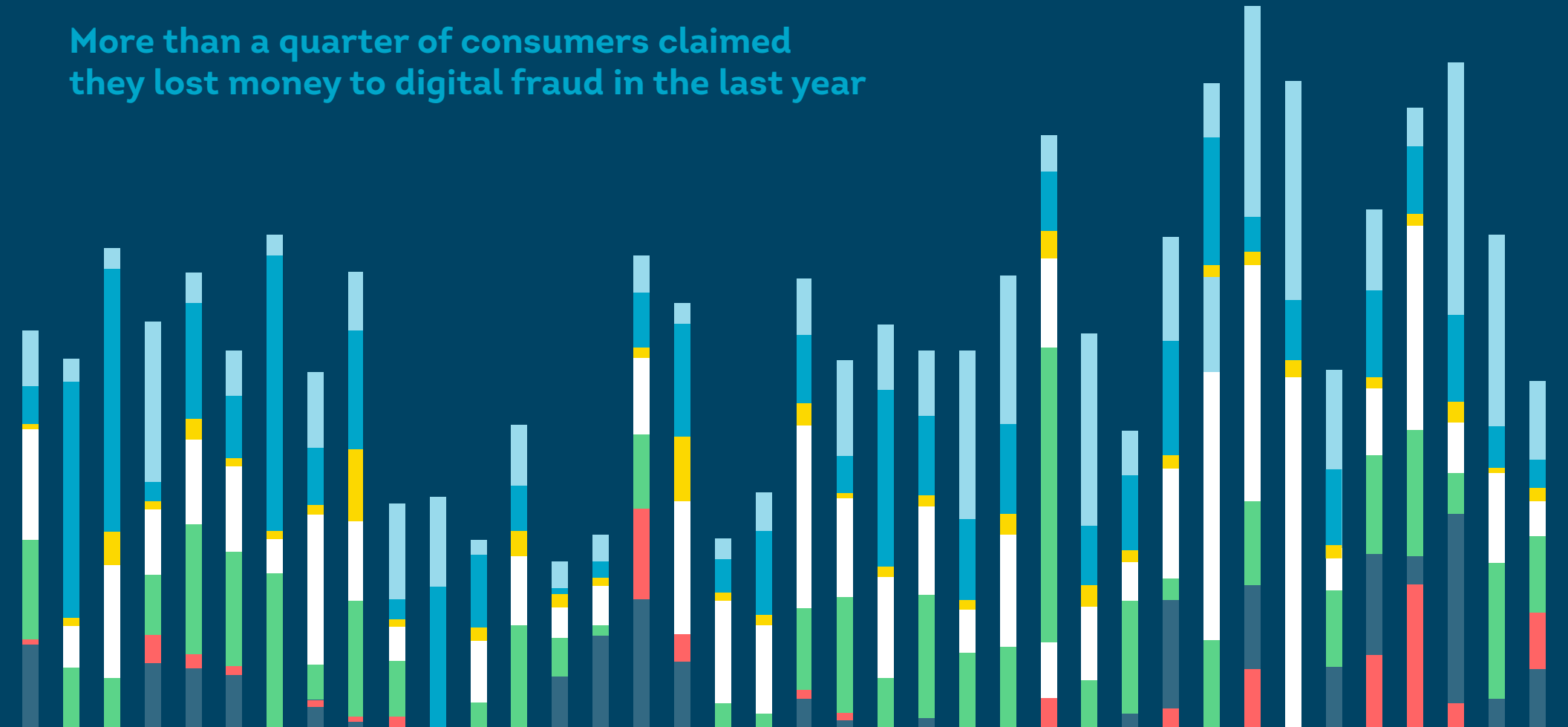
TransUnion

H1 2026 UPDATE: TOP FRAUD TRENDS

THE IMPERSONATION EPIDEMIC DRIVES COSTLY FRAUD ATTACKS

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



Executive Summary

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

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

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

KEY TAKEAWAYS

Identity-based fraud impacts consumer trust – and wallets

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

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

Fraud risk persists at every stage of the consumer lifecycle

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

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

Compