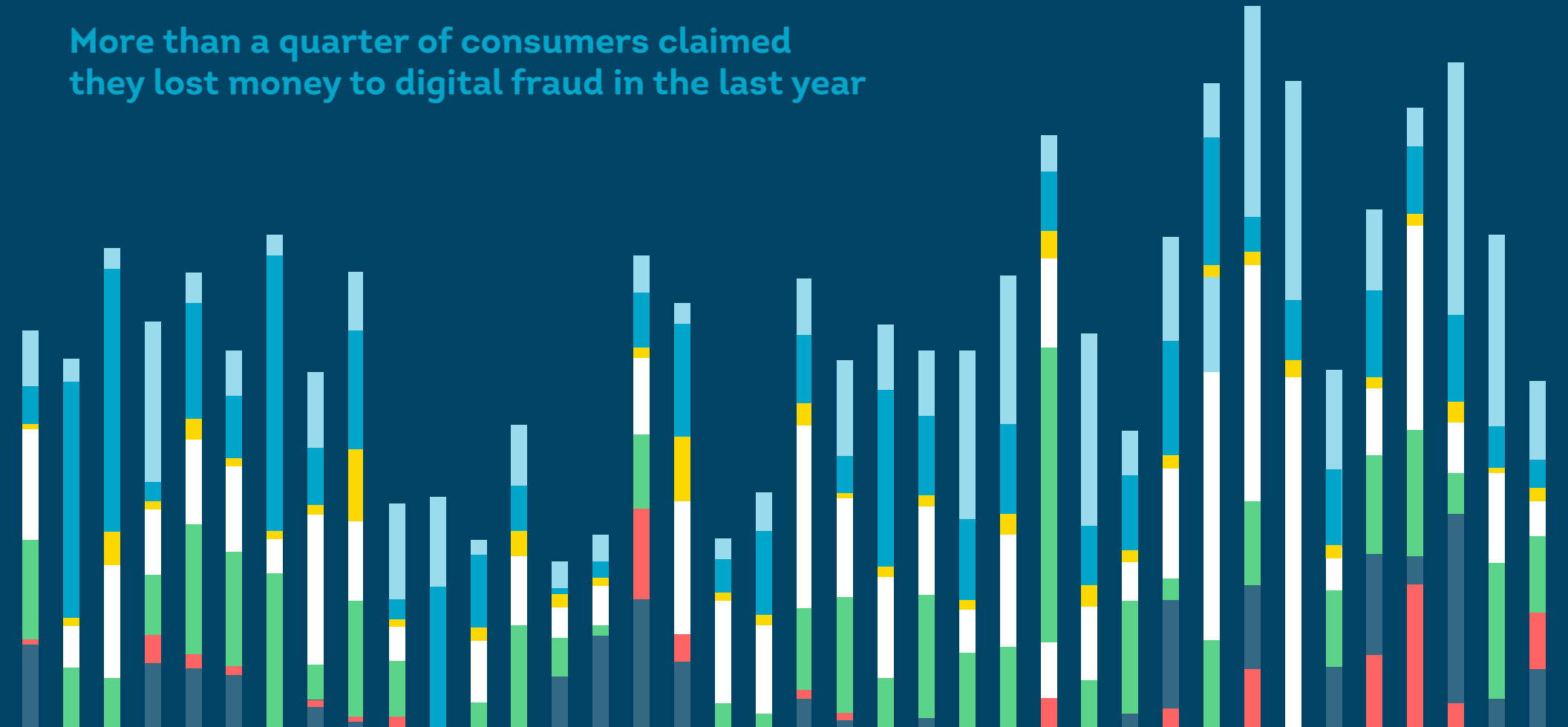
TransUnion

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 78 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.

US specific data considerations

Data breaches: Breach volumes rely on publicly disclosed information; actual exposure may be higher. Breach Risk Score (BRS) measures how easily exposed credentials can enable identity fraud.

Call centre fraud: High-risk call rates are influenced by how each institution configures its scoring thresholds.

Synthetic identity exposure: Synthetic fraud estimates reflect only credit categories TransUnion measured; the true exposure may be larger.

Credit report disputes: These metrics depend on credit report disputes where consumers claimed fraud against them and may fluctuate with guidance and consumer behaviour.

TransUnion

Contents

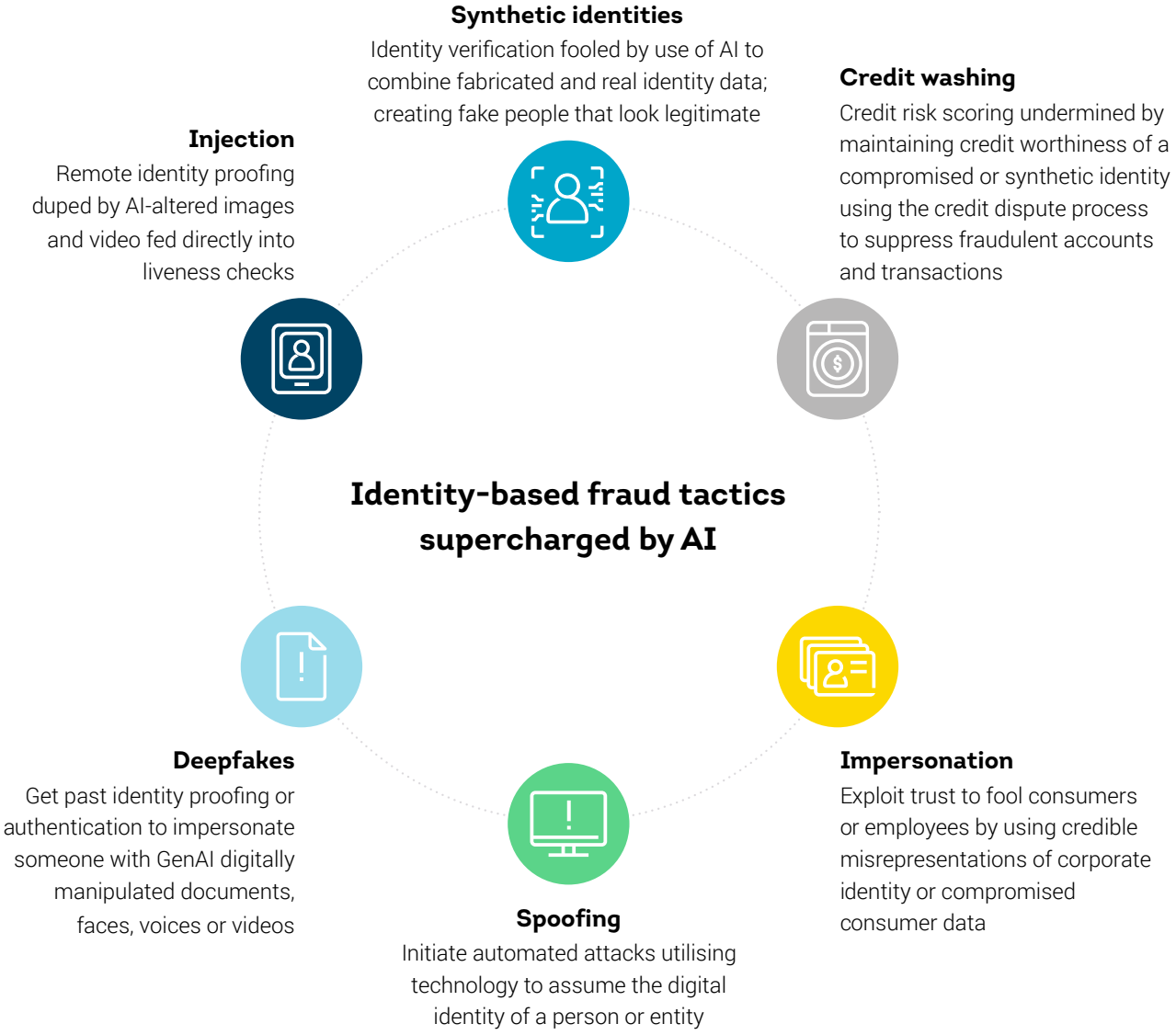
Are Your Customers Real?

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

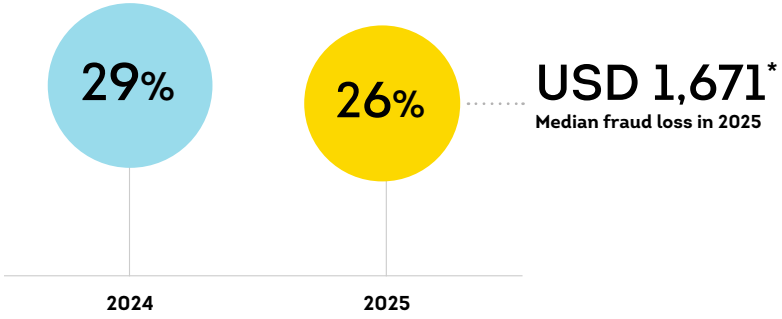
Gen Z most susceptible to losses from trust-based fraud schemes

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

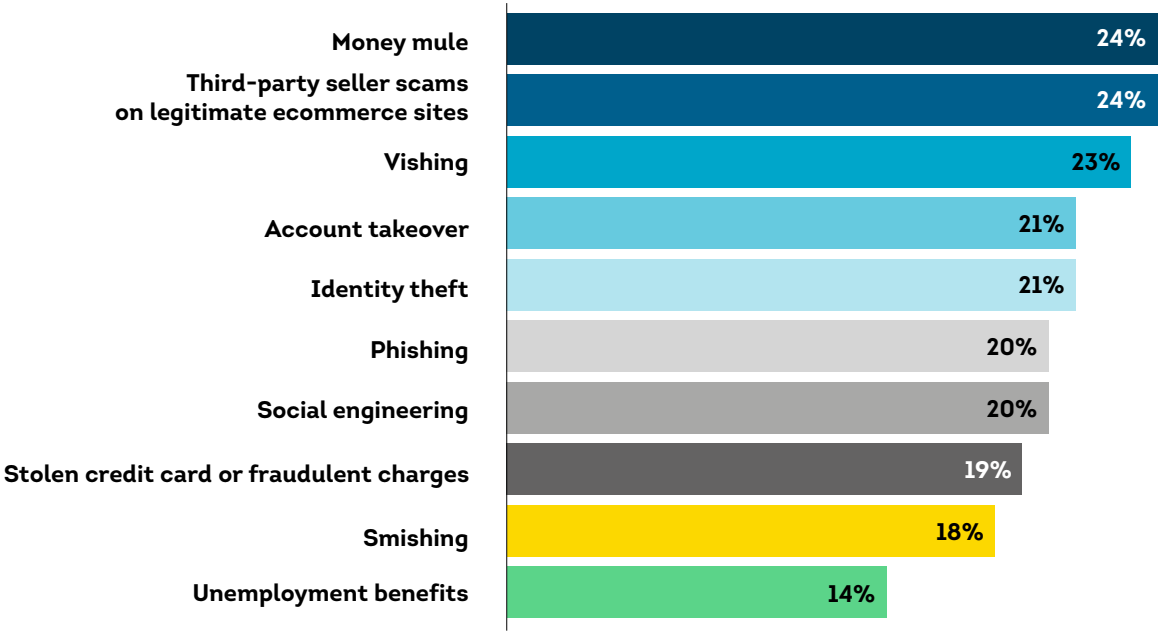


*USD conversion based on currency exchange value on Dec. 29, 2025

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

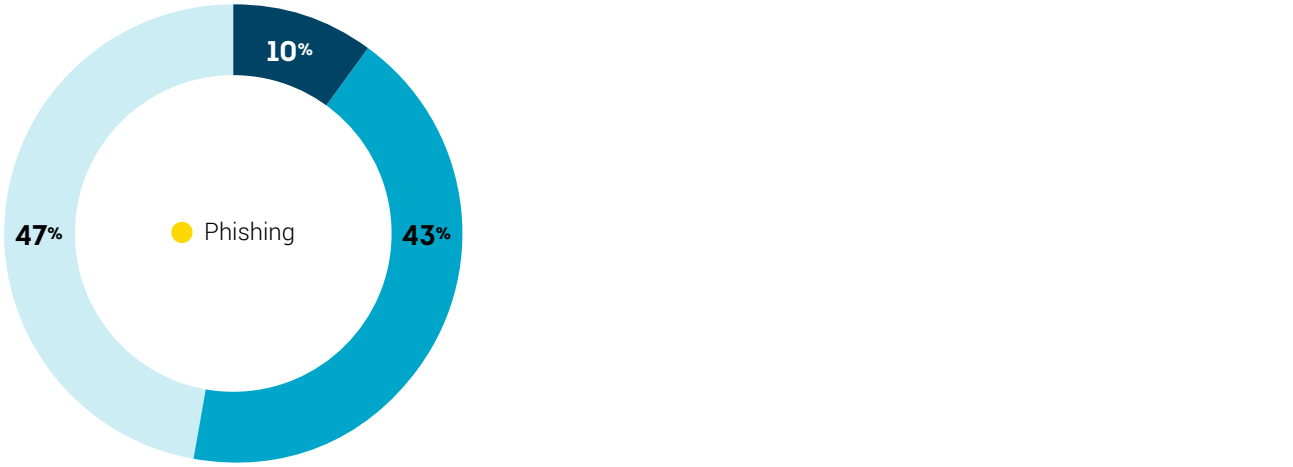
Identity-exposing scams dominate consumer reported fraud

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

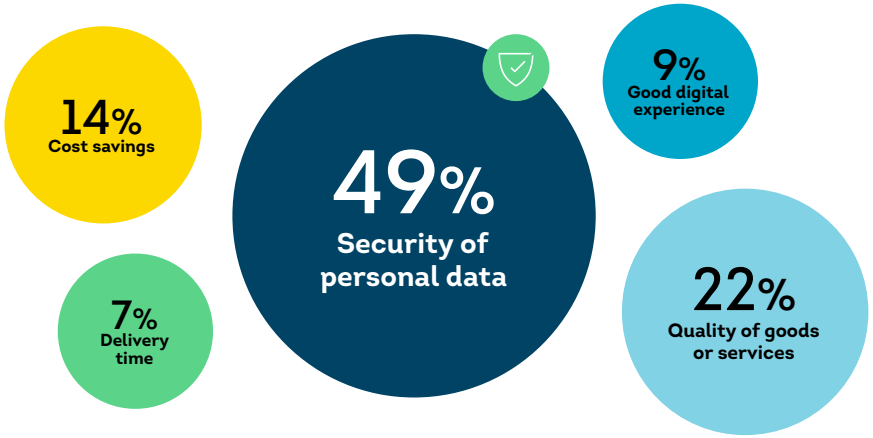
Safe and seamless online transactions drive consumer brand preference

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%.

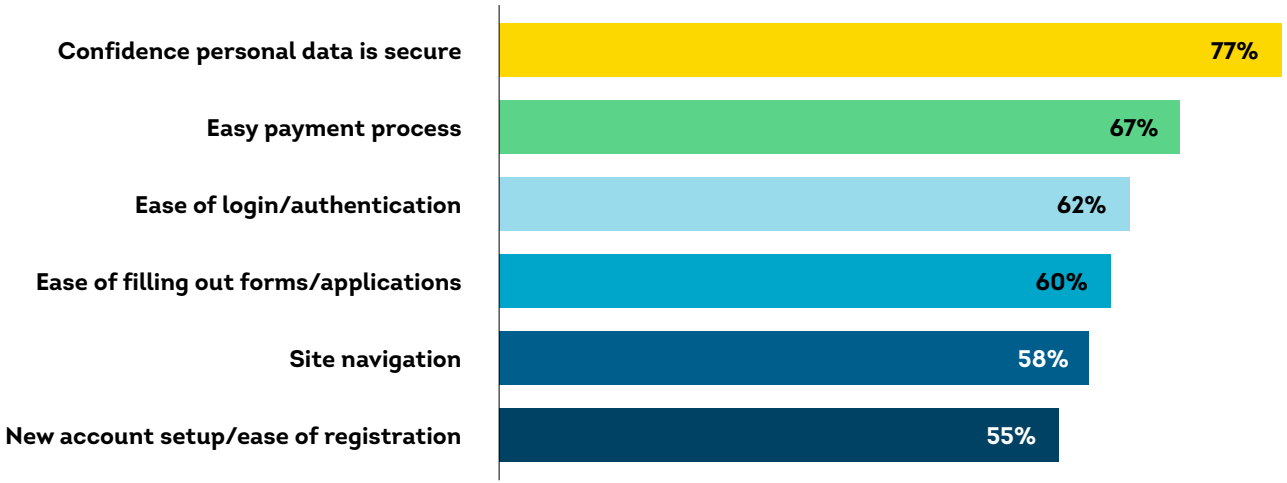
To gain more customers, organisations need to demonstrate trust when it comes to consumer data. About half (49%) of consumers ranked personal data security as the highest expectation or quality in preferred online companies. Not only that, over three-quarters (77%) said confidence their personal data 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

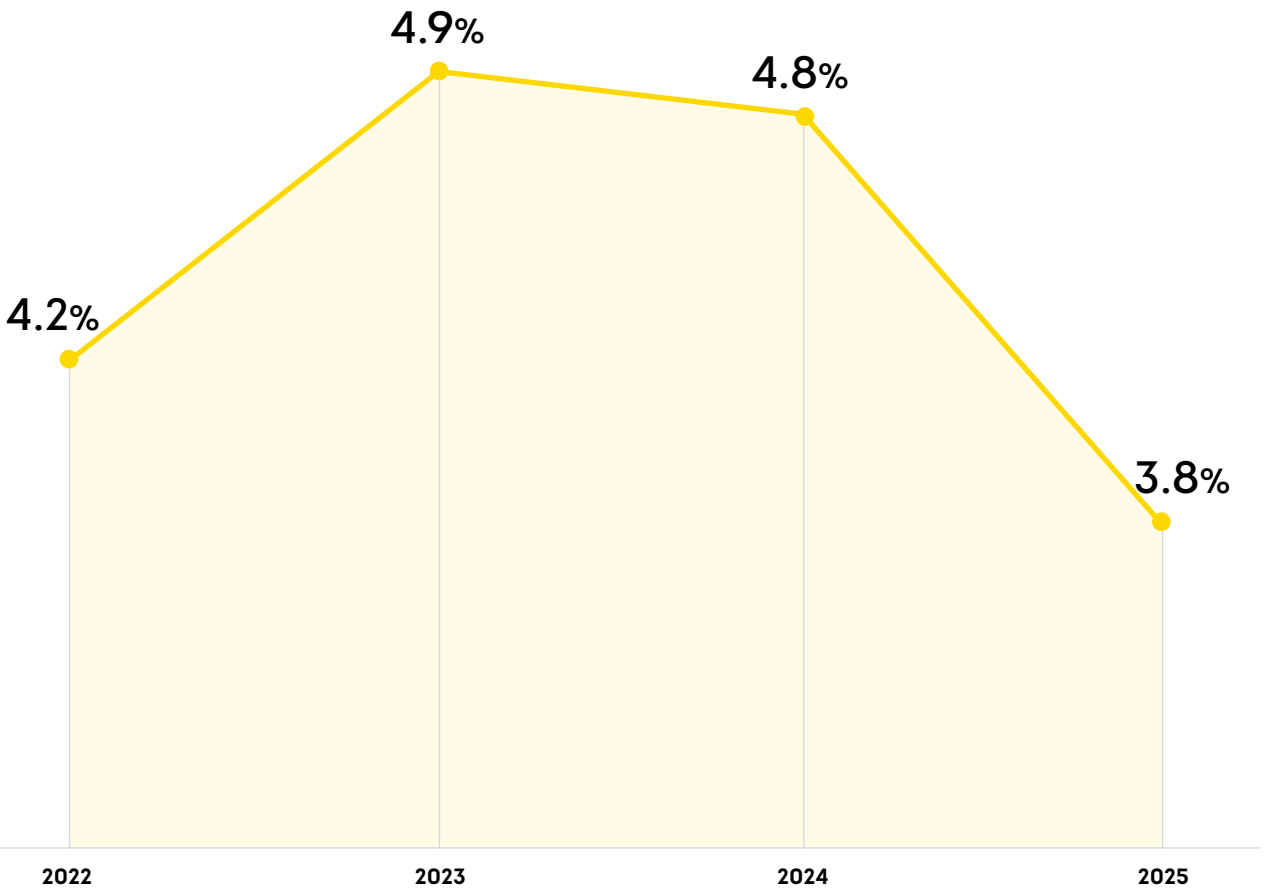
Digital Fraud Trends

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

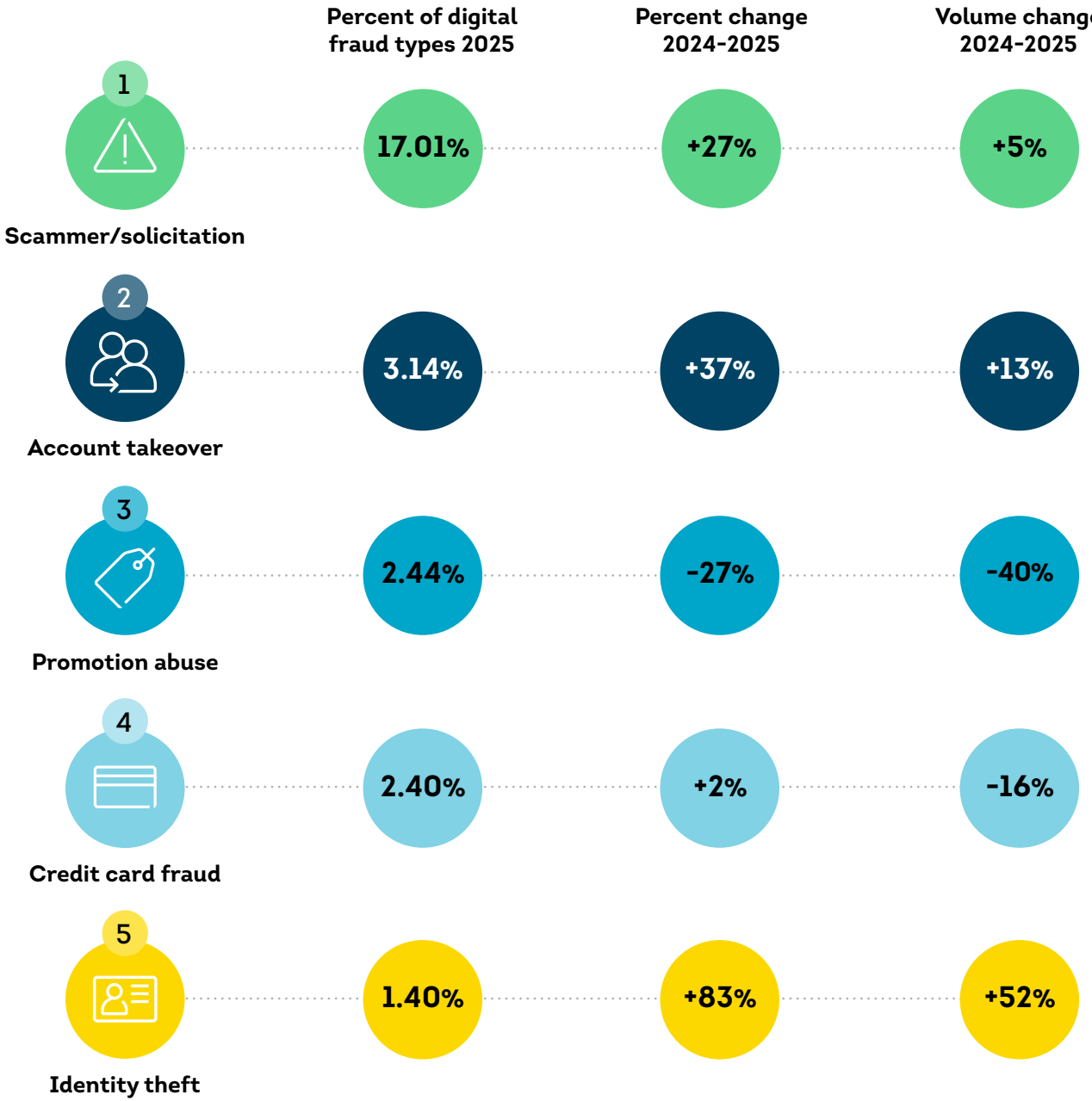
TransUnion

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

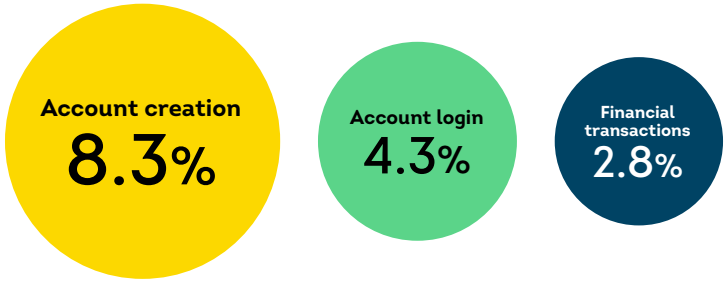
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

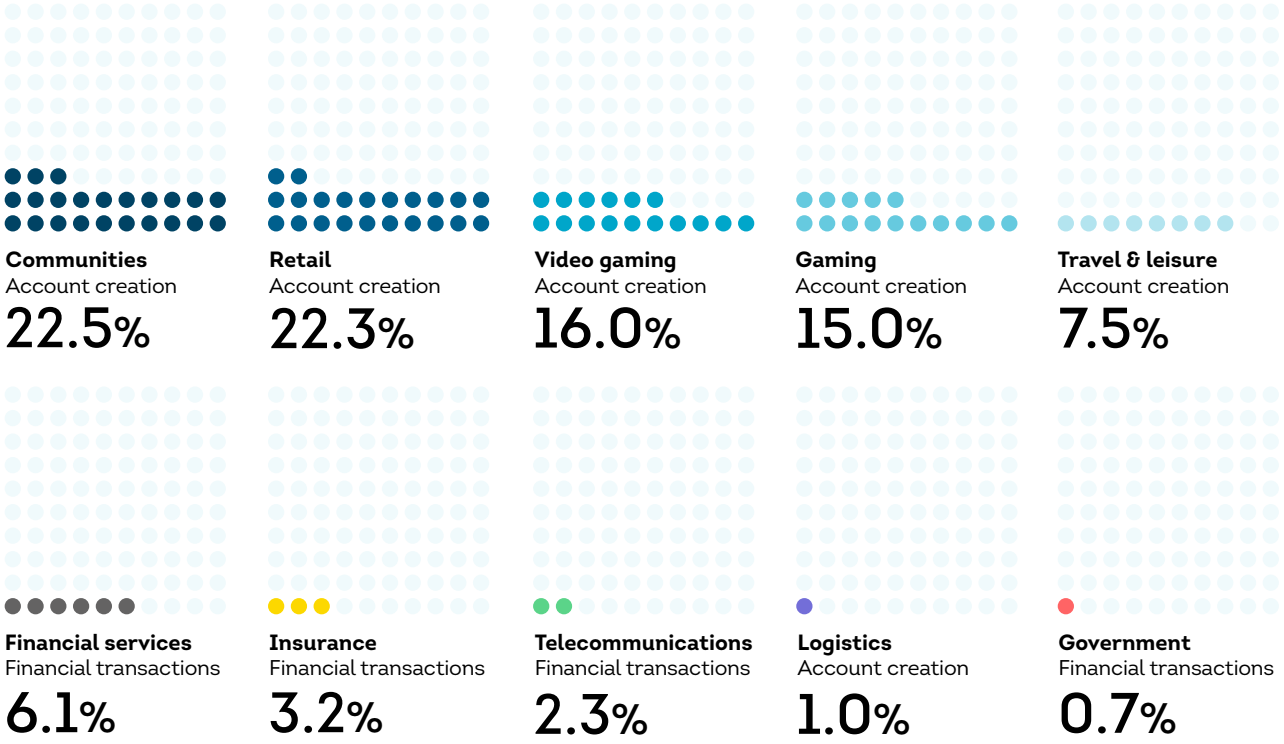
Percentage of each attempted transaction type suspected to be digital fraud in 2025



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

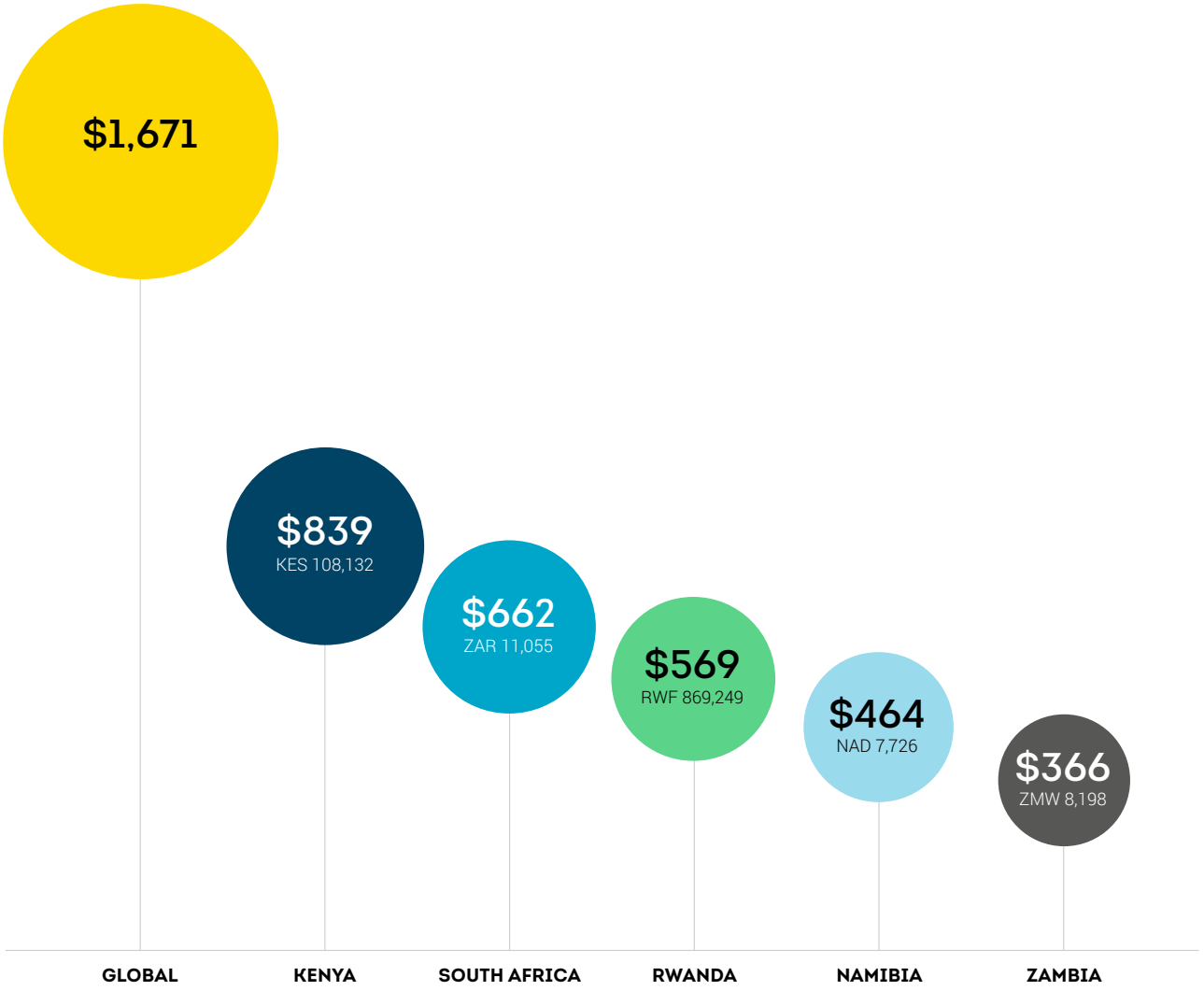
African fraud losses lower than global average but still significant

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



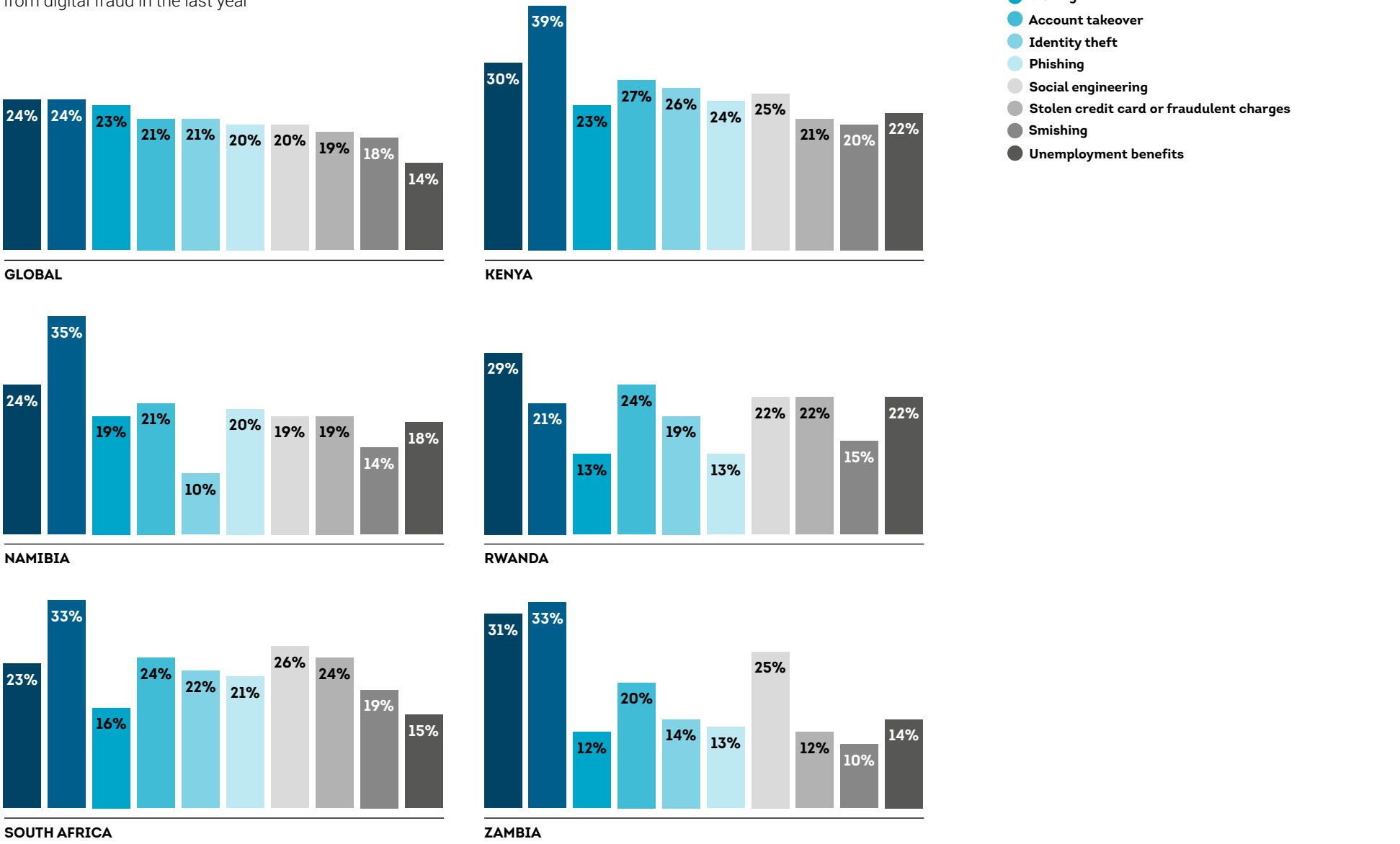
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

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

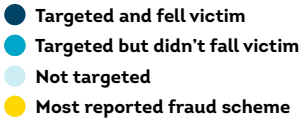
Fraud attempts target majority of African consumers, with smishing most common

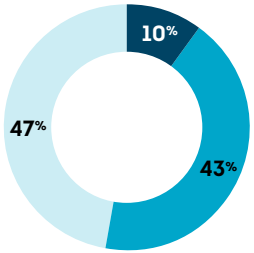
In Africa, a large share of consumers said they faced frequent fraud attempts, with most reporting they were targeted by digital fraud attempts from August to December 2025 but avoided falling victim. Kenyan and Zambian consumers reported the highest rates of being targeted but not falling victim in 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.

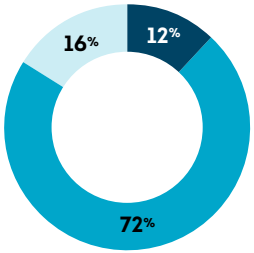
Consumers Targeted With Fraud

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

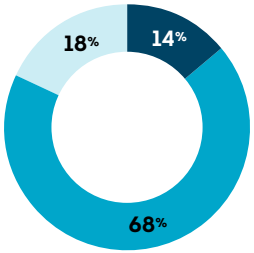




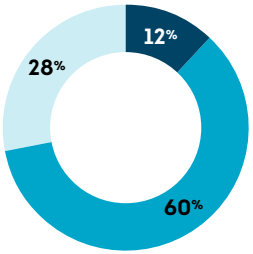
GLOBAL
Phishing



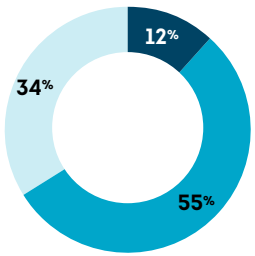
KENYA
Smishing



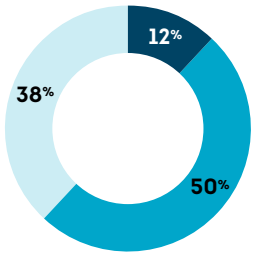
ZAMBIA
Smishing



RWANDA
Phishing



NAMIBIA
Vishing



SOUTH AFRICA
Third-party seller scams on legitimate ecommerce sites

Source: TransUnion consumer survey

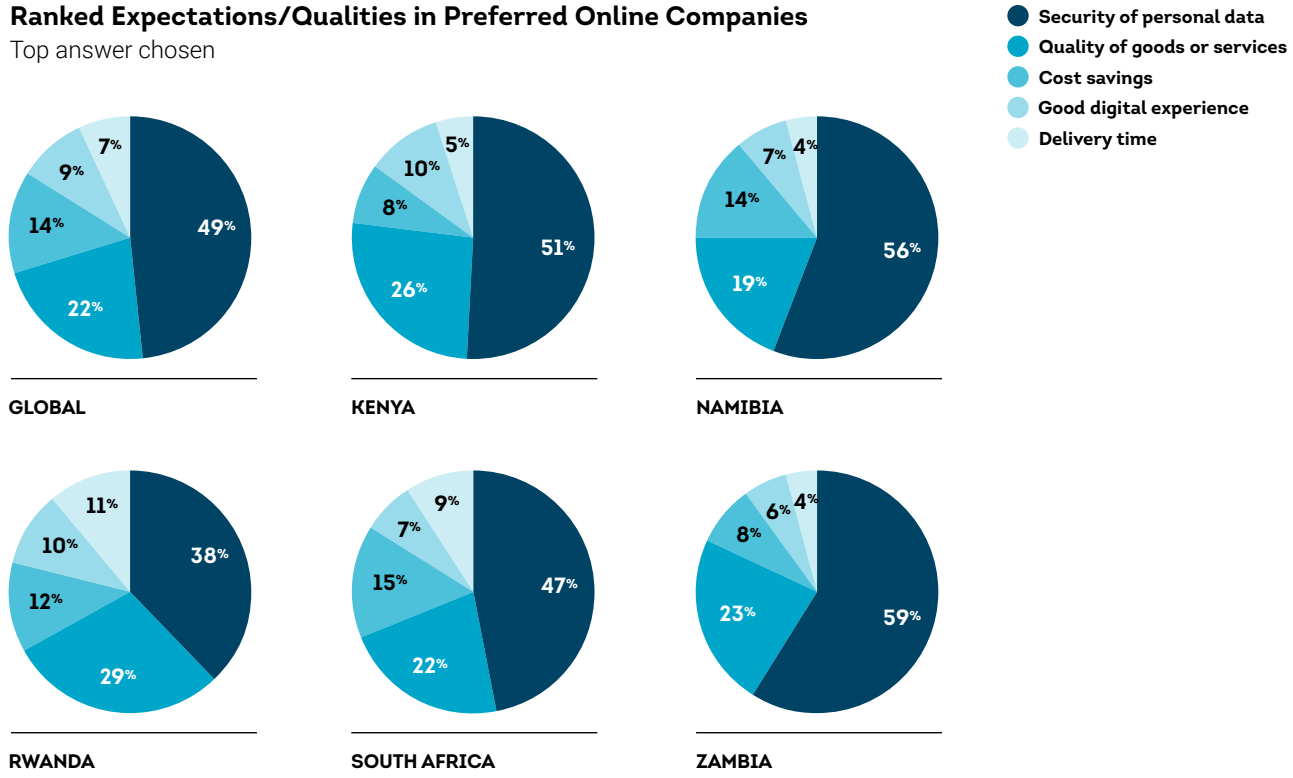
TransUnion

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

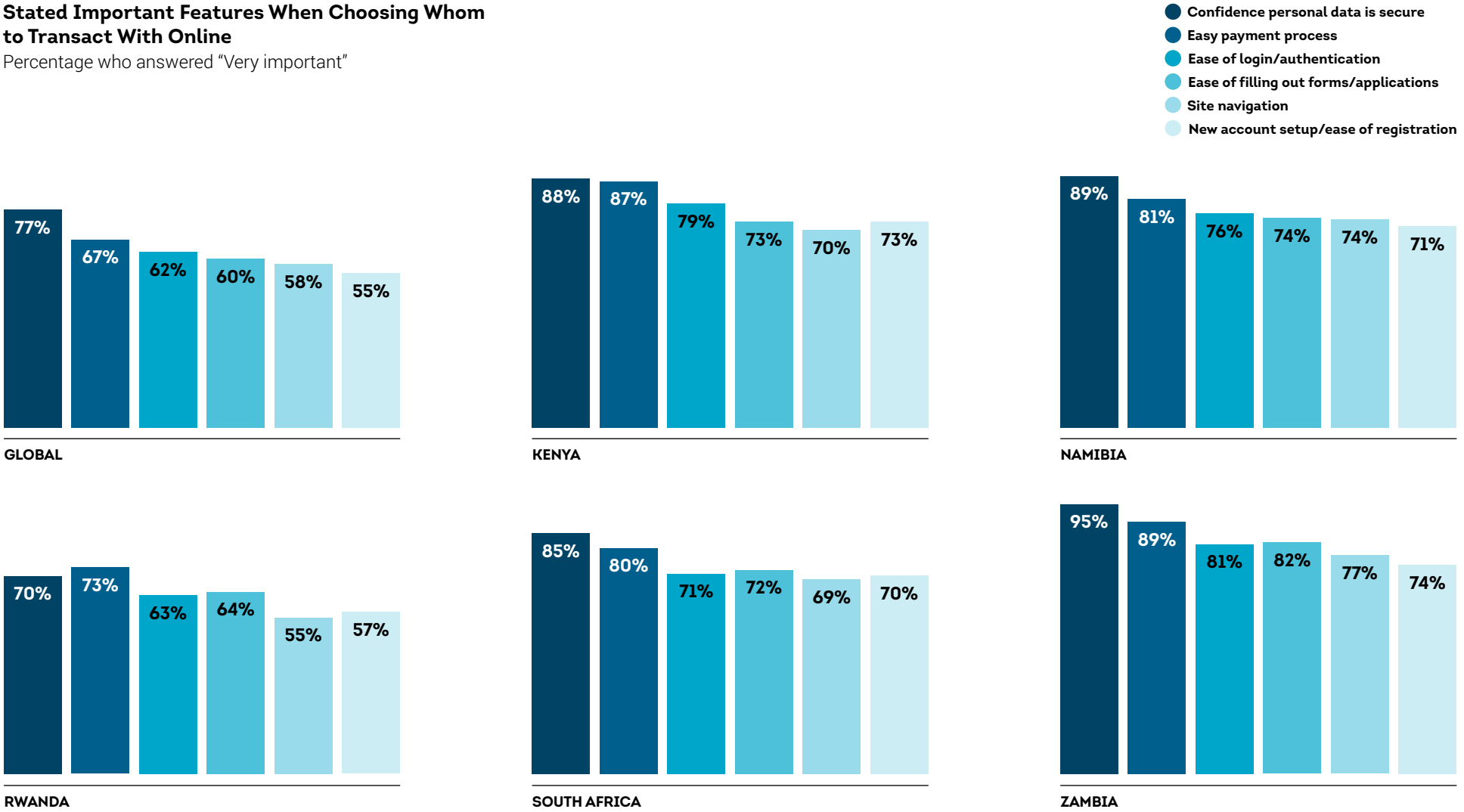


Source: TransUnion consumer survey

TransUnion

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

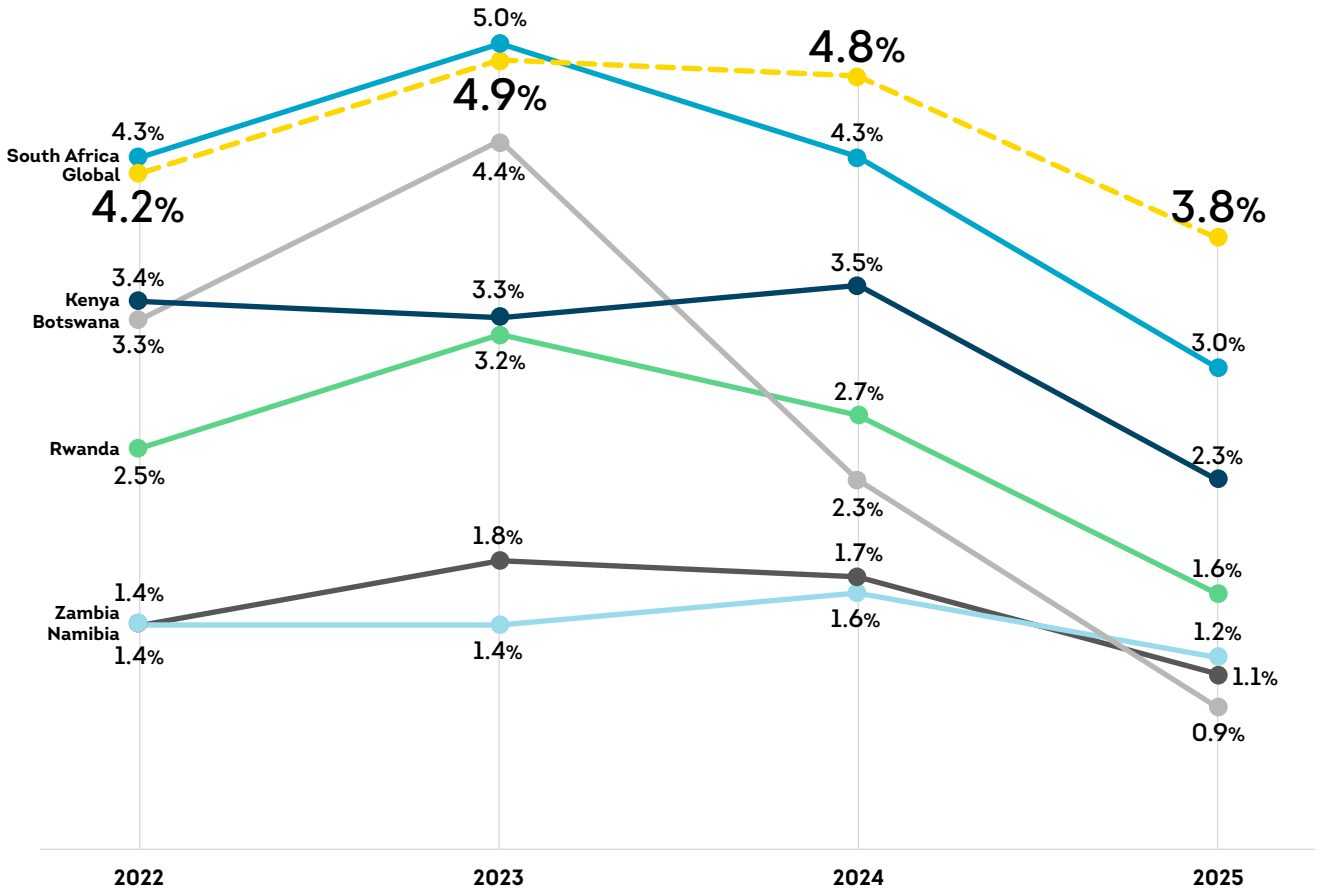
Digital Fraud Trends

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

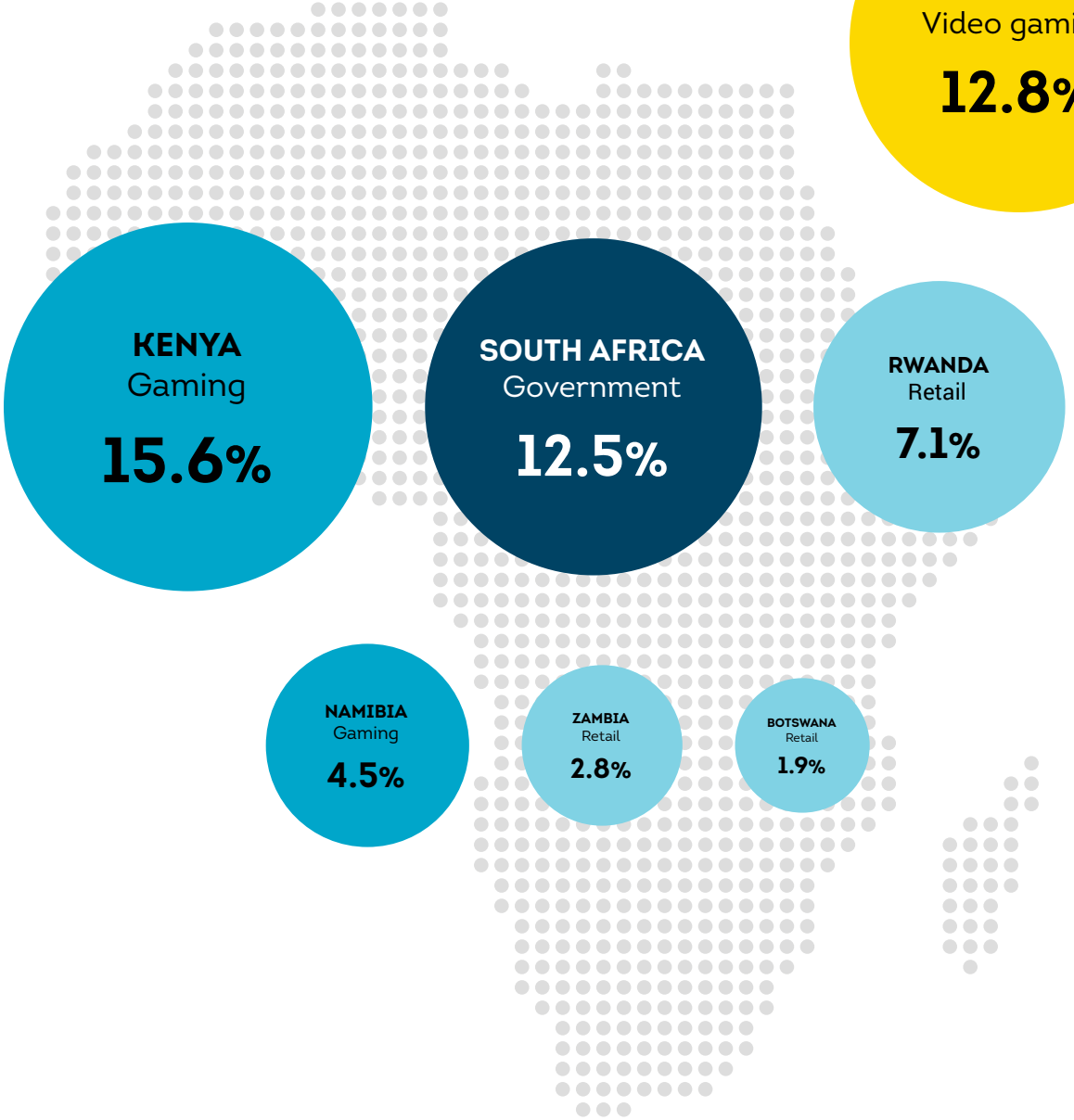
Industries targeted by fraud vary widely across Africa

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

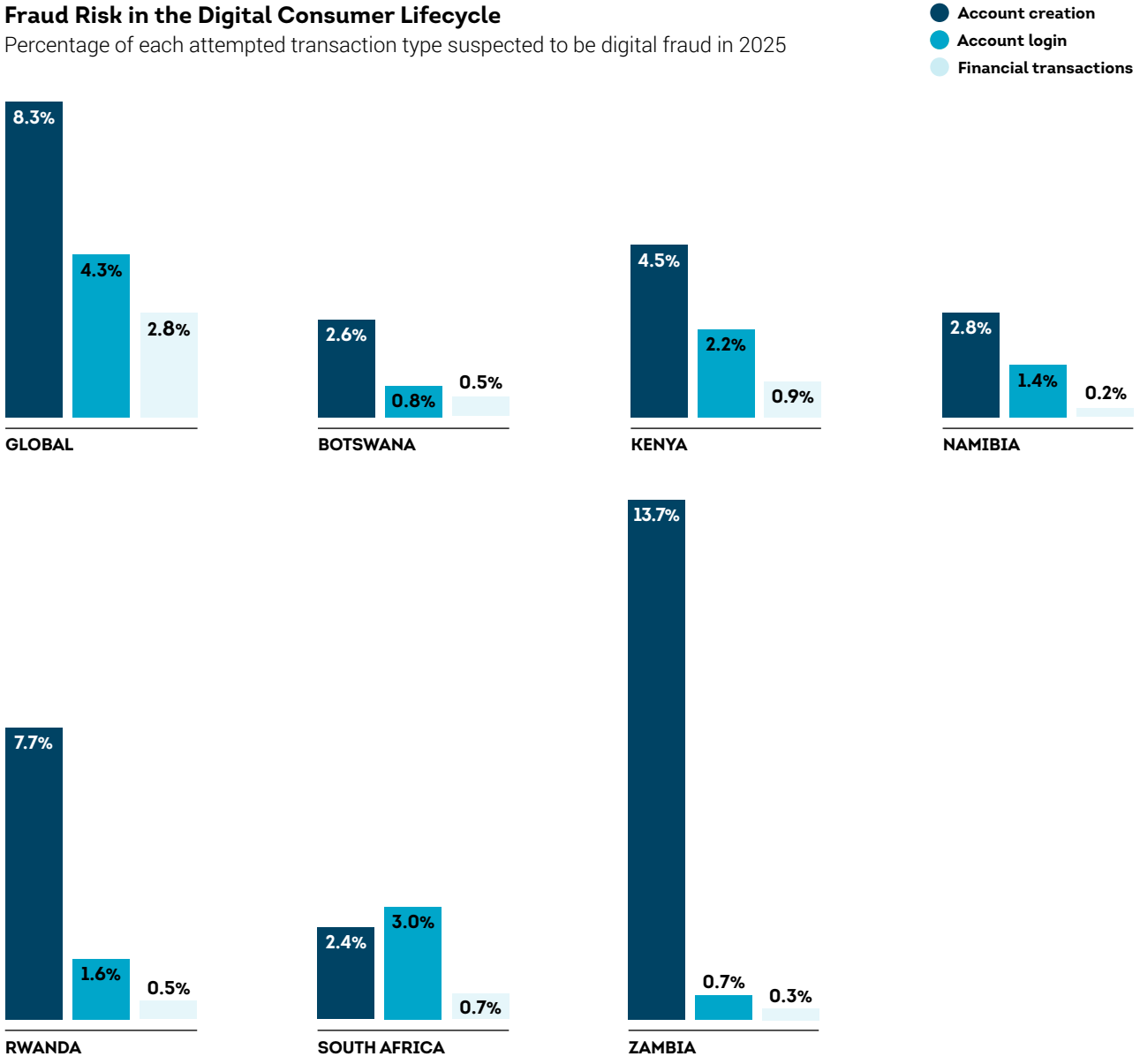
Account creation: Account signup, registration and loan origination

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


INDIA
HONG KONG
PHILIPPINES
ASIA

Asia Overview

India faces a heightened fraud landscape where median consumer losses were 36% above the global median. While the rate of suspected digital fraud declined to 7.1% in 2025, it was almost double the global rate, indicating persistent vulnerability — even as verification helps keep account creation and financial transaction fraud below global benchmarks.

Hong Kong showed a contrasting pattern of low-frequency but high-severity fraud. The suspected digital fraud rate was 2.8% last year, below the global average. However, consumer reported losses were higher when incidents occurred. Risk was concentrated at early consumer lifecycle stages, particularly account login, while downstream financial transaction fraud was low.

In the Philippines, fraud pressure is driven more by scale than severity. Median losses were below global levels, but exposure was high due to widespread targeting across digital channels. Suspected digital fraud declined in 2025 yet remained above the global rate. Risk was concentrated around account login in the consumer lifecycle and the logistics industry.

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

KEY TAKEAWAYS

Fraud losses show sharp market contrasts

USD 6,155, 2,265 and 850

Hong Kong, Indian and Filipino consumer-reported median fraud loss, respectively, among those who said they lost money to digital fraud in the last year.

High consumer targeting persists, but victimisation varies by market

72%, 59% and 47%

of Filipino, Indian and Hong Kong consumers, respectively, who said they were targeted by digital fraud from August to December 2025.

13%, 11% and 6%

of Indian, Filipino and Hong Kong consumers, respectively, who said they fell victim to digital fraud from August to December 2025.

Suspected digital fraud higher than globally; risk focused at login

5.9%

rate of suspected digital fraud in Hong Kong, India and the Philippines combined in 2025, higher than the 3.8% global average.

10.1%, 6.1% and 3.9%

of all digital account login transactions that were suspected of digital fraud in Hong Kong, the Philippines and India, respectively, in 2025; the riskiest part of the consumer lifecycle for all of those markets.

TransUnion

Consumer Fraud Experiences

Fraud losses and reasons behind it vary widely by market

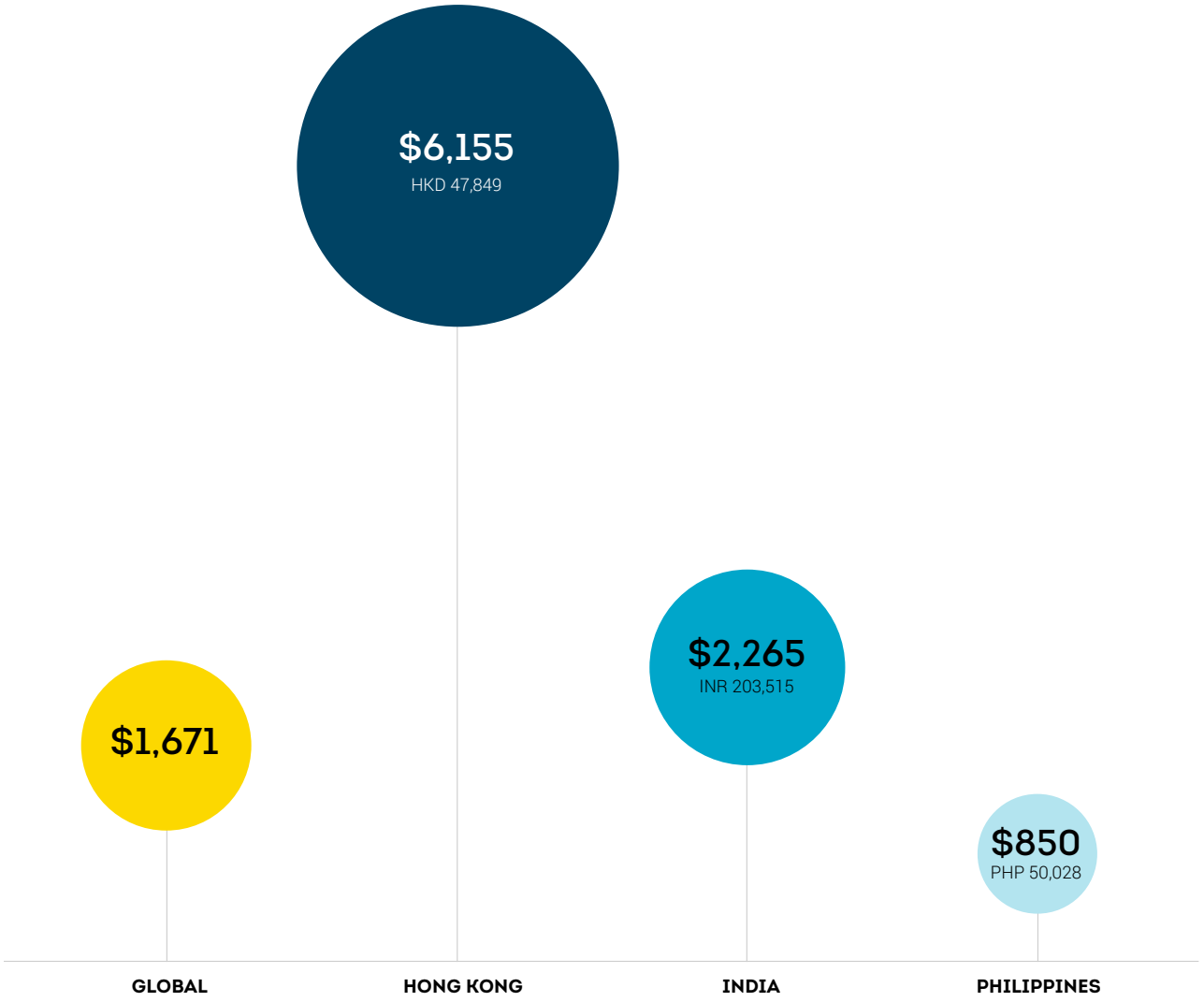
Indian consumers who said they lost money in the last year due to digital fraud reported a median loss of USD 2,265 (INR 203,515) in that period — 36% above the global median. They reported losing money in the past year due to schemes like phishing, vishing, smishing and third-party seller scams on legitimate online retail websites, all exceeding global levels. Separately, lower reported monetary fraud loss due to stolen credit cards or fraudulent charges in India and globally may reflect broad adoption of chip-based cards.

Hong Kong consumers who said they lost money in the last year due to fraud reported a median fraud loss of USD 6,155 (HKD 47,849). This signals higher-value incidents with reported monetary fraud loss led by identity theft, vishing and money mule activity.

Filipino consumers who said they lost money in the last year due to fraud reported a lower median loss of $850 (PHP 50,028) than other Asian countries, led by money mule activity and third-party seller scams on legitimate online retail websites. Together, these patterns highlight diverse consumer fraud loss drivers across Asia, with identity-led and commerce-linked scams remaining key risks.

Consumer-Reported Fraud Loss

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



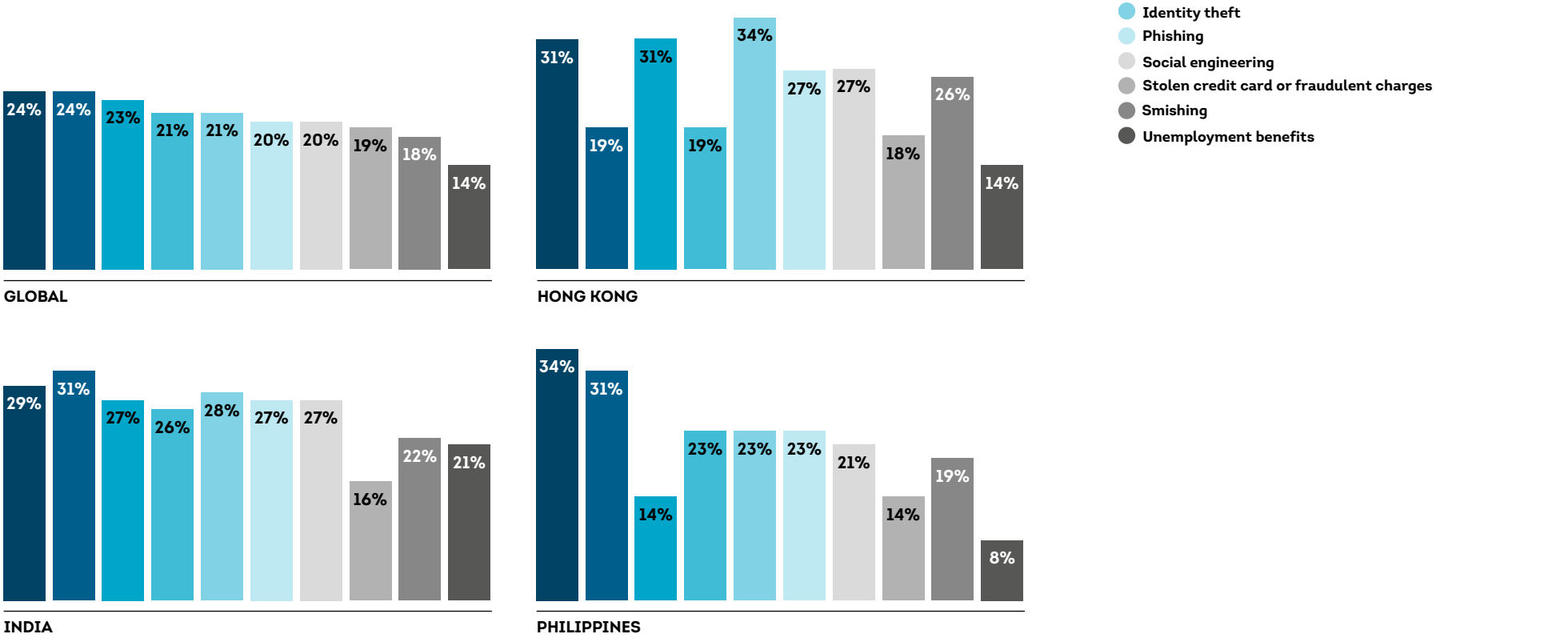
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

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

TransUnion

Despite large differences in fraud exposure, phishing the top scheme across the region

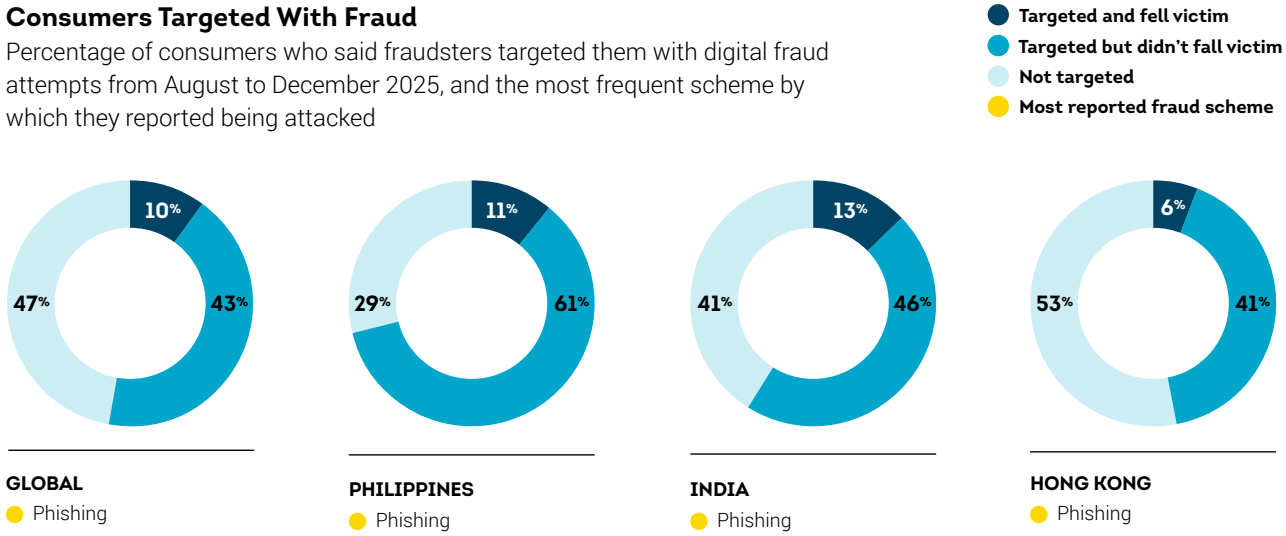
Indian consumers reported higher than global targeting and victimisation when asked if they were targeted by digital fraud attempts in the last three months, with 59% saying they were targeted and 13% of them reporting they fell victim. Among those who said they were targeted, phishing was the most reported scheme, reflecting broad exposure and gaps in financial literacy that increased susceptibility to digital deception.

Hong Kong showed lower victimisation but higher loss severity. While 53% said they were not targeted and only 6% reported falling victim (below the global average of 10%), median losses among those who said they lost money to fraud in the last year reached USD 6,155 during this period as reported above. Phishing was the most frequently reported scheme in Hong Kong, possibly due to a mobile-first environment where consumers routinely engage with digital communications, creating opportunities for impersonation attempts despite strong consumer awareness.

In the Philippines, 72% reported being targeted and 11% falling victim — both higher than the global average. Phishing was the top reported scheme in the Philippines too, possibly driven by extensive use of mobile channels for commerce and social interaction, resulting in high contact volumes and sustained attack frequency. As mentioned above, Filipino fraud losses tend to be lower, but repeated attempts contributed to elevated exposure across the market.

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

Security of personal data is the defining expectation across Asia, with ease of use a key complement

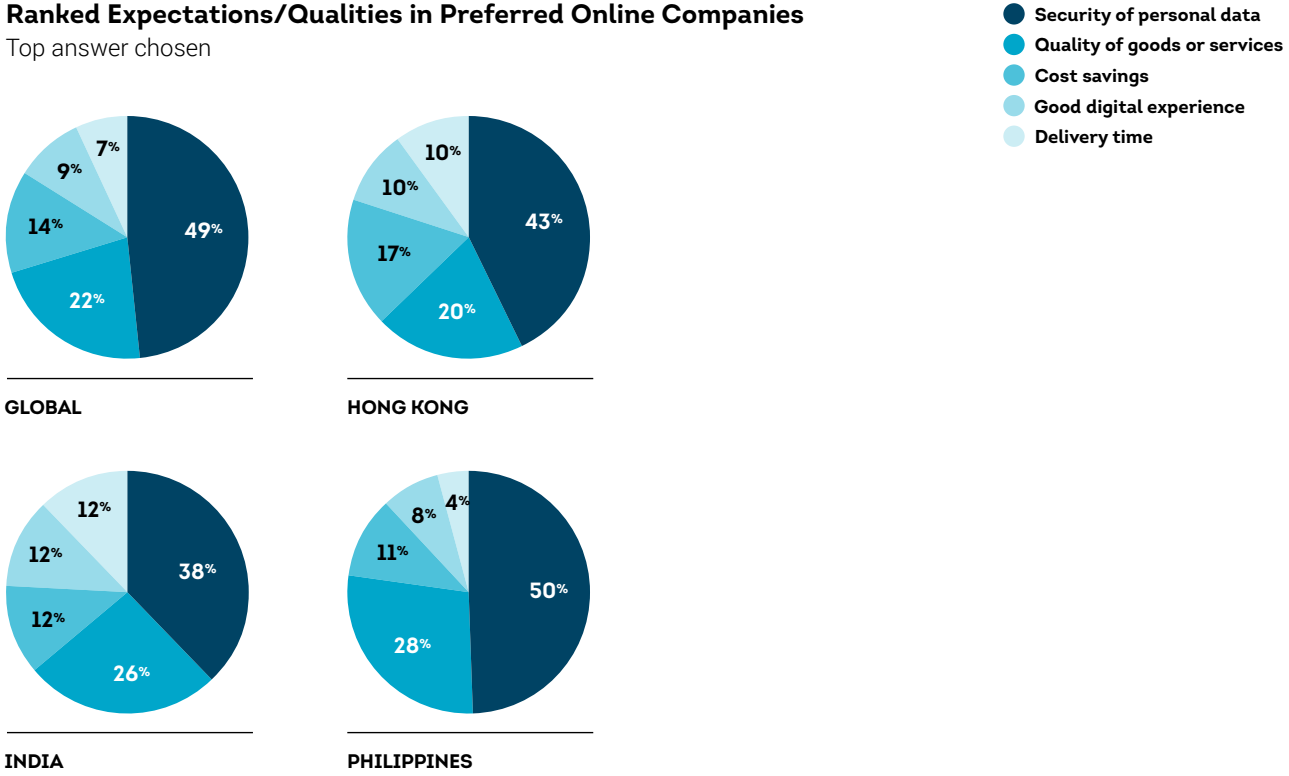
Security and convenience work together as core decision factors, highlighting a digital environment where trust and low friction are equally central to consumer choice. In India, security of personal data (38%) and quality of goods and services (26%) were the top expectations they consider when deciding what online company to do business with.

When asked which features matter most when choosing whom to transact with online, Indians said security of personal data (67%) and an easy payment process (65%) were very important. Those were both below global benchmarks, indicating room to strengthen trust and usability in digital interactions.

Hong Kong consumers also placed security first (43%) followed by quality of goods and cost savings when asked their top expectations when deciding what online company to do business with. "Very important" features when choosing whom to transact with online — such as confidence personal data is secure (52%) and ease of use with login/authentication and site navigation — scored lower than global norms.

In the Philippines, however, security of personal data (50%) had a higher percentage than other Asian countries when Filipinos were asked their top expectations when deciding what online company to do business with. This was reinforced with answers around which features matter most when choosing whom to transact with online. Filipinos said confidence personal data is secure (85%), an easy payment process (80%) and ease of login or authentication (74%) were very important.

Ranked Expectations/Qualities in Preferred Online Companies
Top answer chosen

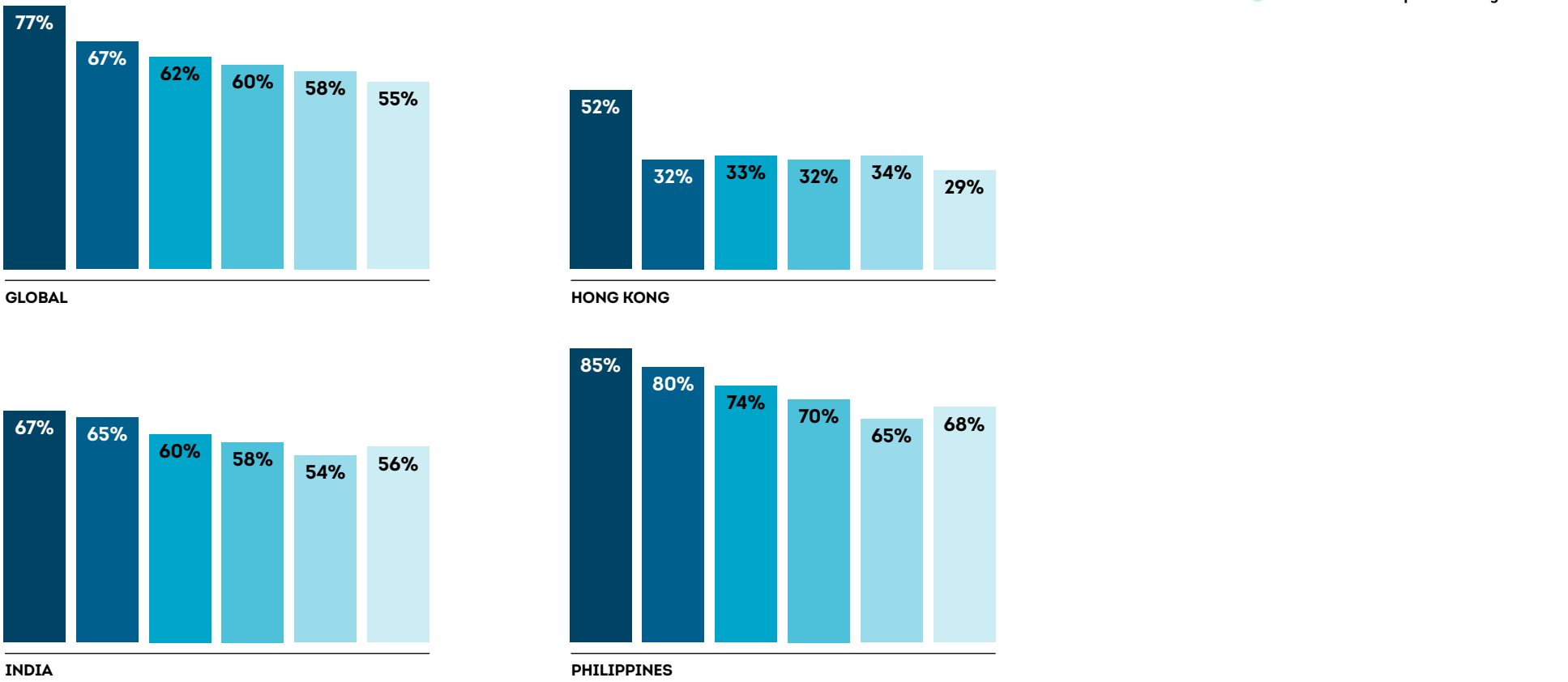


Source: TransUnion consumer survey

TransUnion

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

Suspected digital fraud in region higher than globally despite declines

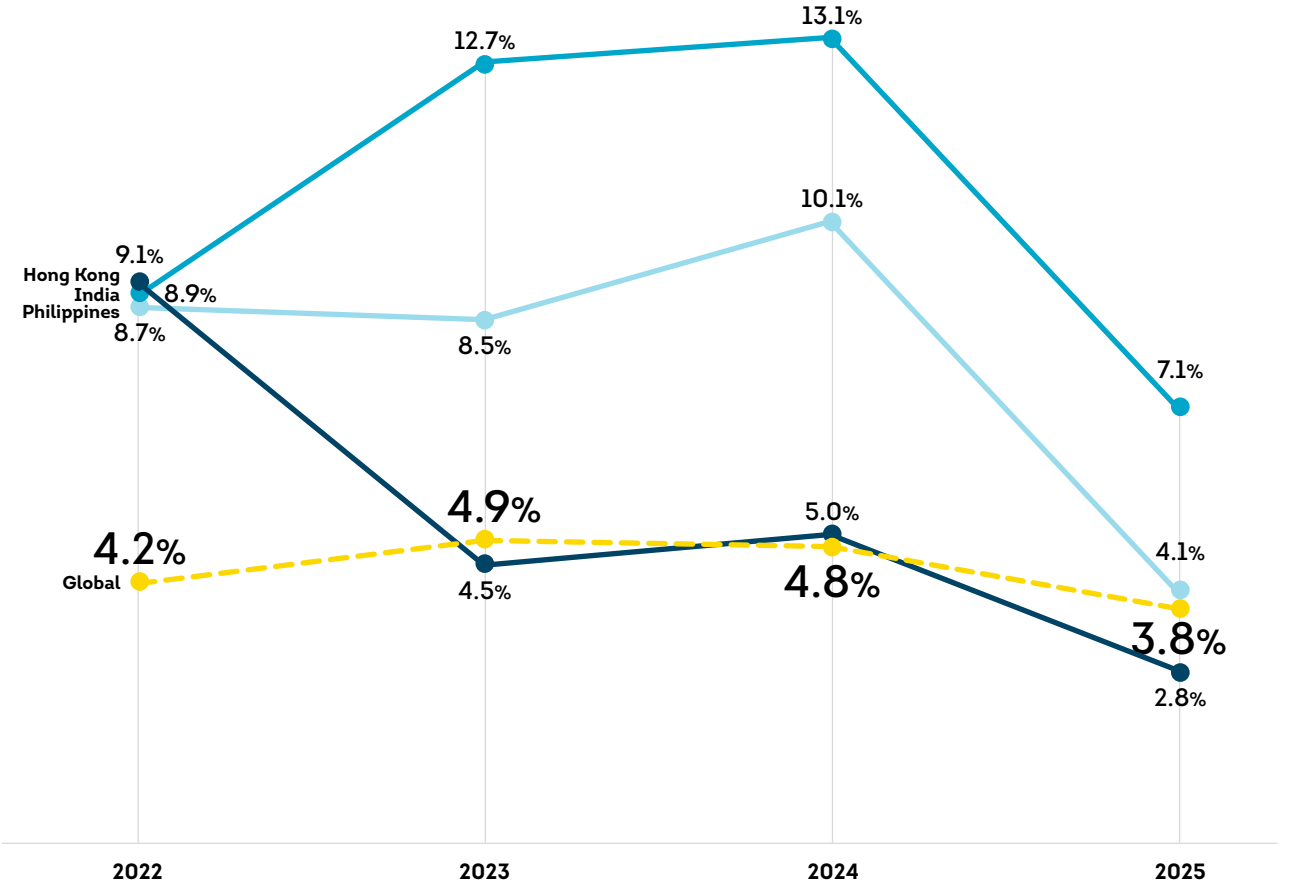
Even as suspected digital fraud attempts decreased across countries analysed in the region, the rate (5.9%) for those countries combined in 2025 still sat above the global rate.

For transactions where the consumer was in India, the suspected digital fraud rate fell sharply to 7.1% in 2025 from 13.1% in 2024, though it remained almost twice the global rate of 3.8%. The decline aligns with sustained government and industry efforts around digital literacy, customer education, phone number verification and cyber intelligence sharing — all contributing to reduced fraud attempts.

Hong Kong also recorded a notable decline in suspected digital fraud, falling to 2.8% in 2025 from 5.0% in 2024, now below global levels. The trend suggests normalisation after prior volatility, with fewer incidents but continued severity when cases occur.

In the Philippines, the suspected digital fraud rate dropped to 4.1% in 2025 from 10.1% the previous year. While still slightly above the global rate, the reduction reflects easing pressure after years of elevated fraud activity. Together, the data indicates broad improvement across the region, even as exposure levels and fraud dynamics vary by market.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

TransUnion

Digital fraud attempts in region concentrate in high-engagement and transaction-heavy sectors

For transactions where the consumer was in India, logistics emerged as the sector with the most suspected digital fraud attempts in 2025 at 16.3%, ahead of telecommunications, insurance, video gaming, communities, financial services, retail and travel & leisure (in that order).

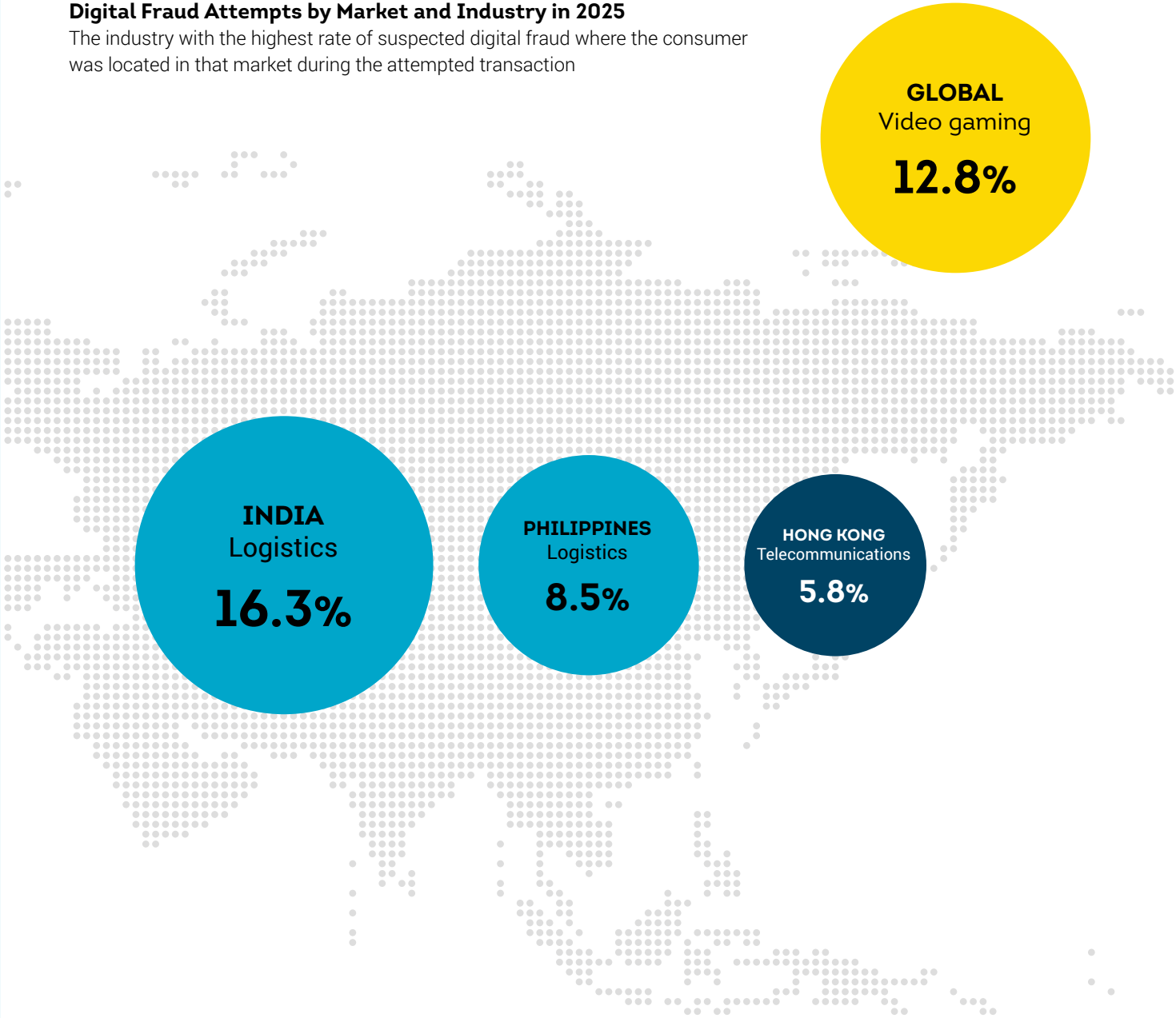
In Hong Kong, telecommunications recorded the highest level of suspected digital fraud attempts in 2025 at 5.8%, exceeding the global benchmark and outpacing sectors like communities and financial services.

In the Philippines, logistics led with an 8.5% suspected digital fraud rate in 2025, reflecting the central role of delivery coordination, payment updates and customer communication in the country's commerce-driven digital ecosystem.

These findings show fraud attempts across the region tend to cluster in industries with high digital engagement or transaction flows.

Digital Fraud Attempts by Market and Industry in 2025

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



Source: TransUnion global intelligence network

TransUnion

Fraud risk in digital consumer lifecycle concentrates highest at login

Across all Asian markets analysed, fraud pressure last year was concentrated before or at the moment of digital access — particularly during authentication — while downstream transaction activity remained comparatively resilient.

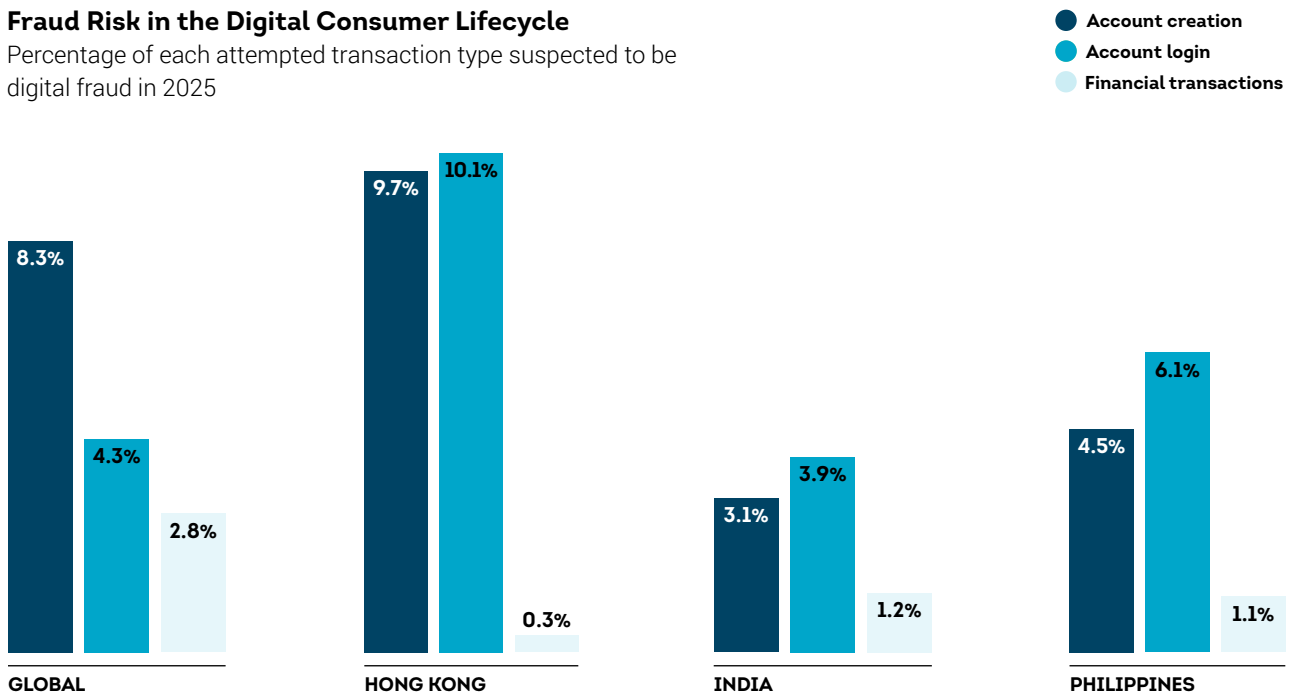
For transactions where the consumer was in India, fraud penetration across the digital consumer lifecycle was lower than global levels, with suspected digital fraud at account creation (3.1%), account login (3.9%) and financial transactions (1.2%) in 2025. Account creation suspected digital fraud was less than half the global average, reflecting widespread use of mobile numbers for verification — which reduces exposure at onboarding. Login carried the highest risk within India's digital lifecycle but still below global benchmarks, indicating relatively strong controls across early access stages.

In Hong Kong, the account login stage presented the greatest exposure in 2025, with 10.1% of digital login attempts suspected to be fraudulent, slightly above the 9.7% at account creation. Financial transaction fraud was significantly lower at 0.3%, suggesting strong protection once users are authenticated.

The Philippines showed a similar pattern: 6.1% suspected digital fraud attempts at login, 4.5% at account creation and lower exposure at financial transactions (1.1%) in 2025.

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

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

TransUnion


UNITED KINGDOM
SPAIN
EUROPE

Europe Overview

Consumers are increasingly digital-first, with high expectations of trust across their digital interactions. And while nearly half of all Spanish and UK consumers surveyed said they conduct more than half of their transactions online, a significant barrier to optimal conversion is the fear of fraud and misuse of personal data. The fraud threat is evolving rapidly, with bad actors leveraging increased democratised access to technology to leverage deepfakes, document manipulation, synthetic identity creation and bot attacks to expand their threat vectors against consumers and businesses.

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

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

KEY TAKEAWAYS

Trust in security of personal data is a top factor for consumers online

76% and 71%

of UK and Spanish consumers, respectively, who said confidence their personal data will not be compromised was very important when choosing organisations to transact with online.

Reduced digital fraud rates may mask new threat vectors

2.6% and 2%

suspected digital fraud rates in 2025 for attempted transactions where the consumer was in Spain and the UK, respectively, continuing a recent downward trend. This contrasts with the rising threat of fraud being reported across channels.

Schemes consumers claim they lost money to vary by country

27%

of Spanish consumers who said they lost money in the last year to digital fraud reported doing so due to vishing – the highest of any scheme.

26%

of UK consumers who said they lost money in the last year to digital fraud reported doing so due to phishing – the highest of any scheme.

Consumer Fraud Experiences

Consumers report incurring material losses to fraud across a wide range of vectors

Financial losses from fraud are often the first point of reference when assessing its impact. However, as is the overall impact on consumer trust cannot be overlooked.

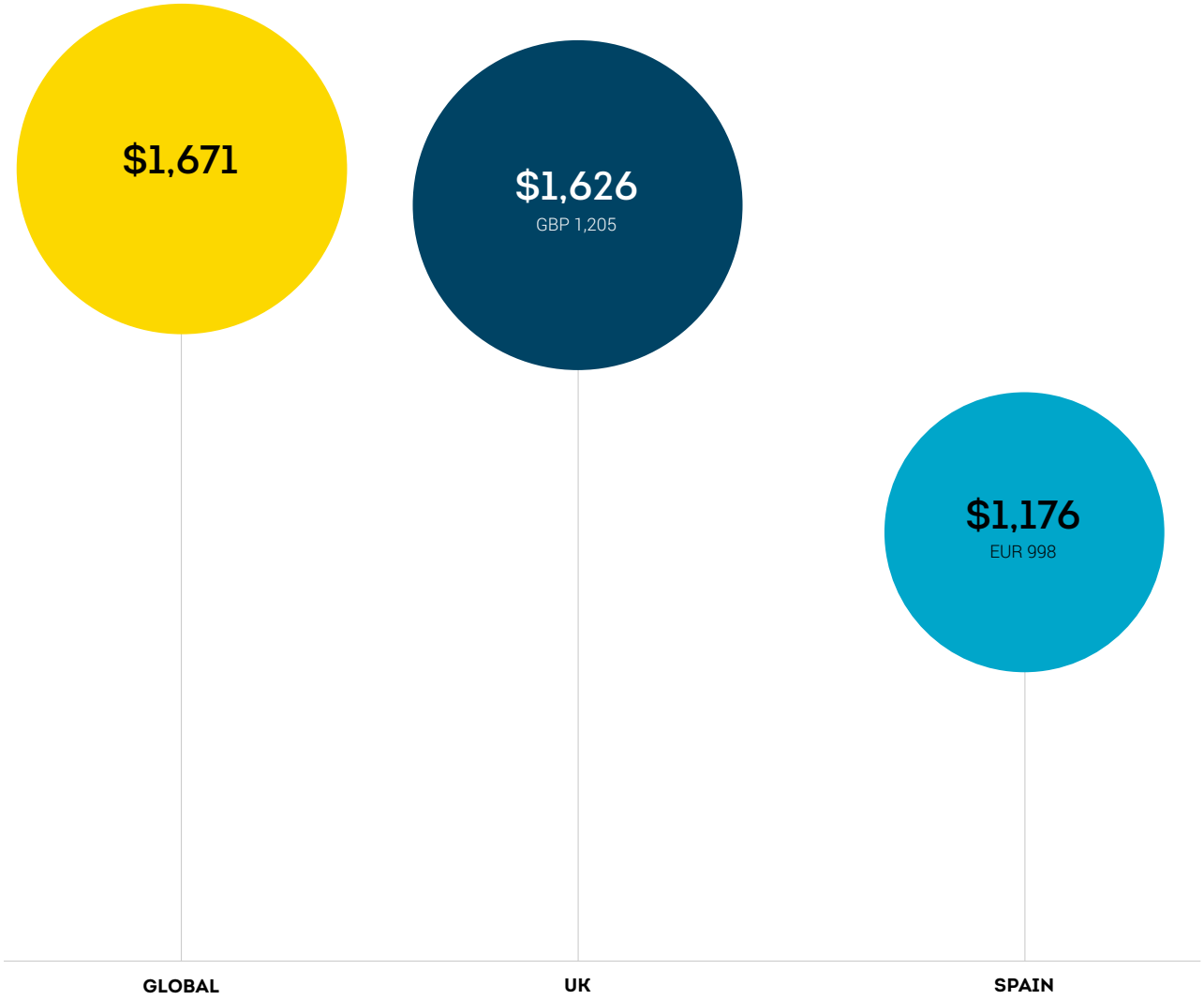
The median consumer-reported fraud loss among those who said they lost money to digital fraud in the past year was USD 1,626 (GBP 1,205) in the UK and USD 1,176 (EUR 998) in Spain. However, when scaled to income, the burden in Spain was higher than the UK and global median.

When it came to what kinds of reported schemes resulted in monetary fraud loss in the last year among those who said they lost money to digital fraud in that timeframe, phishing (26%) was the highest in the UK followed by stolen credit card or fraudulent charges (23%). In contrast, consumers in Spain reported vishing (27%) and smishing (19%) the most.

Regional threats continue to evolve. As strong customer authentication (SCA), European regulatory requirement mandating multi-factor authentication for electronic payment has dampened credential theft, fraudsters have shifted to engineering and authorised push payment (APP) scams. In Spain, "reverse Bizum" where criminals send payment requests disguised as deposits has emerged.

Consumer-Reported Fraud Loss

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



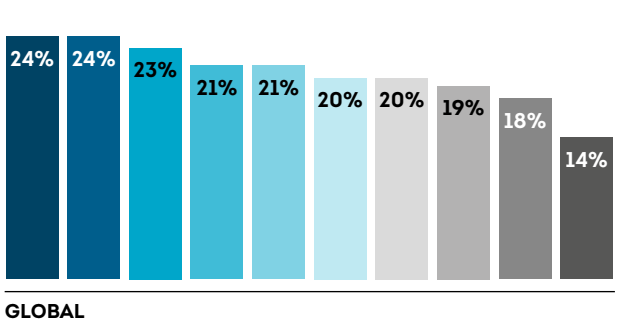
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

Source: TransUnion consumer survey

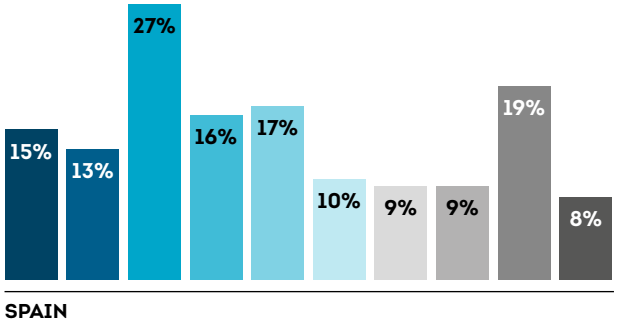
TransUnion

Most Prominent Cause of Fraud Loss

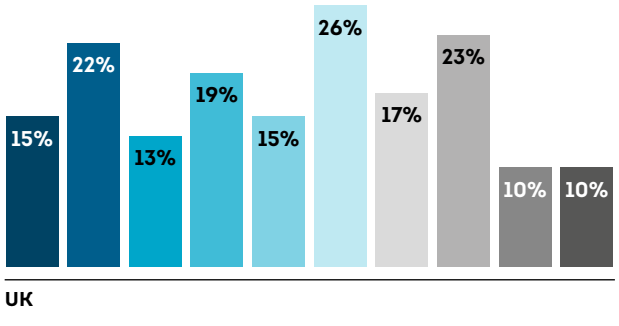
Percentage reporting losing money to these schemes among consumers who said they lost funds from digital fraud in the last year



GLOBAL



SPAIN



UK

- Money mule
- Third-party seller scams on legitimate ecommerce sites
- Vishing
- Account takeover
- Identity theft
- Phishing
- Social engineering
- Stolen credit card or fraudulent charges
- Smishing
- Unemployment benefits

Source: TransUnion consumer survey

TransUnion

More consumers report being targeted and falling victim to fraud

In the UK, consumers reported fraud patterns that closely aligned with those previously identified by TransUnion. Exactly half of consumers said they hadn't been targeted by digital fraud in the last three months, matching the percentage found in the last consumer fraud survey TransUnion conducted from November to December 2024. Notably, 7% stated they were targeted and fell victim to fraud most recently (vs. 6% previously).

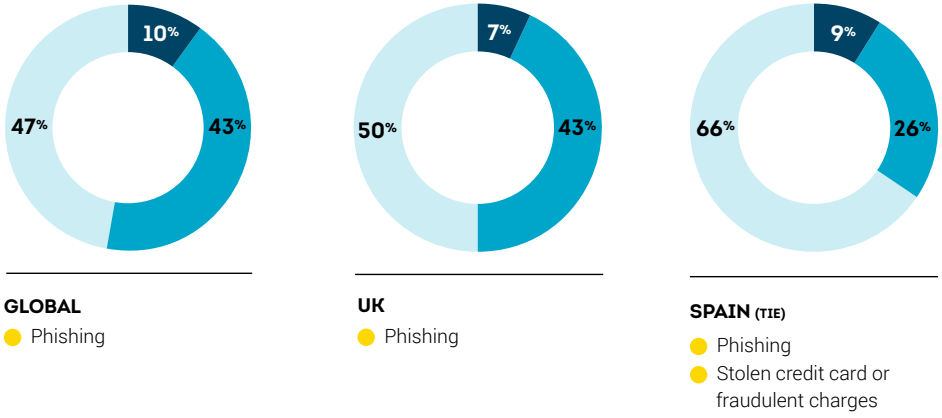
Spain had a higher percentage than the UK of those who said they hadn't been targeted at 66%, up slightly from 65% in 2024, as did those who reported falling victim at 9%, slightly lower than 10% previously.

Among those who said they were targeted, consumers in both countries reported phishing as the top scam, with Spain having it tied with stolen credit card or fraudulent charges. We found phishing is often combined with other attacks; for example, testing both identity-based and payment card vulnerabilities.

Organisations need to continue building trust-based communications and experiences while designing proportionate friction into customer journeys. More targeted programs are often required; for example, promoting fraud awareness to young people should leverage relatable examples and appropriate channels.

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

Security concerns lead consumer online expectations despite strong infrastructure advancements

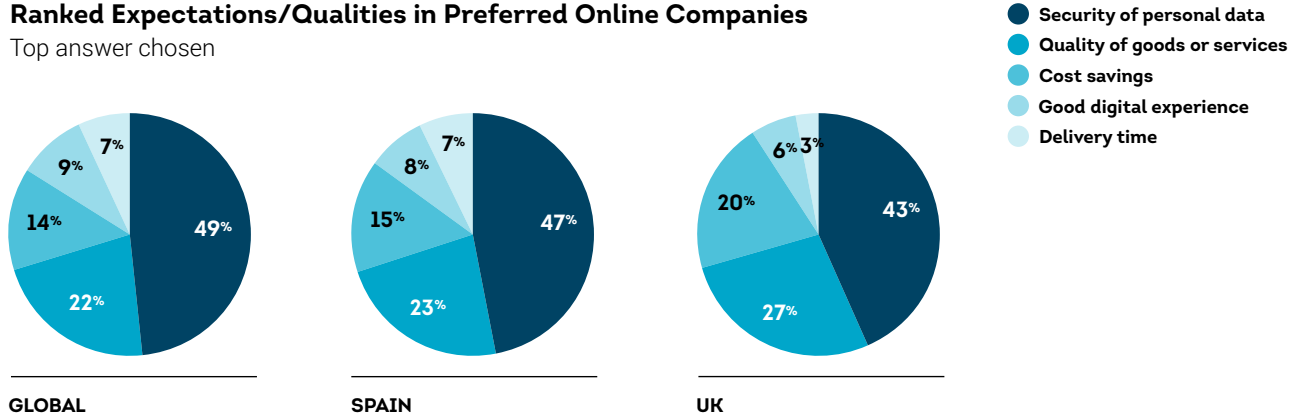
It is widely accepted SCA has reduced credential abuse — even as the threat of social engineering has expanded.

However, when asked to rank the qualities or expectations you consider when deciding what online company to do business with, security was a decisive brand separator in the UK and Spain. The top answer among Spaniards was security of personal data (47%), ahead of quality of goods or services (23%) and price savings (15%). Similarly, when asked what features they find important when choosing whom to transact with online, confidence personal data is secure was very important for 71%, by far the highest. This was followed by easy payment process (61%) and ease of login/authentication (53%).

Similar trends were observed in the UK; 43% cited security of personal data as the top expectation when selecting online companies, with quality of goods or services (27%) and cost savings (20%) ranking much lower. There appears to be slightly higher expectations from UK consumers when it comes to features when choosing whom to transact with online, particularly in relation to new account setup, which is an important business consideration when reflecting on conversion and drop-off rates. However, confidence in security of personal data (76% said it was very important) was by far consumers most-stated important feature when choosing whom to transact with online.

Ranked Expectations/Qualities in Preferred Online Companies

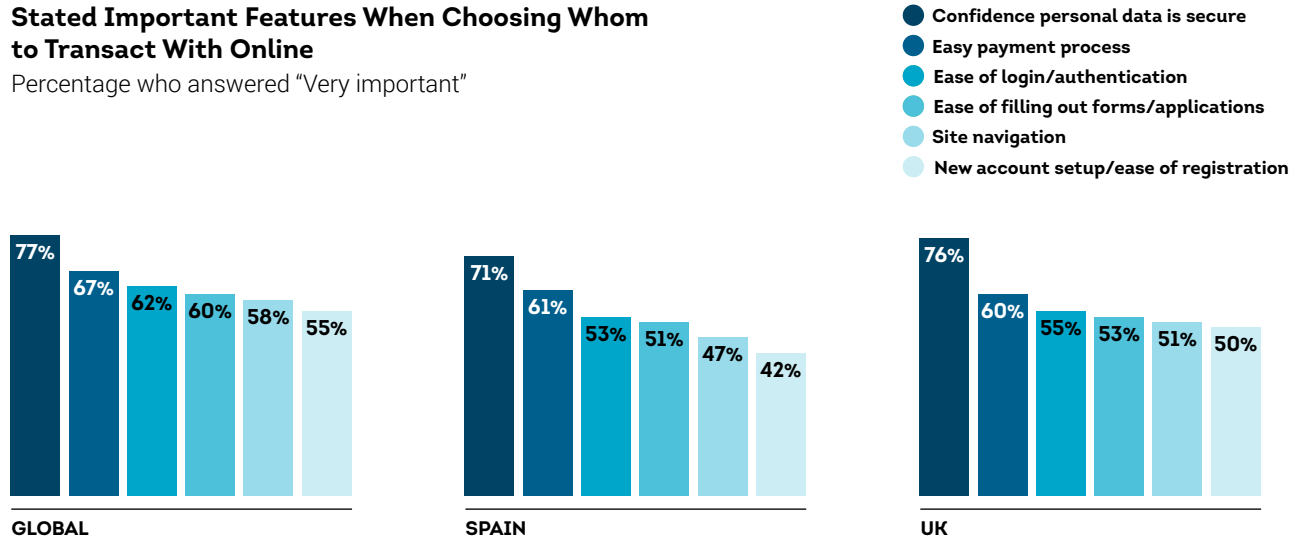
Top answer chosen



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

Continued reduction in suspected digital fraud rates masks the overall elevated fraud threat

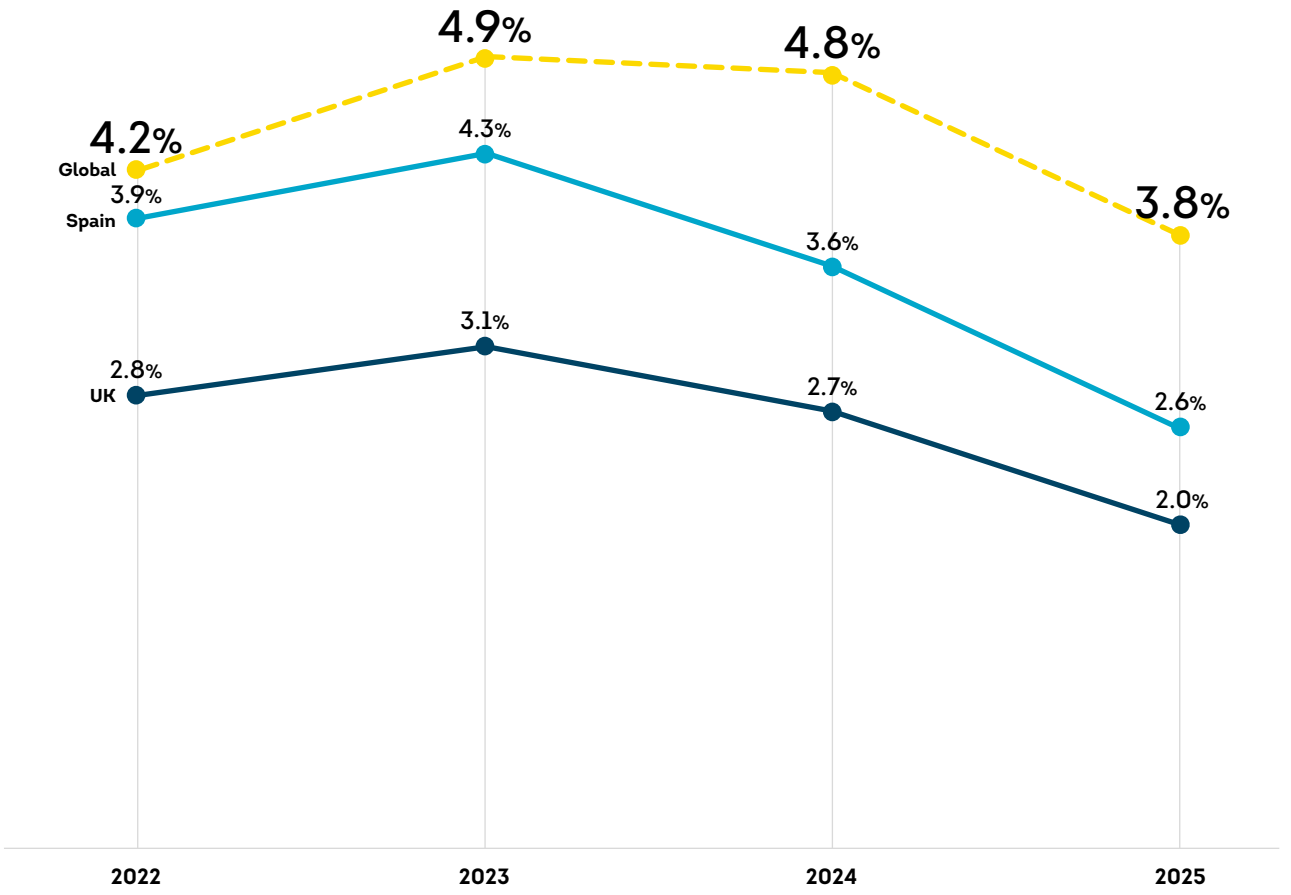
The UK and Spain observed more pronounced reductions in suspected digital fraud rates from 2022 to 2025 when compared to global trends. Notably, these rates were among the lowest across regions, including developed markets like Canada and the US. This may, in part, be related to European organisations being early adopters of new strategies and fraud prevention technologies like device intelligence.

Transaction attempts where the consumer was in the UK steadily declined from a 3.1% suspected digital fraud rate in 2023 to 2% in 2025. Similarly, Spain saw a reduction from 4.3% in 2023 to 2.6% in 2025.

While the rate of suspected digital fraud may be declining, other threat vectors are being pursued by fraudsters. In particular, consent-based attacks, such as APP fraud, money mule activity and synthetic identity fraud, have become more of a focus.

This continued evolution requires a shift in defence mechanisms. For example, combining device and behavioural analytics with adaptive multi-factor authentication, and adaptive warnings before real-time payment commitments (particularly on mobile) for first-time payees and high-value or unusual transactions.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

TransUnion

The communities industry continues to have the highest rate of suspected digital fraud in the UK and Spain

The communities industry (which includes online dating sites and forums) was identified as the sector most at risk of fraud attempts for transactions where the consumer was in Spain or the UK in TransUnion's last Top Fraud Trends Report and continues to hold this position.

For transactions where the consumer was in the UK, there was a significant jump in the suspected digital fraud rate in communities from 10% in the first half of 2025 to 12.5% for all of 2025. In Spain, the rate in communities rose from 9.5% to 9.9%. Communities was also the sector with the highest rate in other mature markets like Canada (11.9%) and the US (11.7%) in 2025.

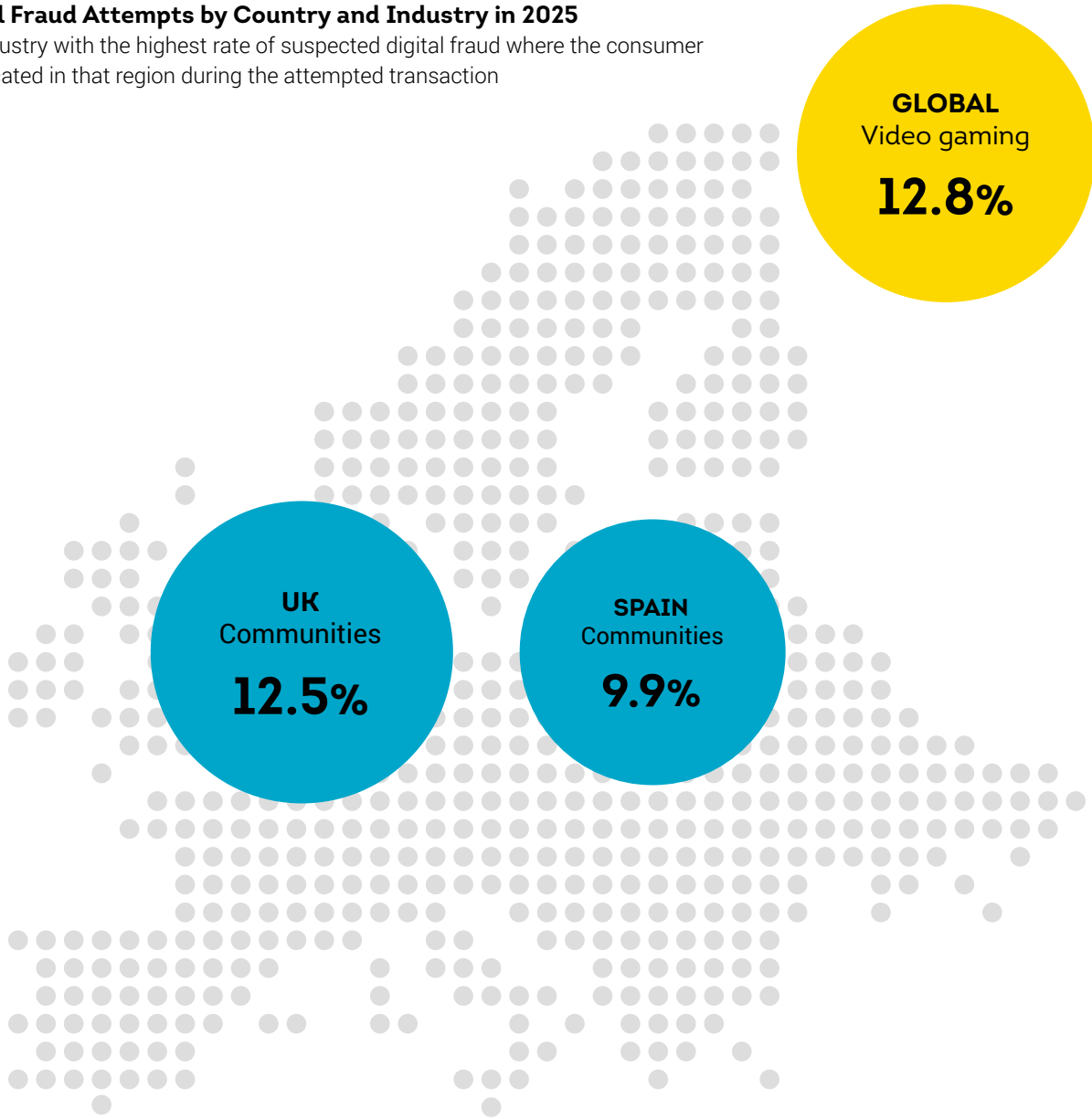
Communities organisations often blend identity-light profiles, and provide access to messaging and journeys that make impersonation and ATO easier — which often spill into marketplaces and payments.

Further advancements are required to increase the level of trust in this sector, particularly important given the level of emotion often linked to interactions on these platforms. Organisations need to enhance anti-impersonation efforts, including verified profiles and secure in-platform messaging. The spillover threat into payment platforms is obvious, with a need for improved beneficiary risk scoring and pre-transfer prompts when sessions look coached or urgent.

Gaming and video gaming industries continued to have elevated suspected digital fraud levels. Like communities, these sectors are often associated with identity-light profiles and limited direct exposure to organisational fraud loss.

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 region during the attempted transaction



Source: TransUnion global intelligence network

TransUnion

Account creation remains the digital lifecycle stage with the highest level of risk

For digital transactions where the consumer was in the UK, there was a noticeable increase between the first half of 2025 and all of 2025 in the suspected fraud rate of account creation attempts, rising from 4.9% to 8.1%. Interestingly, suspected digital fraud rates for account login and financial transactions remained relatively flat.

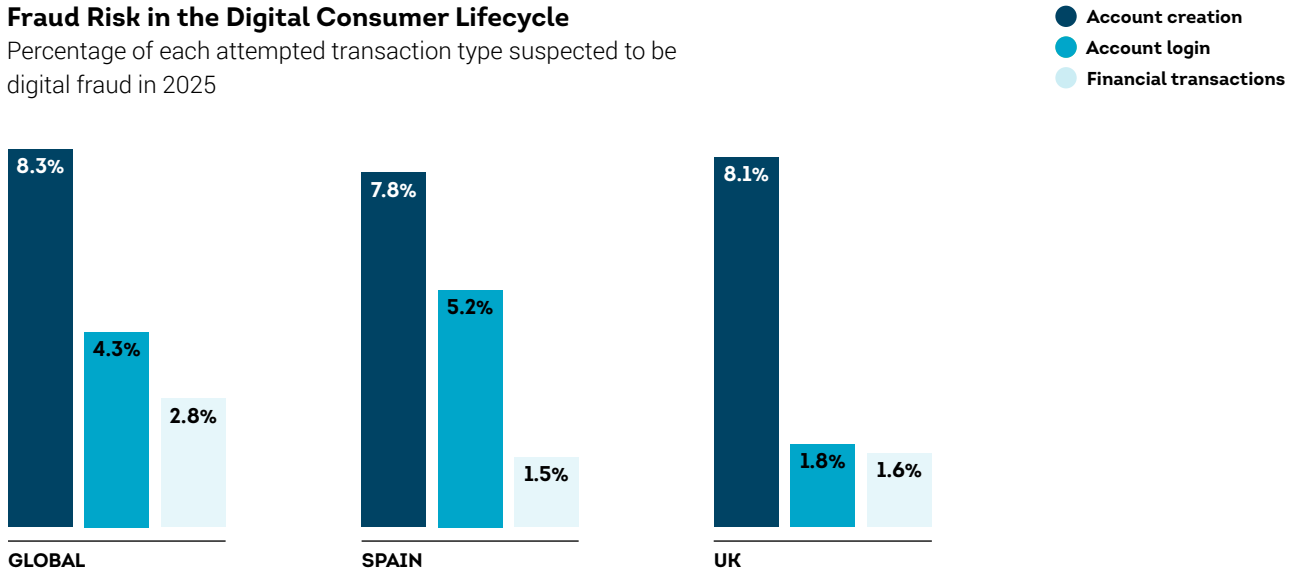
In Spain, there was also an increase (from 6.8% to 7.8%) in the rate at account creation from mid-year 2025 to the entire year. Meanwhile, there was a pronounced decrease in the rate during the financial transaction stage, dropping from 2.2% to 1.5%, and a slight increase during account login from 4.9% to 5.2%.

With the rise of bot and distributed denial-of-service attacks, there's an expansion of vulnerabilities across the digital consumer lifecycle organisations need to defend against. Fraud at the transaction layer often looks legitimate from the account's perspective. Organisations can block or employ step-up authentication when risk spikes during a transaction, not just at login.

Mechanisms like device intelligence have historically been used primarily as onboarding interventions. However, there's an increasing need for this intelligence to be leveraged across the digital consumer lifecycle. Creating a robust device identifier will help identify bad actors but — perhaps more importantly — build trust with genuine consumers to deliver improved experiences and drive top-line growth.

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

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

TransUnion

LATIN AMERICA

Latin America Overview

Thanks to corporate investments in mitigating fraud, the rate of suspected digital fraud attempts for the Latin American countries analysed decreased 46% from 2024 to 2025. However, a high percentage of suspicious digital transactions continued to be observed during account creation and login. Latin American consumers who said they lost money in the last year due to digital fraud reported a median loss of USD 1,973. This represents significant challenges to their personal finances and impacts their abilities to continue transacting with confidence.

Vishing emerged as the most reported fraud scheme in Latin America. As such, fraud prevention strategies must continue to emphasise consumer responsibility around protecting their personal information and credentials. This should be achieved through sustained consumer fraud education and awareness.

Companies must continue strengthening and investing in their fraud-mitigation programs to ensure consumers can trust their personal data is safeguarded and used appropriately. This remains one of the most important factors consumers cited when deciding which company to transact with online.

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

KEY TAKEAWAYS

Fraudsters focus on vishing

41%
of Latin American adults said they were targeted by digital fraud from August to December 2025.

27%
of Latin American consumers who said they were targeted by fraud indicated they were targeted by vishing, making it the top fraud scheme in the region.

Fraudsters persist – pressuring account creation the most

5.7%
of digital account creation attempts when the consumer was transacting from Latin America in 2025 were suspected to be digital fraud, making it the riskiest part of the consumer lifecycle in the region.

83%
of Latin American consumers said it's very important to have confidence their personal data will not be compromised when choosing whom to transact with online.

Ongoing digitalisation – fraudsters lying in wait

37%
of Latin Americans said they conduct most of their account management activities online, two percentage points higher than a year before.

33%
of Latin American Gen Z respondents said they lost funds from digital fraud in the last year, making them the generation with the highest percentage, likely correlated with their extensive online presence.

Consumer Fraud Experiences

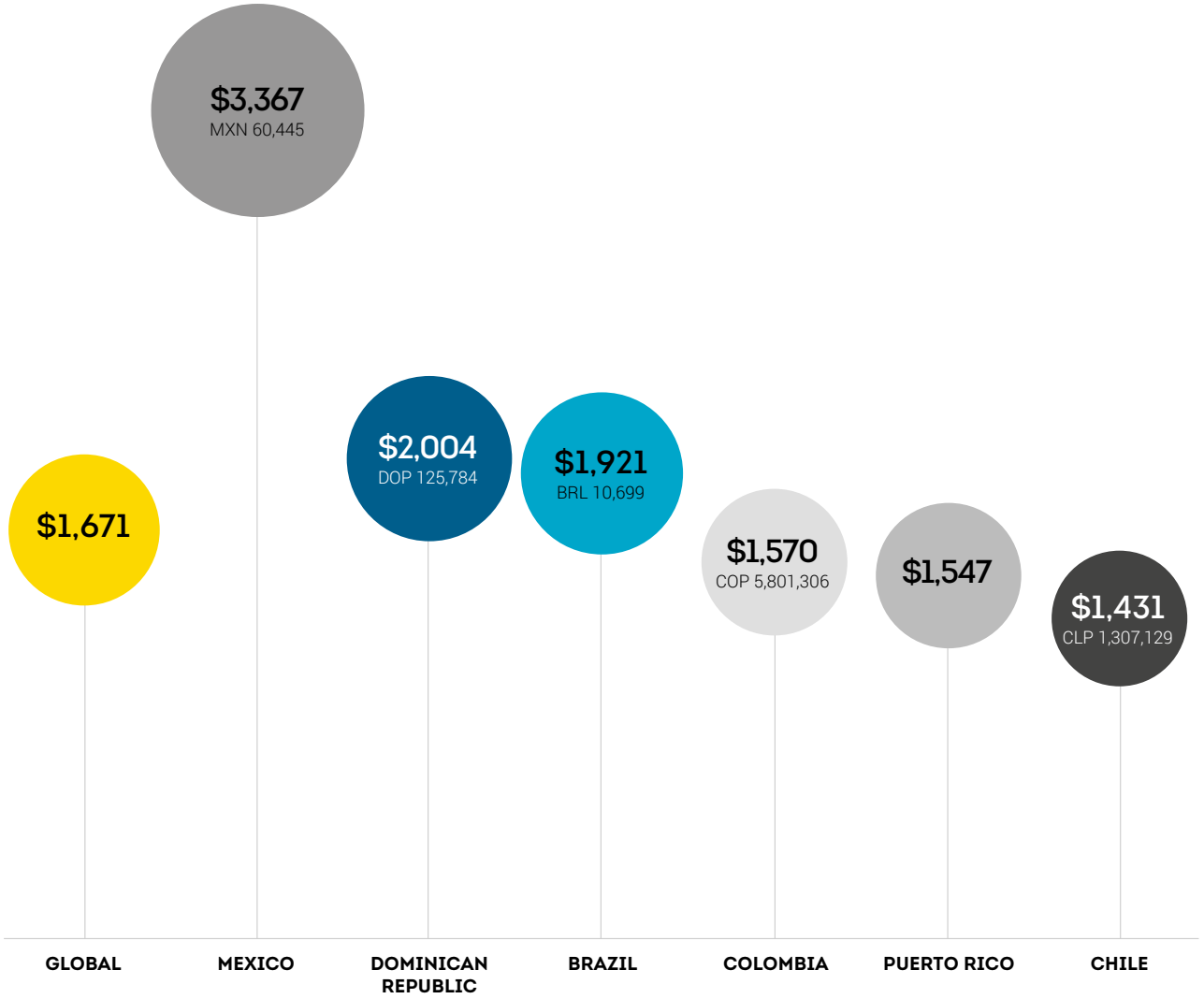
The significant impact of fraud on consumers

With a median reported loss of USD 1,973 by consumers in Latin America who said they lost money in the last year due to digital fraud, the region stands above the global average and exceeds countries like Canada and Spain. These costs have a long-term impact on consumers as financial and credit recovery often require extensive and gradual remediation processes.

Vishing was the most reported fraud scheme Latin American consumers said they lost money to in the last year. That's in contrast to what was reported globally — where third-party seller scams on legitimate ecommerce sites and money mule schemes ranked as the most prevalent. Vishing was reported by more than a quarter of Latin Americans in Brazil (32%), Chile (29%), the Dominican Republic (40%), Mexico (37%) and Puerto Rico (42%), significantly above the global average of 23%.

Consumer Reported Fraud Loss

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



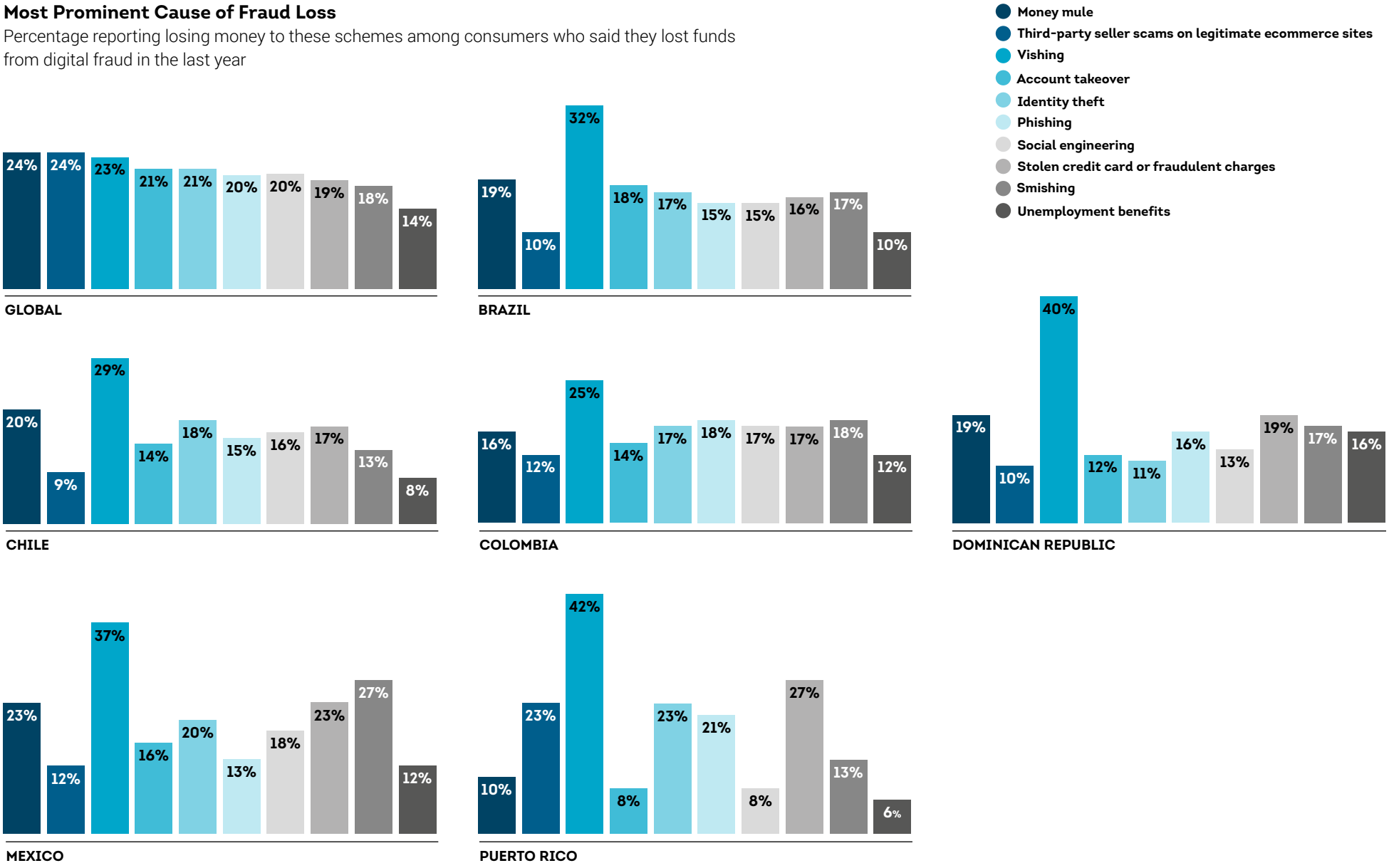
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

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

TransUnion

Fraudsters continue targeting consumers, although many may not be aware

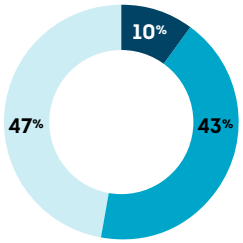
While 41% of consumers surveyed in Latin America reported being targeted by an digital fraud scheme in the last three months (less than the global rate of 53%), a significant portion of the population may not recognise potential fraud. Nearly 6 in 10 (59%) said they were unaware of being targeted.

Globally, phishing was the most reported fraud scheme among those who said they were targeted. In contrast, vishing was the most-reported fraud scheme by those who said they were targeted in Brazil, Chile, Colombia and the Dominican Republic. Stolen credit cards or fraudulent charges also had significant relevance in the region, where consumers in Mexico and Puerto Rico reported it as the top fraud scheme.

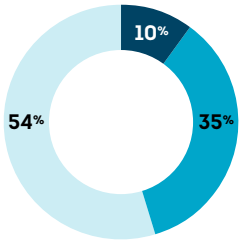
Combined across surveyed Latin American countries, vishing was the most reported scheme. To address it, companies should focus on advocating for consumer-centric protection and education to mitigate account takeover pathways.

Consumers Targeted With Fraud

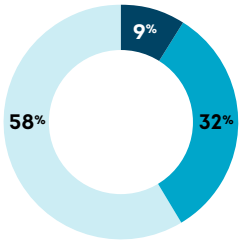
Percentage of consumers who said fraudsters targeted them with digital fraud attempts from August to December 2025, and the most frequent scheme by which they reported being attacked



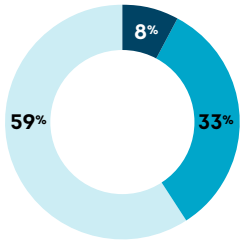
GLOBAL
Phishing



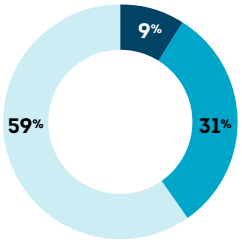
DOMINICAN REPUBLIC
Vishing



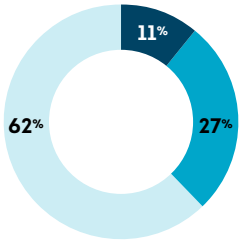
BRAZIL
Vishing



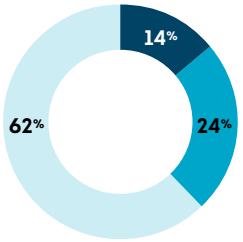
MEXICO
Stolen credit card or fraudulent charges



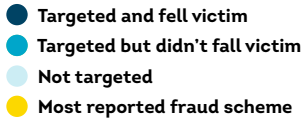
COLOMBIA
Vishing



CHILE
Vishing



PUERTO RICO
Stolen credit card or fraudulent charges



Source: TransUnion consumer survey

TransUnion

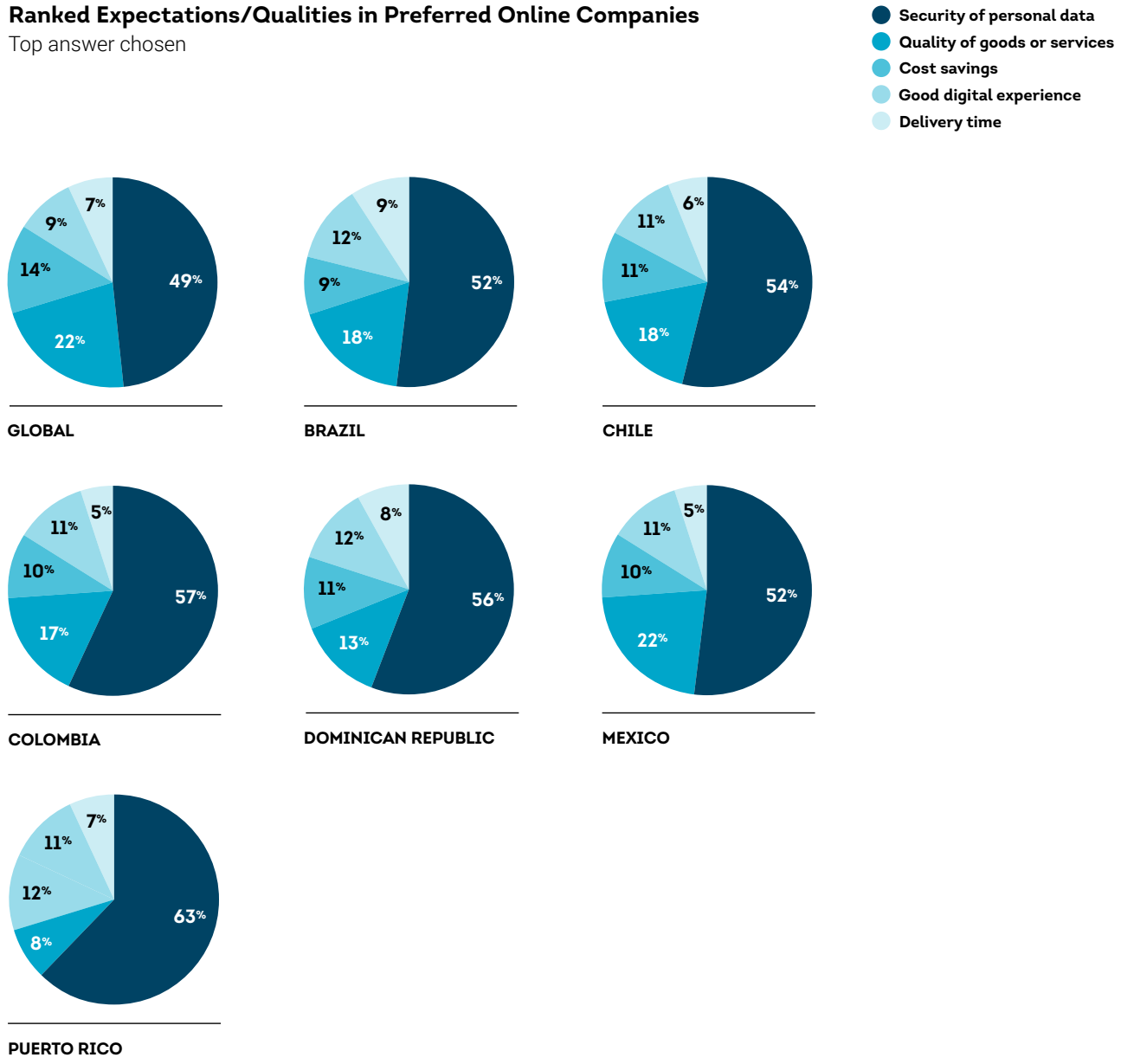
Security of personal data online top consumer expectation

Consumers globally are clear about their expectations when transacting online. When asked to rank the qualities or expectations they consider when deciding what online company to do business with, security of their personal data was the top choice for 49% and quality of goods and services was the top choice for 22%.

Despite the importance placed on delivery times and digital experiences, consumers in Latin America are aligned with global expectations; personal data security remained the top quality across the region, particularly in markets like Puerto Rico and Colombia.

When asked to what extent they find certain features important when choosing whom to transact with online, confidence their personal data is secure once again came out on top for Latin American countries. Consumers in Puerto Rico said confidence their personal data will not be compromised was very important (93%), the most among Latin American countries, followed by the Dominican Republic (86%). An easy payment process ranked as the second most important factor for all Latin American countries surveyed, consistent with consumers globally.

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

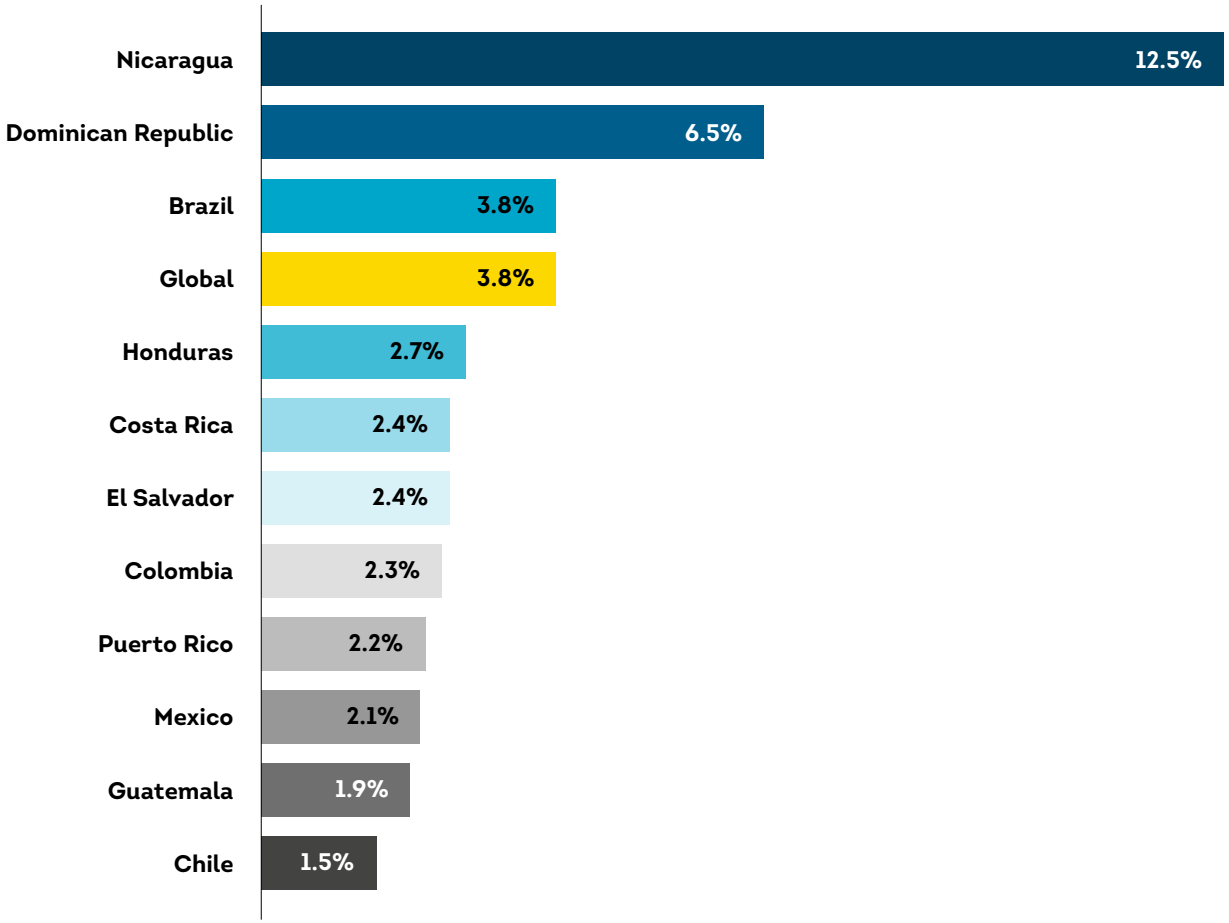
Digital Fraud Trends

Suspected digital fraud elevated in key Latin American markets

The global rate of suspected digital fraud attempts among TransUnion clients was 3.8% in 2025. This reflects the continued effectiveness of fraud prevention strategies across key markets. For Latin American countries analysed, the average rate was 2.7%, with notable variation across countries. Three markets — Brazil, the Dominican Republic and Nicaragua — reported rates above the regional average. These elevated levels suggest fraudsters are more active in these specific markets because vulnerabilities in those locations may be higher than others.

Every market measured in Latin America except Nicaragua reported a year-over-year decline in suspected digital fraud attempts, highlighting the importance and effectiveness of coordinated fraud-mitigation efforts in these countries.

Rate of Suspected Digital Fraud 2025



Source: TransUnion global intelligence network

TransUnion

Government and logistics industries the highest suspected digital fraud rate in most Latin American countries

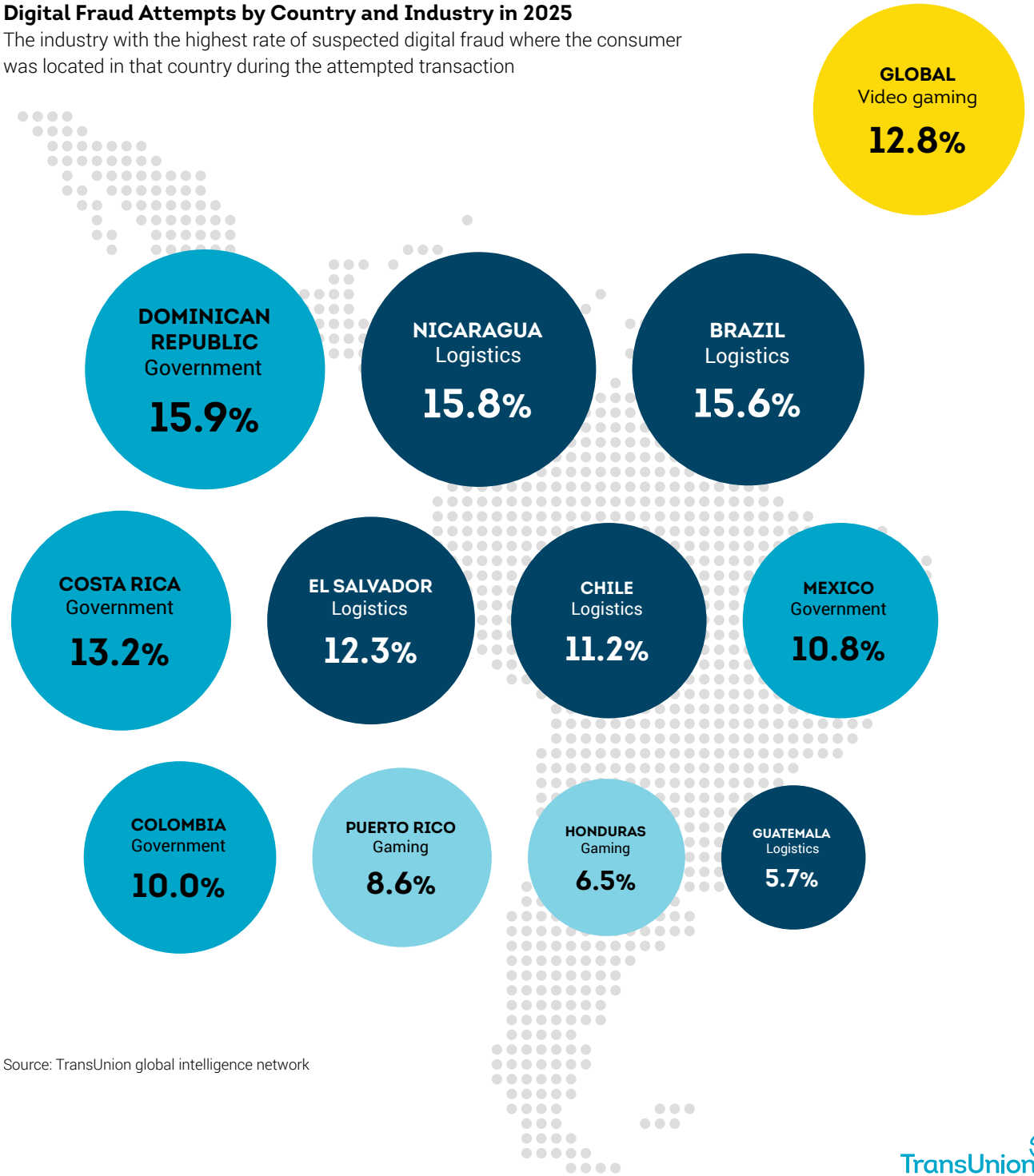
Among the industries analysed globally, the video gaming sector recorded the highest percentage (12.8%) of suspected digital fraud attempts in 2025. The volume of suspected digital fraud in this sector grew a significant 7% from 2024 to 2025, underscoring the sector's growing vulnerability to fraudulent activity.

In Latin America, different industries within individual markets exhibited elevated fraud rates. For attempted transactions where the consumer was in Nicaragua for example, the logistics sector reported the highest rate of suspected digital fraud across all industries analysed at 15.8%.

Across nearly all markets in the region, the government and logistics sectors emerged as those with the highest rate of suspected digital fraud. This trend reflects the continued efforts of fraudsters to exploit sectors handling sensitive personal data and other data, such as addresses or purchase records. These figures also highlight the need for targeted fraud prevention strategies within these verticals.

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

Risky identities impact all stages of the consumer lifecycle, especially account creation

The percentage of suspected digital transaction attempts at account creation represented the highest growth in fraud risk across the digital consumer lifecycle, increasing by 18% from 2024 to 2025 globally. Account login also showed elevated risk in 2025, with a suspected digital fraud rate of 4.3%, exceeding the global rate for all digital transaction attempts of 3.8%.

For digital transaction attempts where the consumer was in the select Latin American countries, account creation emerged as the most targeted transaction type in the digital consumer lifecycle, with a suspected digital fraud rate of 5.7% in 2025. Nicaragua and the Dominican Republic led the region in account creation suspected digital fraud risk, reporting rates of 65.3% and 15.8%, respectively, in 2025. The account login lifecycle stage in El Salvador and Mexico reported similar suspected digital fraud rates to account creation last year.

In some markets like Brazil, lifecycle risk tilted toward transactions. For digital transaction attempts where the consumer was in Brazil, the suspected digital fraud rate was below the global average at account creation (3.7% vs. 8.3%) and login (2.6% vs. 4.3%) but above the global average for financial transactions (3.2% vs. 2.8%) in 2025.

Consumer Lifecycle Stage Examples

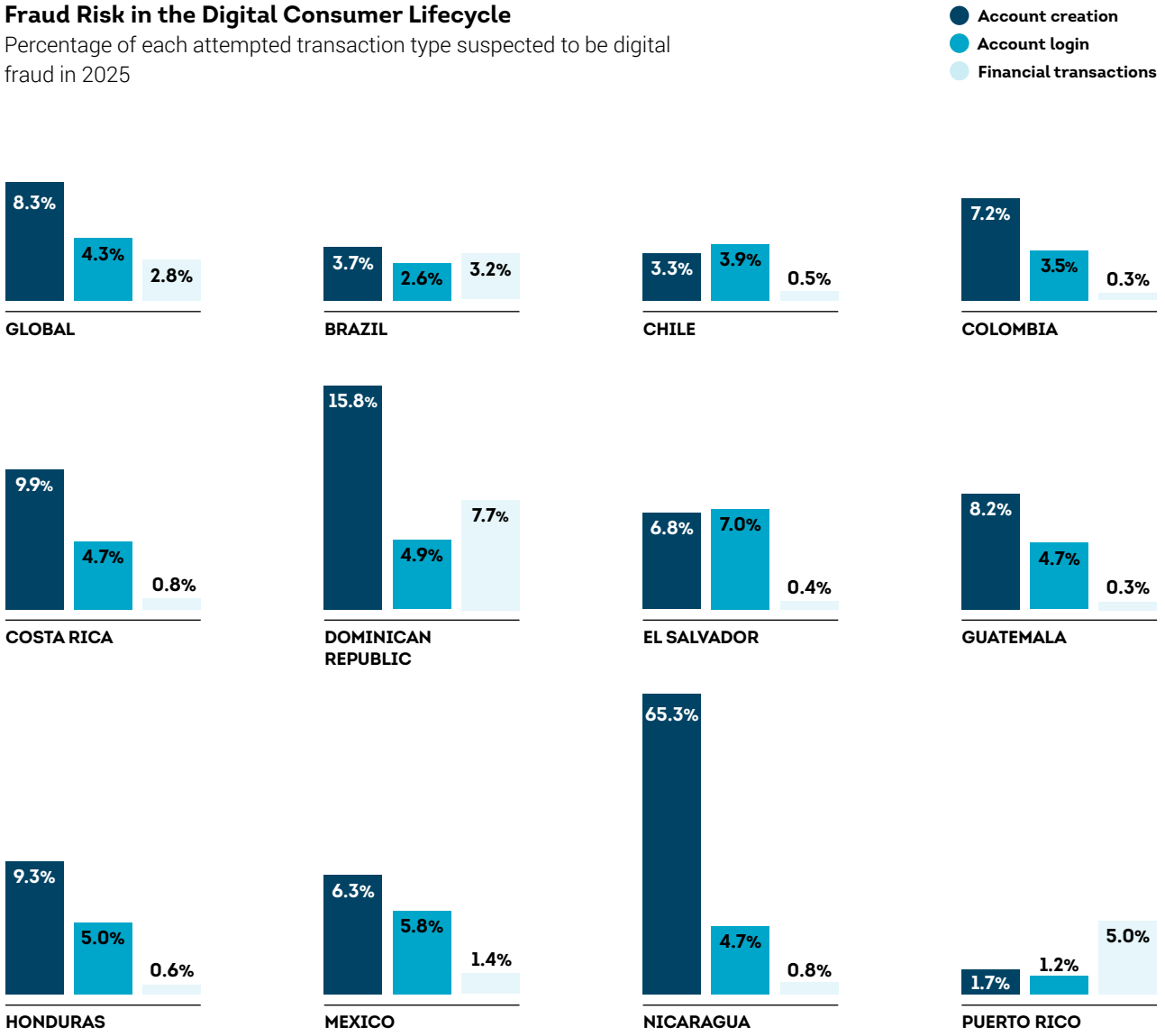
Account creation: Account signup, registration and loan origination

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

NORTH AMERICA

Canada Overview

Canada's digital fraud landscape is becoming increasingly sophisticated, driven by a surge in digital incidents, evolving criminal tactics and widespread exposure of consumer data. Fraudsters are shifting toward high-success, short-term digital schemes, contributing to a higher rate of suspected digital fraud attempts than the global average and an elevated consumer concern around ATO — trends that mirror the growing complexity of cyber threats nationwide. Consumers feel the financial losses from digital fraud, placing pressure on Canadian institutions to deliver strong protection without compromising digital convenience.

Looking ahead, we have growing threats that require advance techniques, such as machine learning models, device risking, consortium analytics and cross-institution intelligence sharing, to shape the next phase of fraud prevention. Institutions must work to strengthen resilience against increasingly adaptable and well-organised digital adversaries.

Canadian data in this section blends proprietary insights for digital fraud from TransUnion's global intelligence network and a consumer survey.

KEY TAKEAWAYS

Canadian consumers are concerned about identity-based fraud

52%
of surveyed Canadians were concerned about falling victim to identity theft.

41%
reported concerns of their accounts being accessed fraudulently (ATO).

Most consumers reported being targeted with digital fraud attempts

55%
said they'd been targeted in the past 90 days.

45%
reported they were unaware of being targeted in that period.

Canadians claim four-figure fraud losses in the last year

13%
reported they lost money due to digital fraud in the last year.

CAD 1,301
the median fraud loss reported by those who said they lost money due to digital fraud in the last year.

Consumer Fraud Experiences

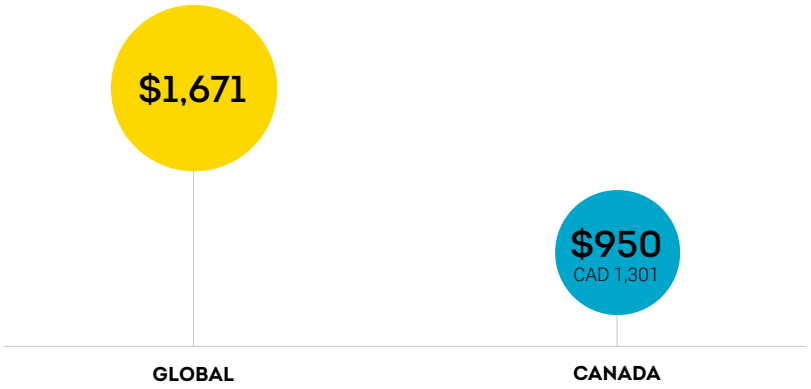
Consumers prefer organisations they feel protect their identities while delivering convenient experiences

Consumers increasingly prefer to do business with organisations they trust to protect their personal information, making strong identity safeguards a clear differentiator in today's digital-first environment. When consumers believe an organisation is prioritising security, confidence and loyalty rise, positioning identity protection as a critical driver of competitive advantage.

This expectation is reinforced by real financial impacts: 13% of Canadian consumers reported losing money to fraud perpetrated through digital channels over the past year, underscoring the personal risk of digital engagement. As fraud becomes more sophisticated, consumers are gravitating to organisations that demonstrate proactive, visible protection — elevating the strategic importance of robust fraud-prevention and identity-security programs.

Consumer Reported Fraud Loss

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

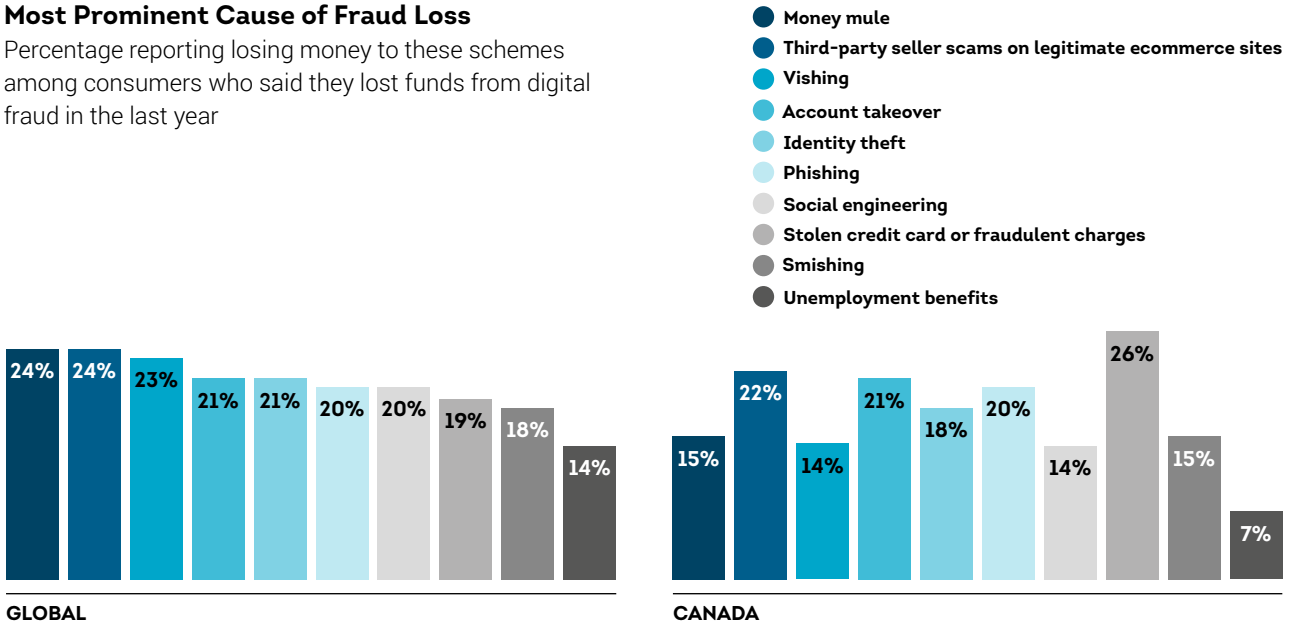


*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

Source: TransUnion consumer survey

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

TransUnion

Canadians report widespread fraud

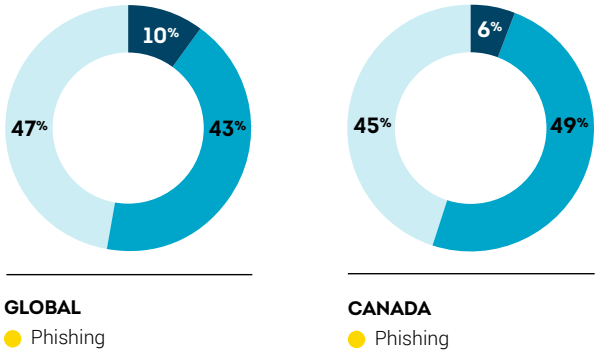
Canadian consumers reporting being targeted by digital fraud is widespread. Despite high targeting rates, only 6% reported falling victim to these fraud attempts from August to December 2025. This is a year-over-year decrease of three percentage points and may suggest education and defences are gaining some traction.

Phishing fraud attempts in Canada continued to be the most reported fraud scheme among those who said they were targeted with fraud as cybercriminals leverage increasingly sophisticated tactics to deceive both individuals and organisations. As cyber threats continue growing in volume and complexity, phishing remains one of the most common and effective entry points for broader cybercrime. And as phishing schemes become more tailored, AI-driven and financially motivated, they pose a growing risk to Canada's digital economy. This reinforces the need for strong awareness, multilayered defences and proactive incident-prevention strategies.

When it came to perceived threats, identity appeared to be at the heart of those concerns. When asked what type of fraud consumers were most concerned about, 52% said identity theft and 41% said ATO.

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

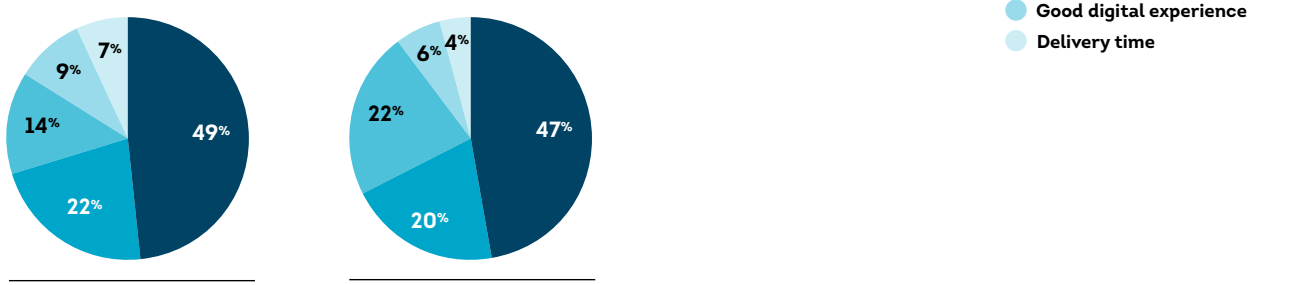
Consumer mindset driven by security of personal data

Consumers place significant importance on the protection of their personal data when interacting online, making it a defining factor in digital trust and engagement. Nearly half (47%) of Canadians identified the security of their personal data as their top quality when choosing whom to do business with online. By comparison, only 20% ranked quality of goods or services as their leading decision-maker and 22% cited cost savings, underscoring a clear shift toward security as the dominant expectation in an online business.

For organisations, the implication is direct and strategic: Strong data-protection practices are no longer just a compliance requirement but a core competitive differentiator. Organisations that demonstrate robust privacy safeguards, transparency in data handling and proactive security measures are far more likely to earn consumer confidence, build loyalty and outperform competitors in an environment where trust is increasingly the currency of digital commerce.

Ranked Expectations/Qualities in Preferred Online Companies

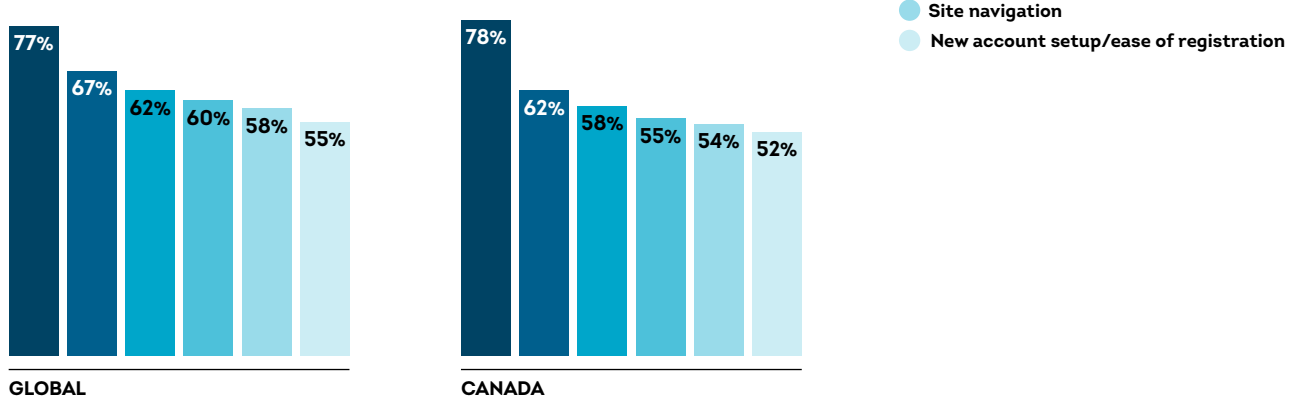
Top answer chosen



Source: TransUnion consumer survey

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

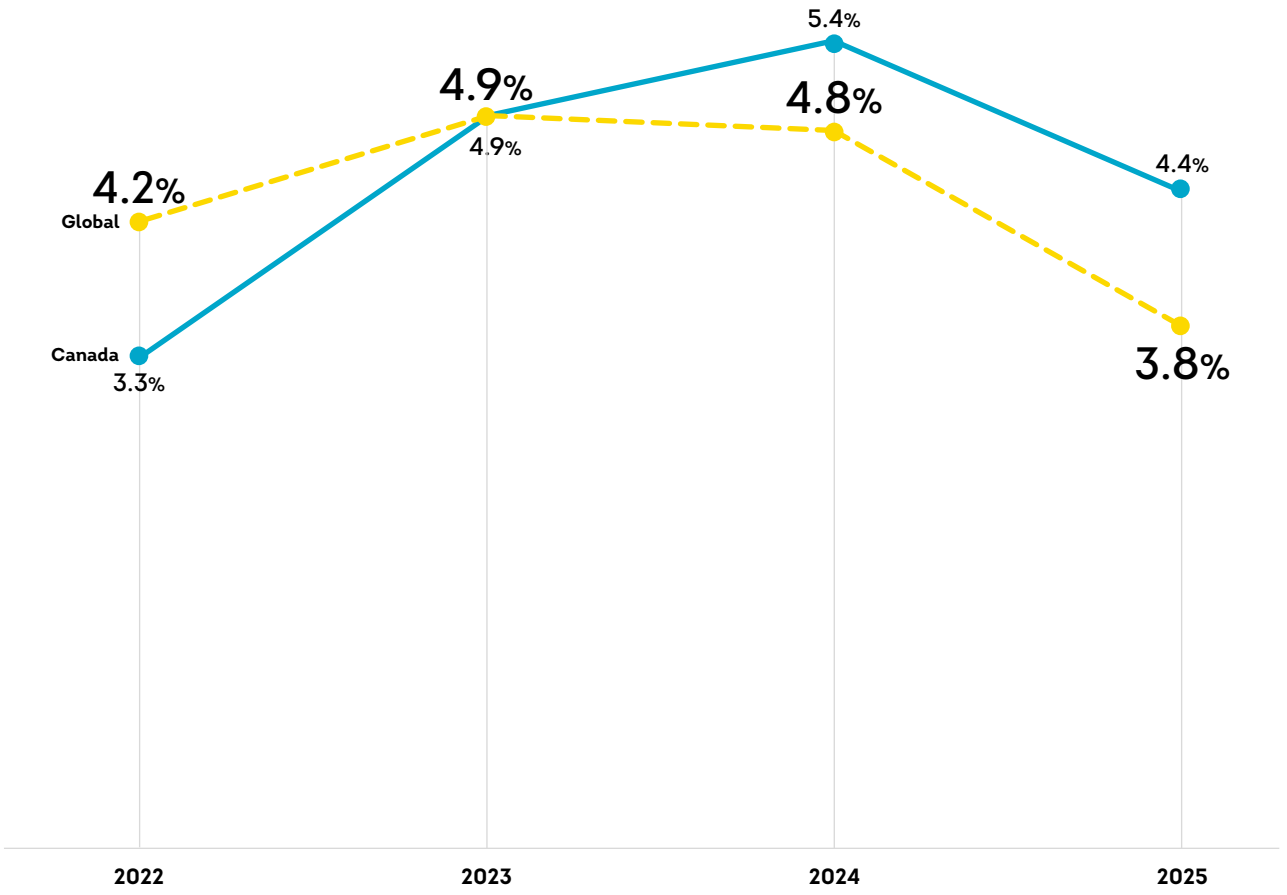
Digital Fraud Trends

Canadian digital fraud attempts ahead of global average

Canada continued to face elevated levels of digital fraud activity, reflecting a threat landscape that remains above the global average. The rate of suspected digital fraud attempts when the consumer is in Canada reached 4.4% in 2025, exceeding the global average of 3.8% during the same period. While this represents a slight year-over-year decline from 2024 levels, it still underscores Canadian digital interactions remain a disproportionately attractive target for fraudsters relative to many other markets.

For organisations, the implication is clear: Even incremental differences in fraud rates translate into significant operational exposure. As digital engagement accelerates and fraud schemes grow more sophisticated, strengthening identity verification, tightening digital-channel controls and investing in advanced fraud-mitigation technologies remain critical to protecting both consumers and organisational trust in Canada's increasingly high-risk digital ecosystem.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

TransUnion

Shifting industry fraud patterns: Certain sectors decline while others accelerate

Canada's digital fraud ecosystem continued to evolve rapidly, with clear divergence across industry sectors as fraudsters adapt their tactics and target areas of emerging vulnerability. Sectors experiencing the sharpest increases in suspected digital fraud attempts when the consumer is transacting in Canada include communities, which surged volume-wise by 63% from 2024 to 2025, followed by video gaming (up 53%) and government (up 14%). These rising risks reflect fraudsters' growing focus on platforms that facilitate person-to-person interactions, online social engagement and public-service access — areas where identity trust gaps and high digital activity create fertile ground for exploitation.

In contrast, several major industries reported significant declines in suspected digital fraud activity, suggesting improved controls and more mature fraud-mitigation capabilities. Online retail experienced a substantial 73% suspected digital fraud volume decrease, while telecommunications saw a 23% decline and financial services reported a 32% reduction.

Taken together, the diverging trajectories highlight a fraud landscape where attackers may be shifting to softer targets while established industries strengthen their defences. Organisations operating in high-growth fraud sectors must move quickly to boost resilience, while those with declining rates must remain vigilant as fraud patterns continue to shift across Canada's digital economy.

Digital Fraud Attempts From Canada by Industry

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

Communities
(online dating, forums, etc.)

2025
11.9%

2024-2025
+63%

Video gaming

2025
11.7%

2024-2025
+53%

Gaming
(online sports betting, poker, etc.)

2025
10.9%

2024-2025
+7%

Government

2025
9.1%

2024-2025
+14%

Insurance

2025
3.1%

2024-2025
+3%

Financial services

2025
2.3%

2024-2025
-32%

Logistics

2025
1.3%

2024-2025
-62%

Retail

2025
1.1%

2024-2025
-73%

Telecommunications

2025
0.2%

2024-2025
-23%

Source: TransUnion global intelligence network

Growing identity-based fraud means attacks could happen at every stage of the consumer lifecycle – all at once

Fraud risk continued to escalate across Canada's digital consumer journey. The data shows clear pressure at every stage, including online account creation when the consumer is transacting from Canada — where 4.6% of all attempts in 2025 were suspected to be fraudulent, highlighting how criminals use synthetic and stolen identities to infiltrate digital ecosystems from the outset.

The highest exposure in 2025 occurred during authentication; 14.2% of account login attempts were suspected to be fraudulent — potentially driven by automated, credential-based attacks and ATO attempts.

Even though only 0.8% of financial transactions in 2025 were flagged as fraudulent, this phase carries significant monetary and reputational impact due to the direct movement of funds. To effectively manage this lifecycle-wide threat, organisations must adopt integrated, intelligence-driven fraud controls that connect intelligent signals across all attack vectors, strengthening trust and reducing friction for legitimate consumers while minimising exposure to increasingly sophisticated fraud models.

Consumer Lifecycle Stage Examples

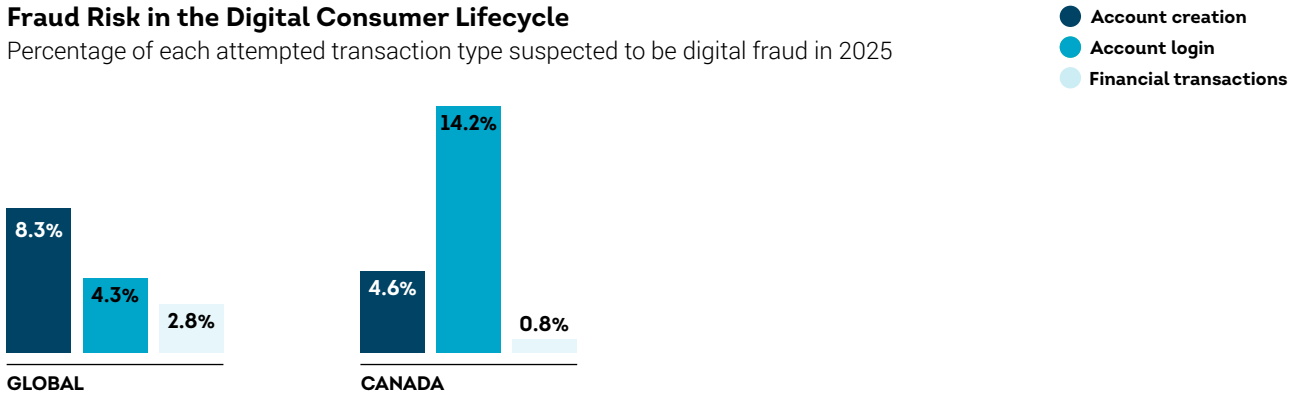
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

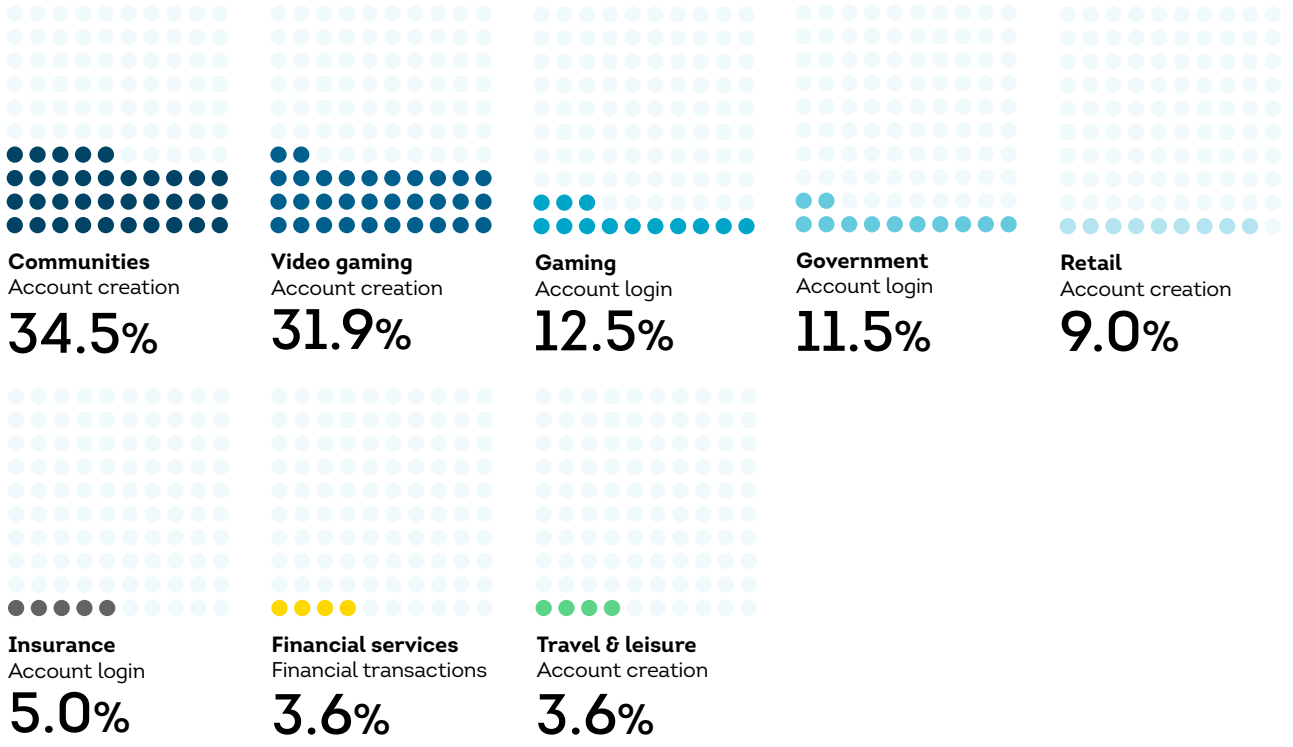
Percentage of each attempted transaction type suspected to be digital fraud in 2025



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 from Canada by industry and the corresponding percentage in that stage in 2025



Source: TransUnion global intelligence network

TransUnion

NORTH AMERICA

United States Overview

Fraud schemes are more sophisticated and harder to see. What's coming into focus is how criminals are working to get around defences. Criminals appeared to be exploiting two parallel digital fraud strategies in 2025, both dependent on weaponising compromised consumer identity information. First, target gullible consumers with increasingly believable scams for immediate gain, thereby avoiding fraud defences altogether. Second, steal credible identity information through data breaches, consumer scams and call centre agent social engineering to bypass authentication systems or fool new account creation fraud detection tools.

In 2025, these strategies resulted in significant consumer fraud losses to identity theft and ATO. It also revealed a paradox: lower overall digital fraud rate with a rising rate of ATO as fraudsters targeted high-value payouts. The high rate of scam and solicitation fraud reported from within a credentialed community, gaming or video gaming platform points to bad actors establishing their own accounts. And synthetic identities are a significant issue for any organisation, only more so for lenders with the weaponisation of credit washing. None of this is going to get easier in an AI-empowered digital fraud environment, demanding greater focus on unmasking identity fraud in every channel and at each stage of the consumer lifecycle.

KEY TAKEAWAYS

Consumer scams lead to large fraud losses

USD 2,307
median reported loss in the last year among the 16% of US consumers who said they lost funds from digital fraud in that period.

29%
of US consumers reported losing money to identity theft among those who said they lost money from any digital fraud in the last year, second only to stolen credit cards or fraudulent charges at 33%.

Compromised identities raise future fraud risk

78%
of US data breaches exposed full Social Security numbers in 2025, the highest since TransUnion's research began in 2020.

39%
of US consumers who said they were targeted by any digital fraud from August to December 2025 said the attack was a phishing scam, the top reported type of fraud.

Sophisticated identity fraud risk coming into focus

13%
increase in high-risk calls received in TransUnion US client call centres from 2024 to 2025, including a 41% increase in high-risk calls received from mobile numbers.

USD 2.6 billion
in lender exposure to synthetic identities in the US for auto loans, bank credit cards, retail credit cards and unsecured personal loans at the end of 2025.

Consumer Fraud Experiences

Identity-based fraud drives consumer fraud losses

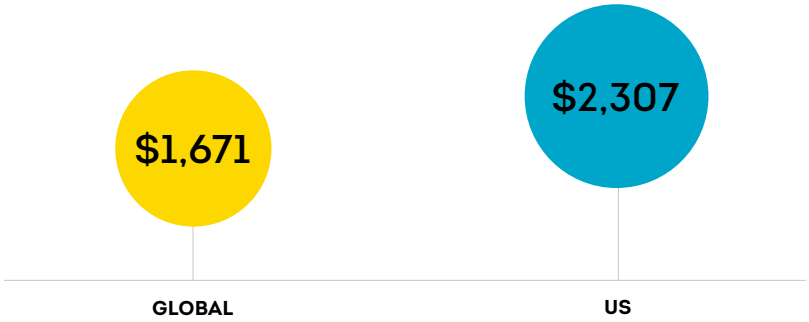
American consumers experienced fraud losses in 2025 that appeared closely related to data breaches and consumer scams — giving criminals the identity data needed to perpetrate fraud. Nearly one in six (16%) of US adult consumers said they lost money due to any digital fraud in the last year, with a median reported loss of USD 2,307.

Extrapolated to the US adult population (268.3 million on July 1, 2025, according to the US Census Bureau), this reflects an estimated USD 99 billion lost by US consumers to digital fraud in the past year.

A third (33%) of US consumers reported the reason for their loss was stolen credit card or fraudulent charge, 29% identity theft and 27% ATO.

Consumer Reported Fraud Loss

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

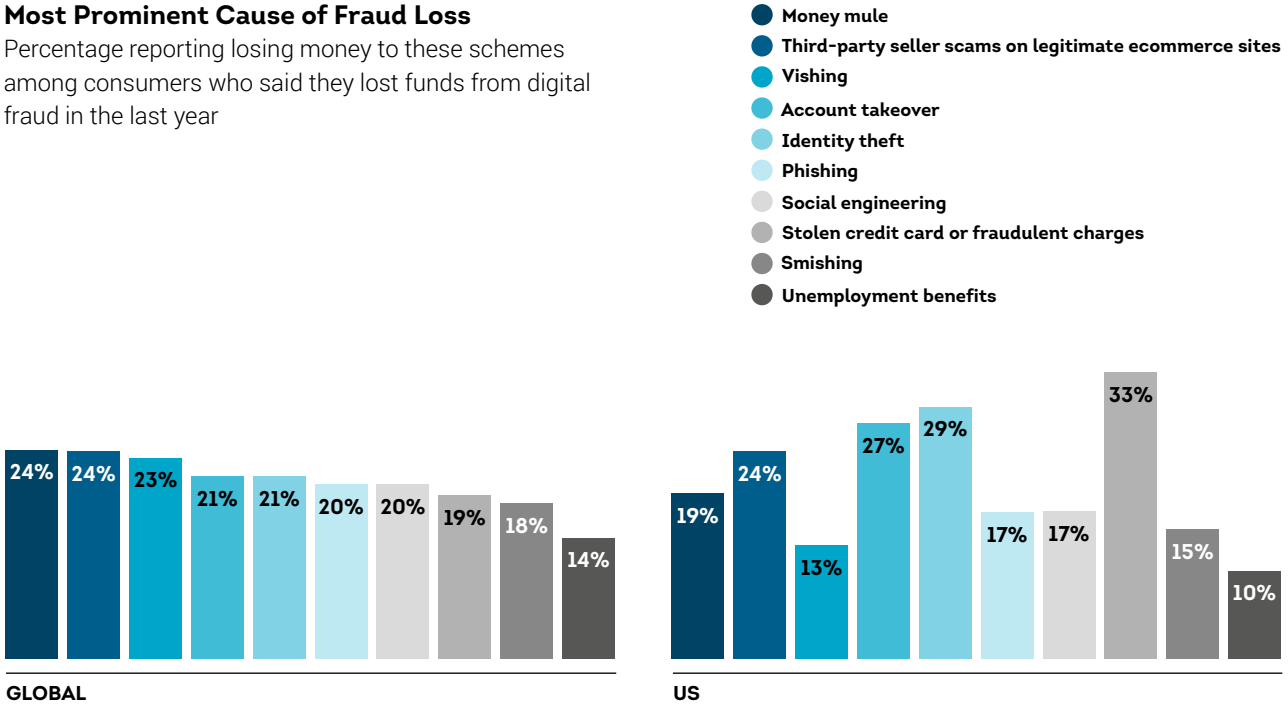


*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

Source: TransUnion consumer survey

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

TransUnion

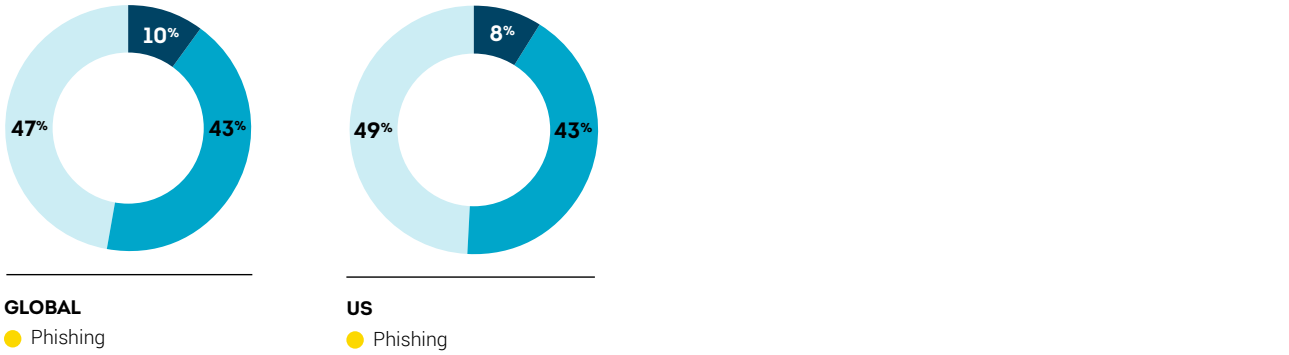
Phishing the most common consumer reported fraud scheme

Over half (51%) of US consumers reported being targeted by a digital fraud scheme, and 8% said they fell victim from August to December 2025. However, a significant portion of the population didn't recognise potential fraud; 49% said they were unaware of being targeted by fraud schemes. These numbers have been consistent for the last two years.

Phishing (fraudulent emails, websites, social posts, QR codes, etc. meant to steal data) was the most reported scam; 39% of US consumers said they were targeted with this type of fraud. This was followed closely by smishing (fraudulent text messages meant to trick someone into revealing data) at 36%.

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

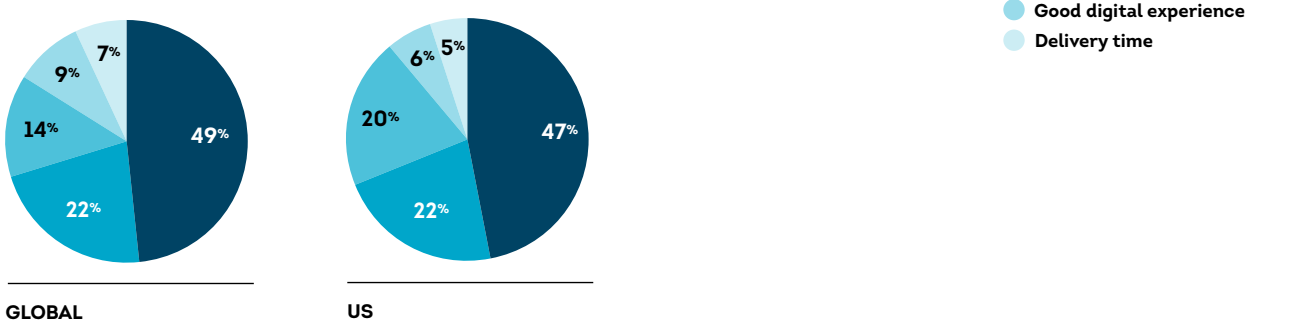
Consumers prefer brands that deliver safe, secure digital experiences

Americans seem to understand the risk of doing business online, but the convenience is too great to pass up. Forty-three percent said they conduct more than 50% of their transactions online and 57% said they do more than 50% of their account management online. But with adoption of digital channels, people expect brands' digital experiences to be secure and easy. Expectations are high — and the stakes are higher. Forty-two percent of US consumers would switch companies for a better digital experience and 70% won't return to a site if they sense any fraud risk.

Earning trust is key. Nearly half (47%) of consumers ranked strong data security as their top expectation from online companies, their top answer, and 76% said confidence their personal data is protected is very important when deciding where to do business, their most important feature. In addition, 44% said fraud concern was a top reason they'd abandon their online shopping cart, second only to shipping costs.

Ranked Expectations/Qualities in Preferred Online Companies

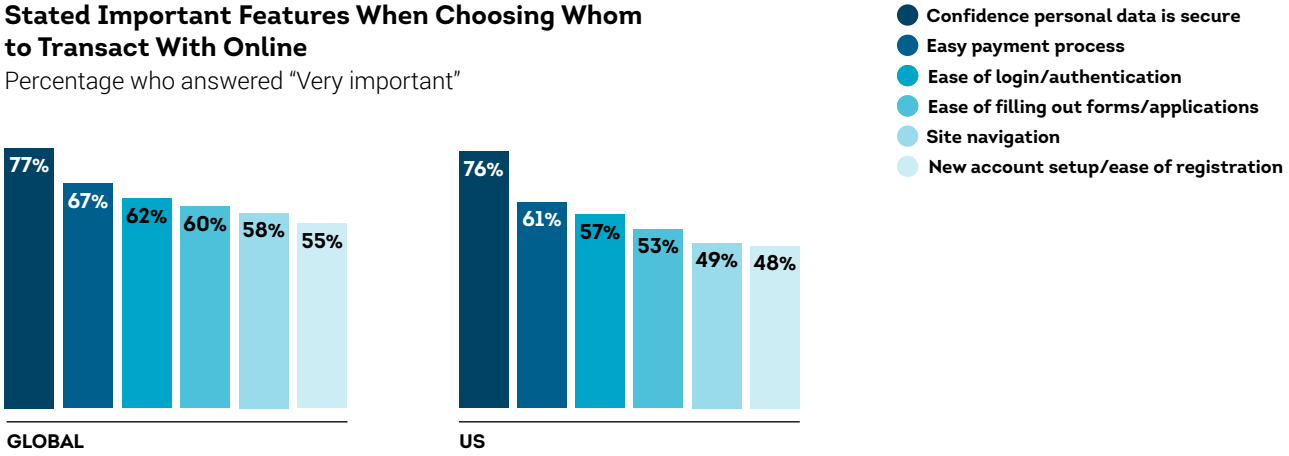
Top answer chosen



Source: TransUnion consumer survey

Stated Important Features When Choosing Whom to Transact With Online

Percentage who answered "Very important"



Source: TransUnion consumer survey

TransUnion

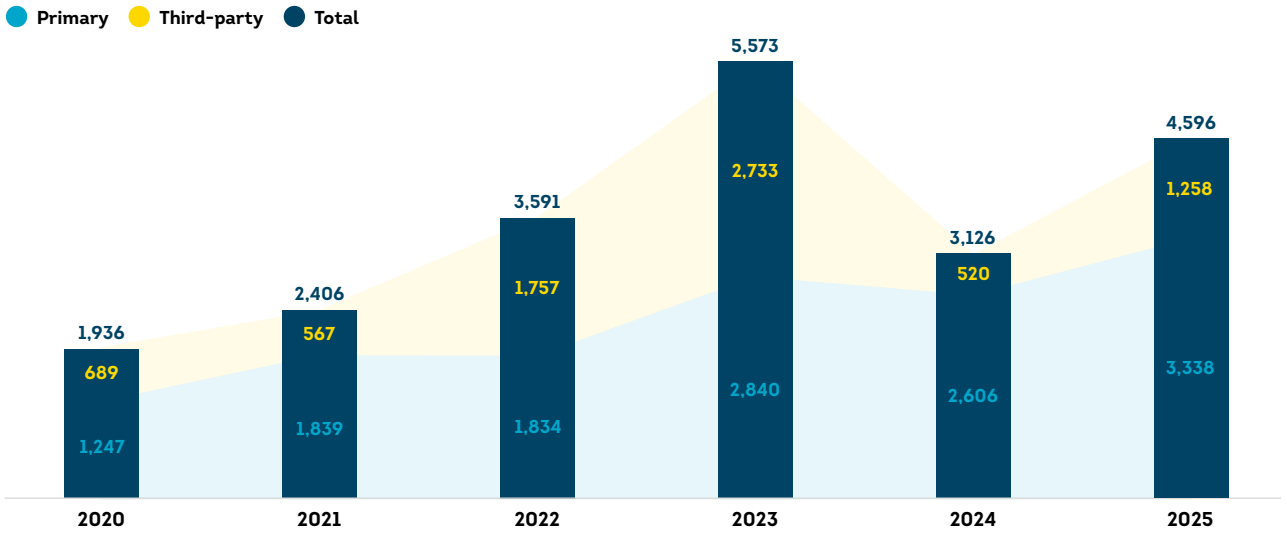
Identity Data Exposure Trends

US data breach severity reaches record level

The US experienced a 47% increase in data breach volume in 2025 compared to 2024. Attacks appeared to seek data not readily available in dark web data marketplaces to source identity credentials for fraud schemes.

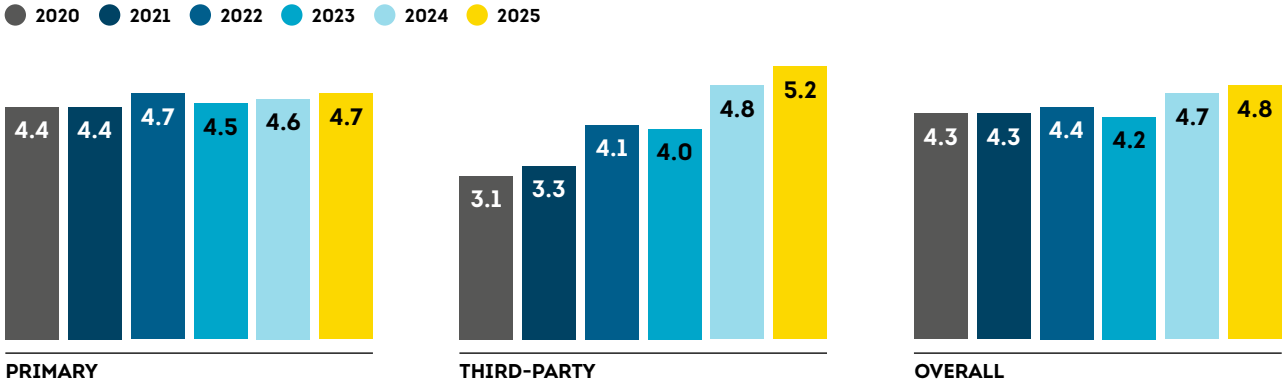
Criminals targeted high-risk credentials, including full Social Security numbers (SSN), that drove the average breach severity (the ability of a breach to enable identity fraud) as measured by TransUnion TruEmpower™ Breach Risk Score (BRS) — a leading indicator of future fraud — to its highest level since our examination dates back to in 2020. Third-party breaches involving attacks on organisations providing business services to brands were significantly riskier than those targeting primary organisations.

US Data Breach Volume



Source: TransUnion global intelligence network

Average Breach Risk Score for US Data Breaches



Source: TransUnion global intelligence network

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

TransUnion

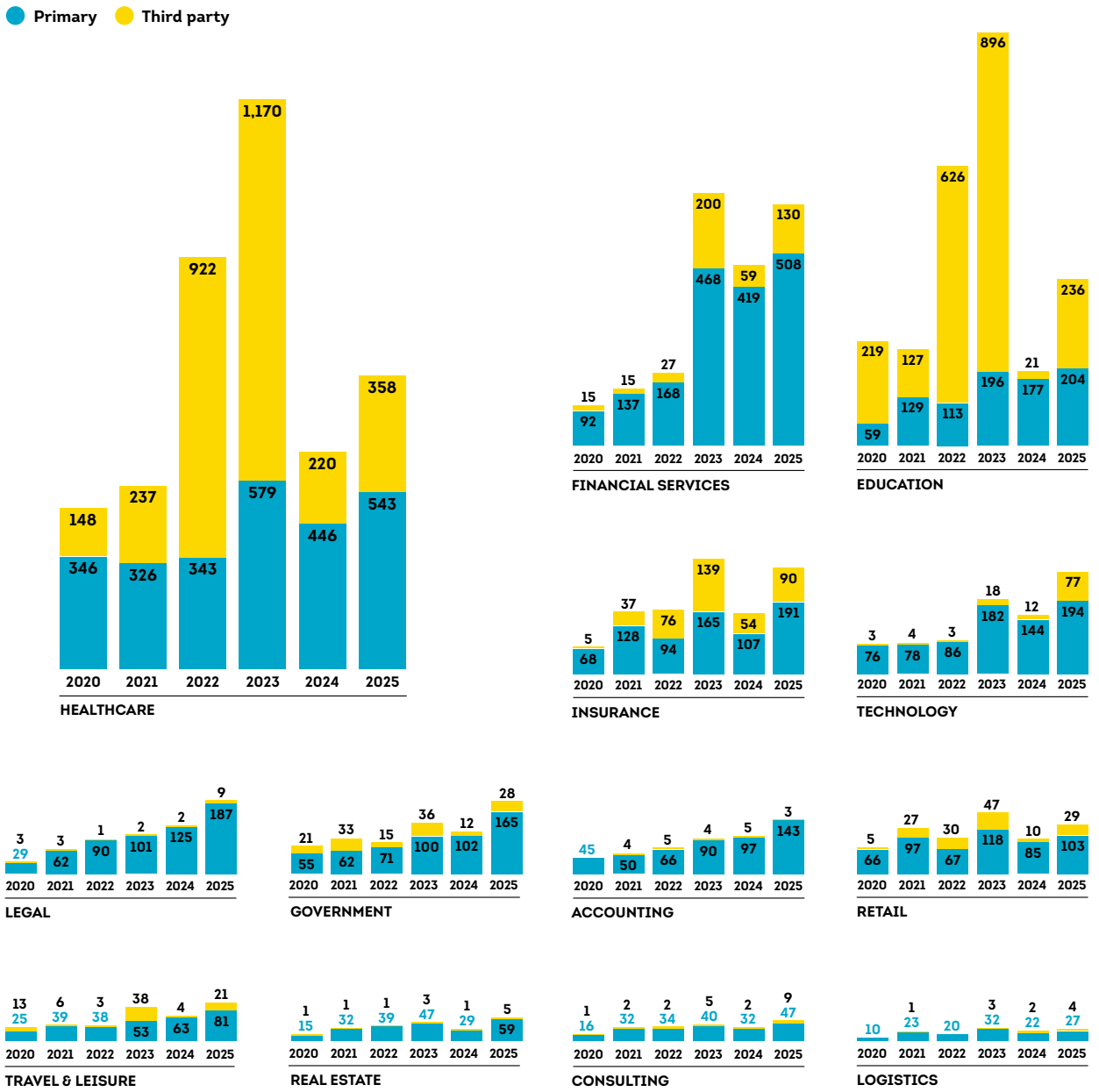
Healthcare continues to yield to more data compromises

The highest number of breaches in 2025 were seen in healthcare — followed by financial services. Meanwhile, healthcare and the accounting industry tied for sectors with the highest BRS (5.1).

Both direct and indirect attacks in healthcare focused on high-value identity credentials, including full SSN, medical history, payment numbers and contact information — all important in perpetrating consumer scams and verifying already-compromised data.

More than 84% of breaches in each of the top four high BRS industries (healthcare, accounting, legal and travel & leisure) were cyber attack-related as opposed to other types of breaches like system and human error. In the meantime, financial services and government experienced a below-average proportion of cyber attack-driven breaches.

US Data Breach Volume



Source: TransUnion global intelligence network

TransUnion

Criminals focus on high-value credentials for ATO and new account fraud

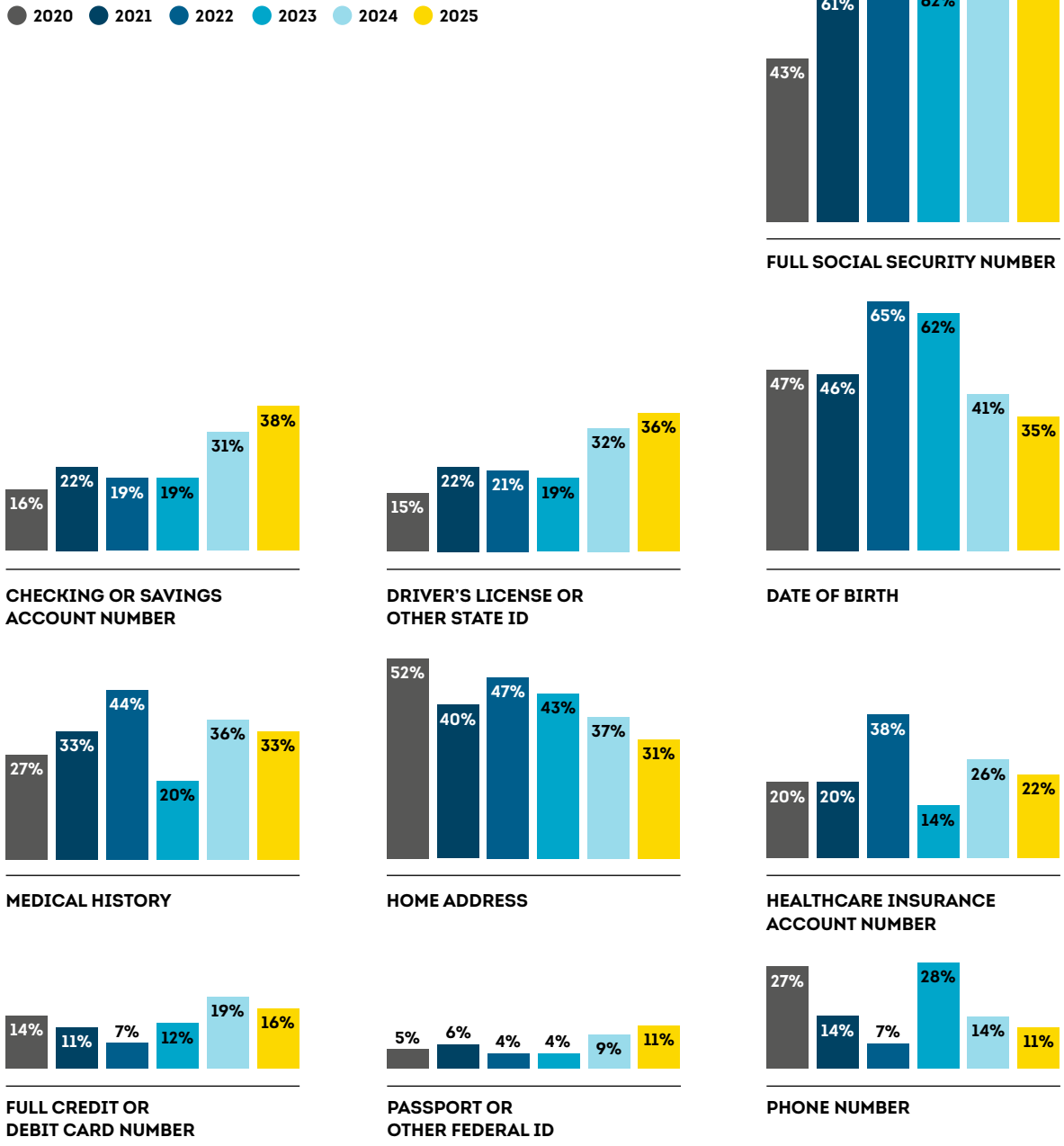
Full SSNs were exposed in 78% of all data breaches in 2025, consistently the top sought-after credential since 2021 and a 10% increase over 2024. This is a vital credential to perpetrate new account, ATO, tax refund and government benefits fraud.

In 2025, for the first time since our analysis began in 2020, the exposure of checking and savings account numbers was the second highest credential exposed, showing up in 38% of data breaches overall and 41% of third-party breaches. These deposit account credential exposures showed significant growth, increasing 138% overall in the last six years and a whopping 356% in third-party breaches.

As cybercriminals seek to utilise GenAI deepfakes to get past biometric authentication systems, the exposure of government identification credentials has grown. Exposure of driver's licenses and other state-issued IDs grew 140% in the last six years and passports grew 120% in the same period. Medical histories (including diagnoses and physicians) were included in 33% of breaches overall, a 22% six-year increase, and 45% of third-party breaches, a 400% increase.

Top 10 Exposed Identity Credentials in US Data Breaches

Percentage of credentials exposed in a data breach



Source: TransUnion global intelligence network

TransUnion

Digital Fraud Trends

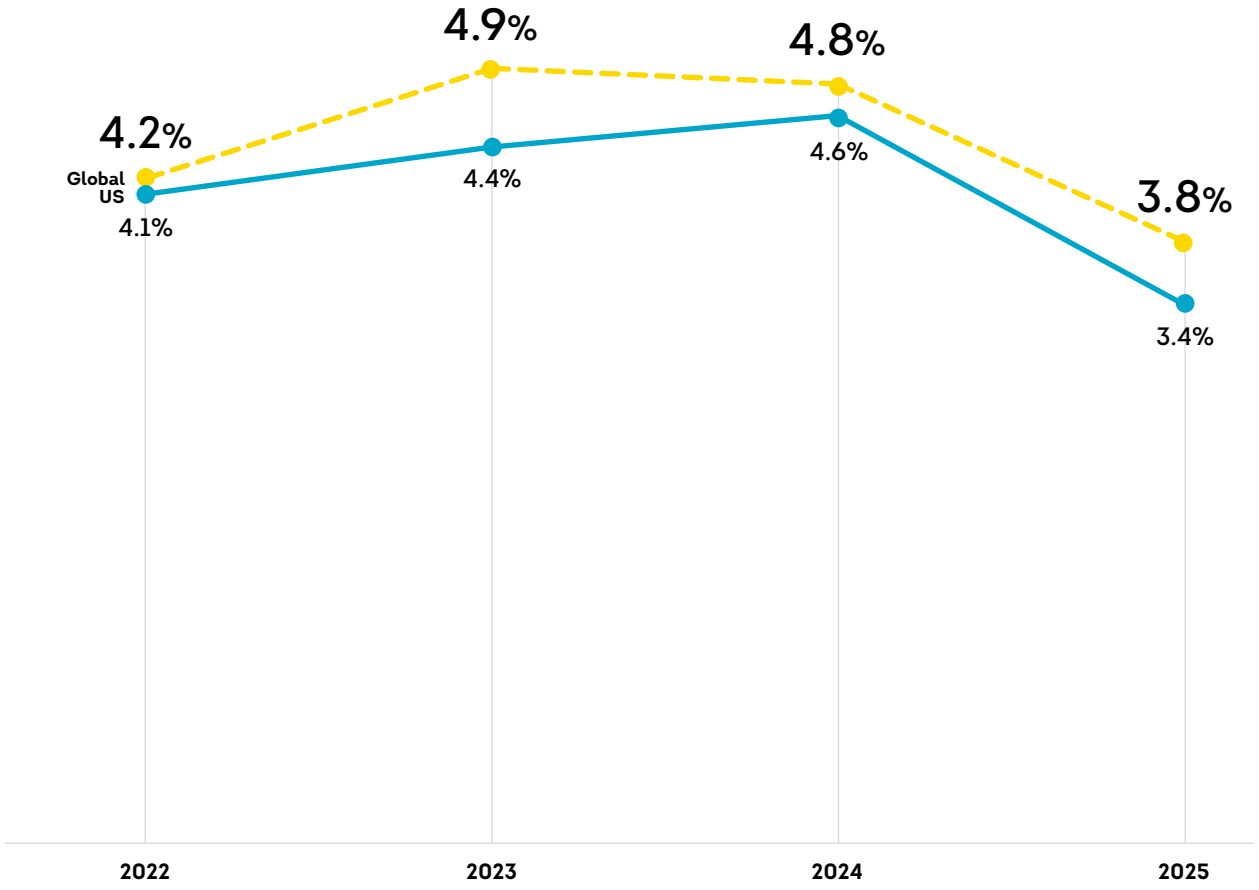
Suspected digital fraud rate declined as attacks grow more sophisticated

The suspected digital fraud rate for attempted transactions where the consumer was in the US fell 26% in 2025 compared to 2024. The rate fell to 3.4% in 2025, slightly lower than the global average of 3.8%.

Criminals tend to focus fraud attacks on the easiest targets while also using AI tools to beat outdated or fragmented fraud detection systems. Digital fraud risk trends seem to reflect this as fraudsters avoid trying to bypass stronger multifactor authentication systems directly, instead opting to use GenAI phishing and vishing scams targeting consumers.

Gaining access to login credentials from consumers emboldens fraudsters to successfully commit ATO using techniques to circumvent one-time passcodes and leverage secondary authentication methods, resulting in larger average losses prevalent in the US. Additionally, theft of personal identity information commonly leads to criminals' use of GenAI techniques, such as synthetic identities or deepfake identity credentials, and may be masking sophisticated fraud attacks at new account opening — without raising alarms until after losses occur days or months later.

Rate of Suspected Digital Fraud



Source: TransUnion global intelligence network

TransUnion

Communities industry experienced the highest digital fraud risk

The communities industry, which includes web properties and apps like online forums and dating sites, experienced the largest percentage (11.7%) of suspected digital fraud for attempted transactions where the consumer was in the US in 2025. This represents a 15% increase from 2024 to 2025 and 7% growth in the volume of suspected digital fraud between those two periods.

Other entertainment-oriented industries also experienced above-average rates of fraud risk. The gaming industry, including online betting sites and apps, continued to see suspected digital fraud attempts for nearly 1 of every 10 transactions (9.8%). Video gaming had an 8.3% rate of suspected digital fraud. Of note, the government industry saw the largest (19%) annual increase in the number of suspected digital fraud attempts of any industry analysed.

Digital Fraud Attempts From the US by Industry

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

Communities
(online dating, forums, etc.)

2025
11.7%

2024-2025
+7%

Gaming
(online sports betting, poker, etc.)

2025
9.8%

2024-2025
0%

Video gaming

2025
8.3%

2024-2025
-32%

Retail

2025
3.8%

2024-2025
-41%

Financial services

2025
3.2%

2024-2025
-23%

Logistics

2025
1.6%

2024-2025
-70%

Government

2025
0.8%

2024-2025
+19%

Insurance

2025
0.5%

2024-2025
-19%

Telecommunications

2025
0.4%

2024-2025
-22%

Travel & leisure

2025
0.2%

2024-2025
-47%

Source: TransUnion global intelligence network

Digital fraud risk impacts all stages of the consumer lifecycle

Every stage of the consumer lifecycle exhibited similar levels of digital fraud risk in the US. In 2025, account creation was slightly riskier than account login and financial transactions. Account creation attempts had the highest rate (3.8%) of suspected digital fraud in the consumer lifecycle for transactions where the user was in the US in 2025 — yet substantially lower than the 8.3% seen globally. Account logins and financial transactions (3.6% and 3.3%, respectively) were similarly risky transactions where the user was in the US in 2025.

Account creation digital risk was driven by specific industries: 35.2% of telecommunications, 28.1% of retail and 21.3% of communities account creation transaction attempts from the US were suspected digital fraud in 2025. At the same time, insurance had the highest account login risk with 42.7% of login transaction attempts from the US suspected of digital fraud.

Consumer Lifecycle Stage Examples

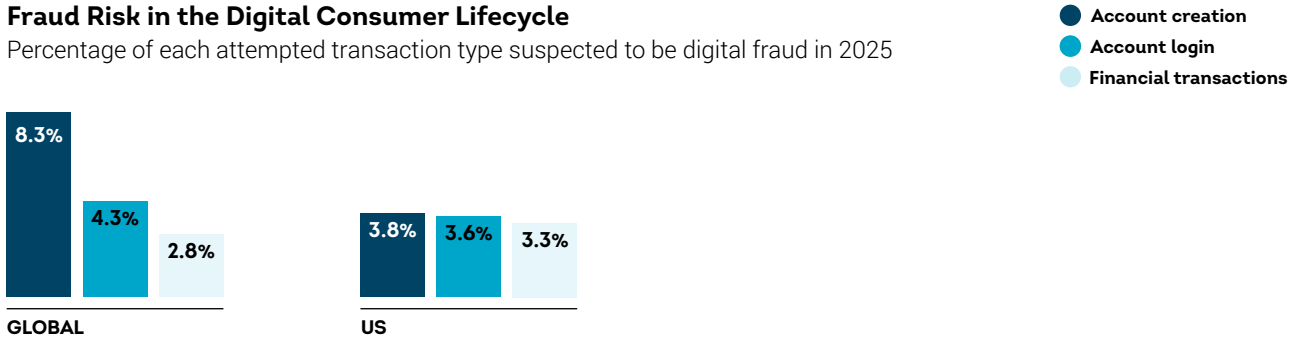
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

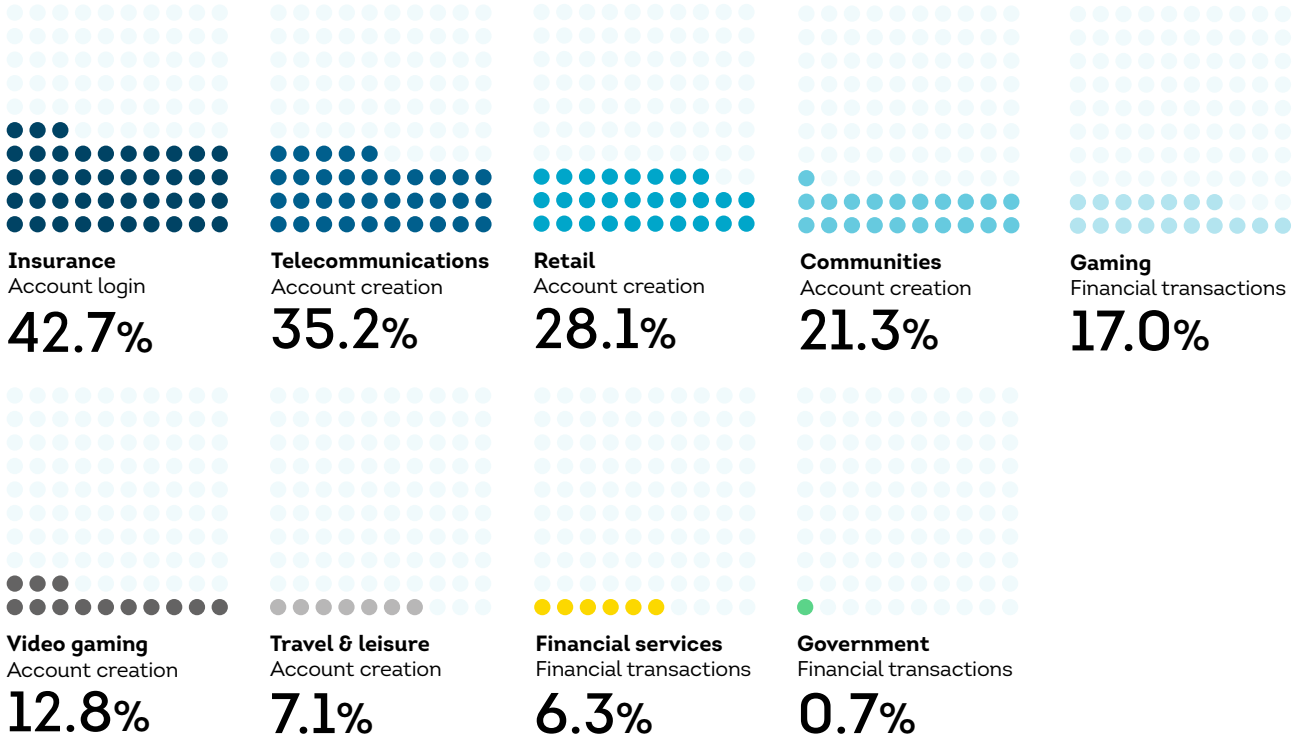
Percentage of each attempted transaction type suspected to be digital fraud in 2025



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 from the US by industry, and the corresponding percentage in that stage in 2025



Source: TransUnion global intelligence network

TransUnion

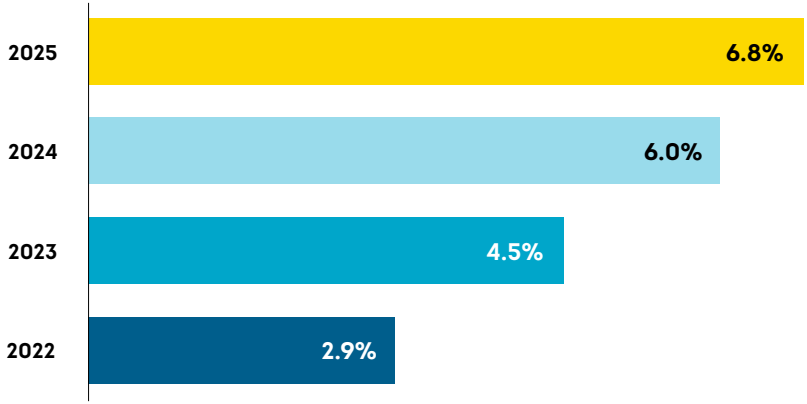
Call Centre Fraud Trends

High-risk calls into call centres continue to rise

Organisations' call centres represent a high-trust channel consumers depend on. Call centres are also a target for criminals to facilitate ATO by socially engineering call centre agents into revealing customer data or changing account details.

Measuring the risk of inbound calls to US call centres, TransUnion documented a 13% increase (to 6.8%) in the percentage of high-risk calls from 2024 to 2025. High-risk calls are any that either obtain a score of 0 or 100. The highest-risk phone calls increased in three of four channels monitored during that period.

High-Risk Calls Into US Contact Centres



Source: TransUnion global intelligence network

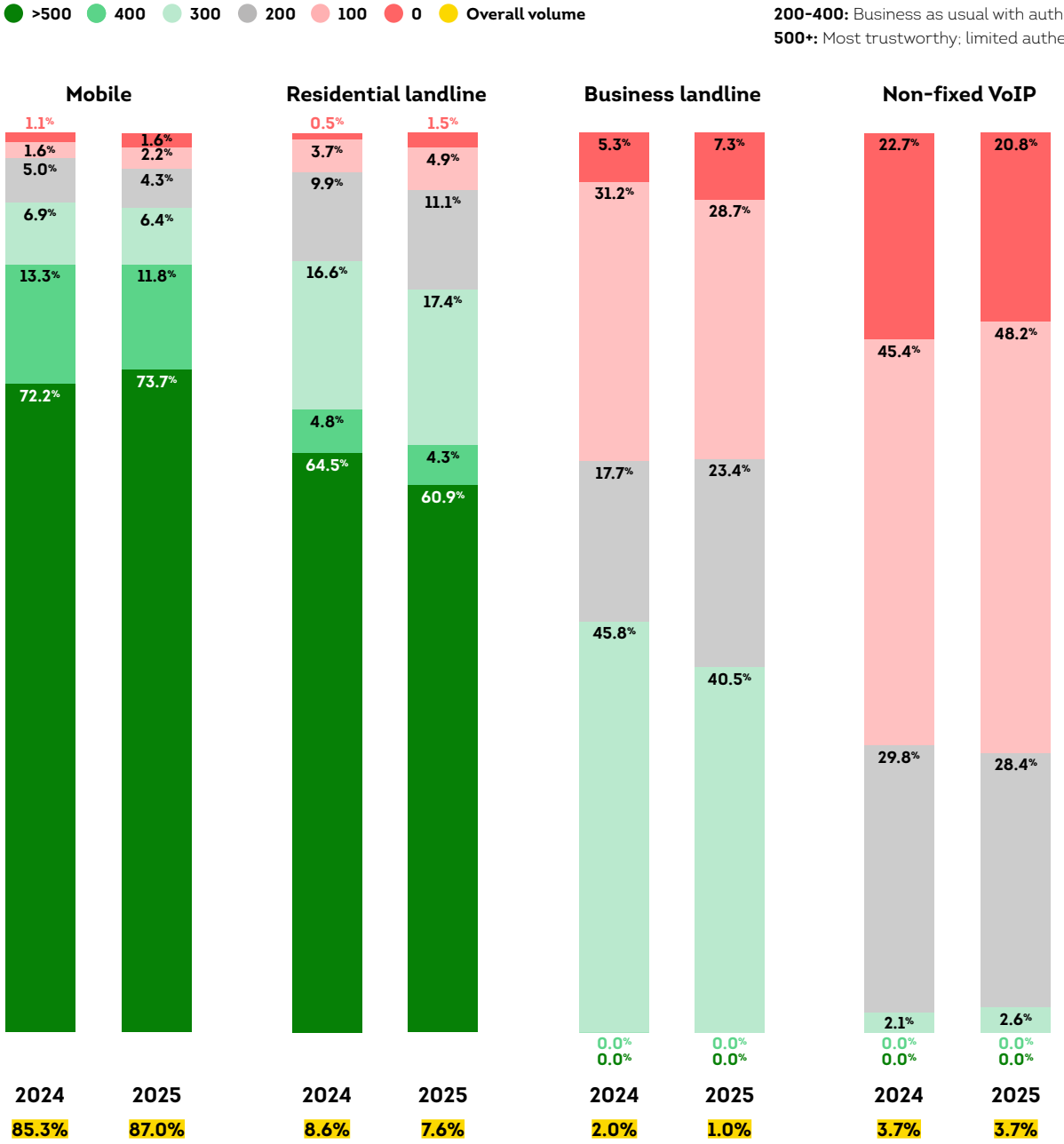
TransUnion

Mobile inbound call risk jumps in call centres

The vast majority (87%) of calls received by TransUnion's US call centre clients in 2025 were from mobile phones and they were riskier than 2024. While just 3.8% of mobile calls were identified as being the highest risk for fraud; that's a 41% increase from 2.7% in 2024.

The riskiest channel for the contact centre was non-fixed Voice over Internet Protocol (VoIP), a phone number that isn't associated with a physical device. While that channel represented only 3.7% of total call volume, 69% of those calls were identified as high risk for fraud in 2025.

US Call Centre Risk by Channel and Overall Volume



Call risk score tiers

0 & 100: Highest; step-up authentication
200-400: Business as usual with authentication
500+: Most trustworthy; limited authentication

Source: TransUnion global intelligence network

TransUnion

Synthetic Identity and Credit Washing Trends

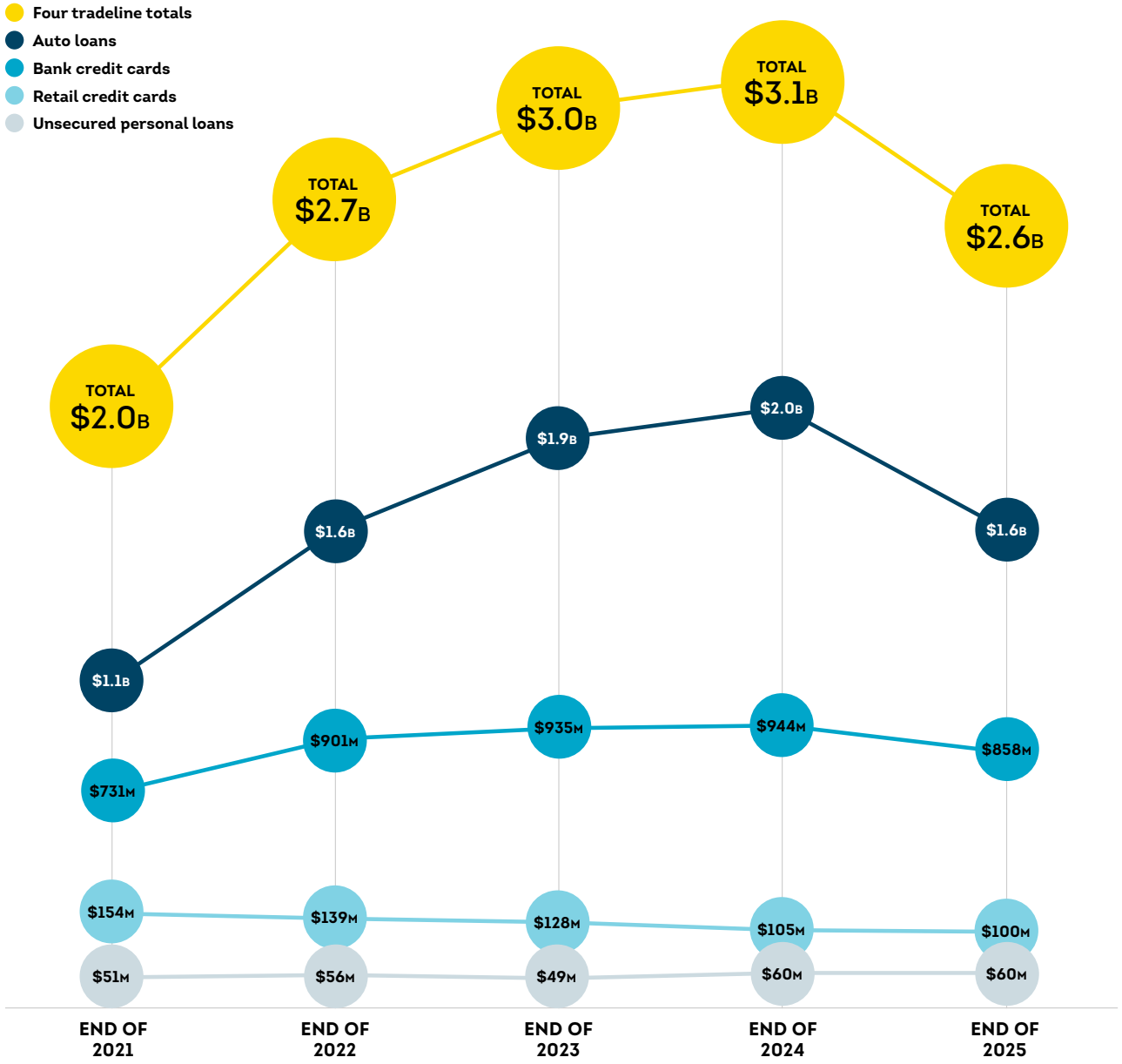
Synthetic identity exposure in lending remains persistently high

Synthetic identities continue to be a high-risk attack vector for organisations' new account creation processes; powered by compromised credentials and supercharged by GenAI. According to TransUnion's consumer credit data, total exposure to synthetic identities among accounts opened by US lenders for auto loans, bank credit cards, retail credit cards and unsecured personal loans was USD 2.6 billion in potential losses at the end of 2025.

Building credit accounts to establish a believable personal history remains a core tactic for synthetic identities, providing legitimacy and making fabricated profiles difficult to detect. As GenAI tools make it easier to generate realistic deepfake documents and create synthetic identities at scale, criminals are expanding beyond financial services. The dip in lending exposure for US lenders may portend a shift in the use of synthetics to less-prepared industries, such as education, FinTech, government, healthcare, retail and telecommunications — widening the surface area for synthetic fraud.

Synthetic Identity Risk for US Lenders 2021–2025

The total credit amount (USD) synthetic identities have access to for US auto loans, bank credit cards, retail credit cards and unsecured personal loans



Source: TransUnion global intelligence network

TransUnion

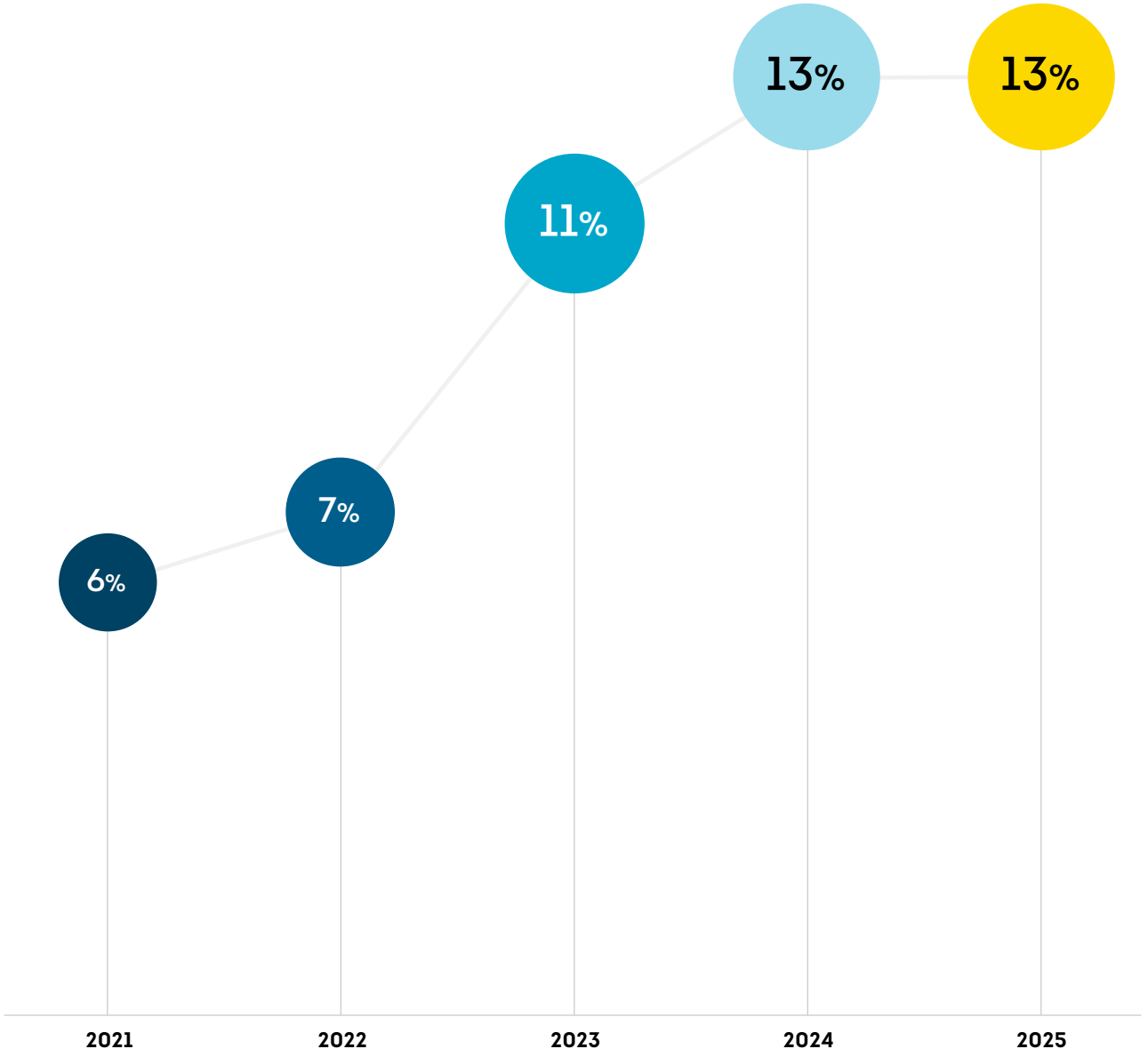
Credit washing breathes new life into risky identities

Criminals bolster altered or synthetic identities with legitimately built credit histories, making it hard to distinguish them from real people. After busting out, they can either abandon an identity or attempt to recycle it. That's where credit washing comes in.

Credit washing is a credit manipulation scam to remove legitimate negative information from an identity's credit history by making a false claim of identity fraud. These false credit report disputes could be made against accounts opened using a stolen consumer identity or synthetic identity — or unauthorised transactions on a consumer's legitimate credit account.

Consumers in the US (or their authorised representatives) have a legal right to dispute inaccurate items on their credit reports, and TransUnion follows a highly regulated dispute resolution process. In 2025, consumer credit report disputes in the US claiming fraud represented 13% of all disputes, unchanged from 2024.

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



Source: TransUnion global intelligence network

TransUnion

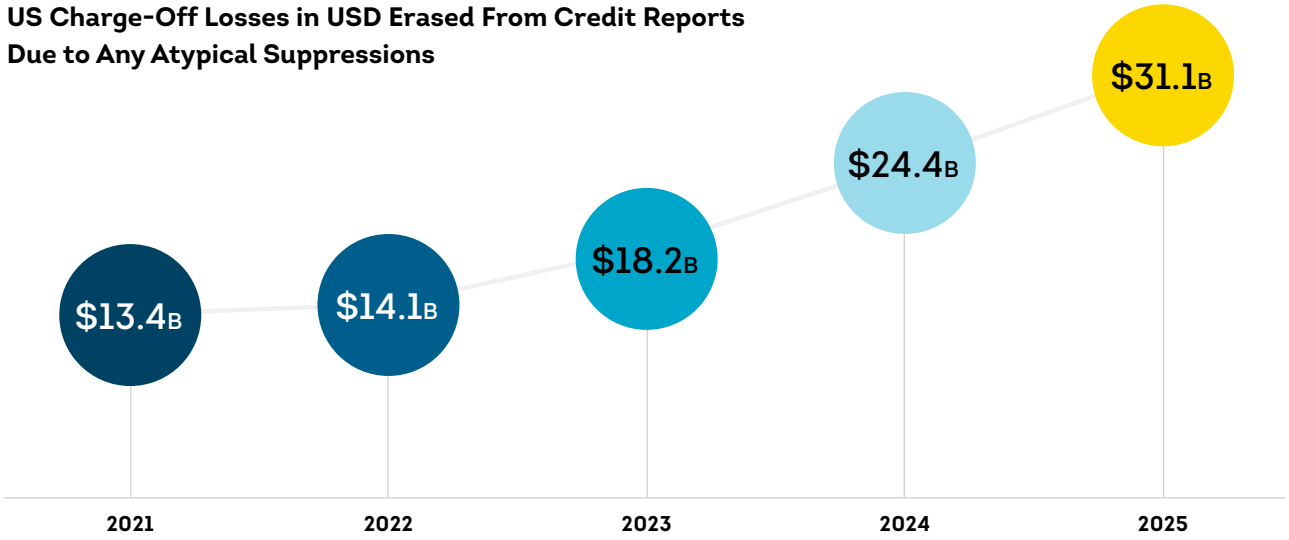
Atypical suppression charge-off growth illustrates credit washing risk

If debt goes unpaid after a period of time, financial institutions typically write it off, calling it a "charge-off." Charge-off losses are a known risk in lending. At the same time, charge-offs result in a negative report on an identity's credit report, impacting their credit score. However, when the negative credit report — be it a loan, credit account or a transaction — is successfully disputed by a consumer as fraud, the result is still a charge-off, but the item is suppressed from credit scoring models as if it never happened; what's referred to as an "atypical suppression."

Atypical suppressions may be reported to credit bureaus by financial institutions or directly by consumers using the credit dispute process. While this is an important tool for consumers to protect themselves from fraud, it also can be a scam method for bad actors to recycle identities used to perpetrate fraud — credit washing.

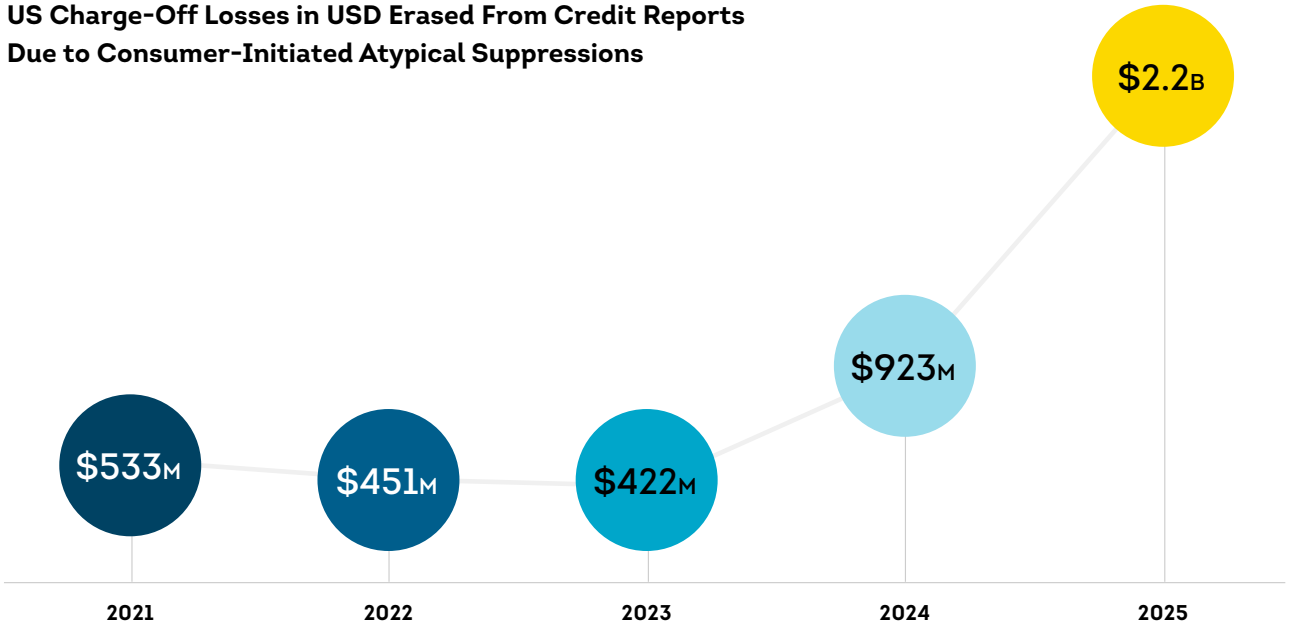
The scale of potential credit washing has been dramatic, especially from consumer-initiated suppressions. Charge-off losses erased from US credit reports due to any atypical suppression grew by 28% from 2024 to more than USD 31 billion at the end of 2025. Consumer-initiated charge-off suppressions, representing about 7% of all atypical charge-off suppressions at the end of 2025, increased 138% since the end of 2024, surpassing USD 2 billion for the first time.

US Charge-Off Losses in USD Erased From Credit Reports Due to Any Atypical Suppressions



Source: TransUnion global intelligence network

US Charge-Off Losses in USD Erased From Credit Reports Due to Consumer-Initiated Atypical Suppressions



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.

Call centre

TransUnion's call centre findings were based predominantly on data from both large and small financial institutions based in the US. The rate or percentage of high-risk calls was determined by the assessment of multiple risk factors.

Consumer credit report disputes

TransUnion's consumer credit report dispute findings were based on US consumer credit data from US states, territories, protectorates and US and overseas military bases. It's routinely sourced from more than 50 years of consumer credit data and contains credit information on approximately 400 million consumers.

Consumer survey

This online survey was conducted 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.

Data breaches

TransUnion obtains its proprietary breach data in partnership with the Identity Theft Resource Center (ITRC). The ITRC staff tracks all US publicly reported data exposure events from sources that include state attorneys general, breached entity press releases, law firms, cybersecurity experts and more. TransUnion expands the ITRC data with a process that computes each breach's top risks, appropriate actionable consumer steps and Breach Risk Score (BRS). The BRS is based on the quantity and severity of the particular identity credentials the affected entity determined to have been exposed. From among 60 possible identity credential choices, each breach is run through TransUnion's TruEmpower Identity Threat Profile to produce a risk score and pattern, and prescribed consumer actions. The BRS uses a 1–10 scale where 1 represents least severe and 10 represents most severe.

Digital fraud

TransUnion uses intelligence from billions of transactions originating from over 40,000 websites and apps. 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.

Synthetic fraud

TransUnion's synthetic fraud findings were based on US consumer credit data from US states, territories, protectorates and US and overseas military bases. It's routinely sourced from more than 50 years of consumer credit data and contains credit information on approximately 400 million consumers. The synthetic fraud analysis encompasses US credit activity recorded between Jan. 1, 2009 and Dec. 31, 2025. Lender exposure measures were based upon TransUnion's proprietary formula to capture potential total loss at risk for lenders.

ABOUT TRANSUNION (NYSE: TRU)

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

transunion.co.uk/business

TransUnion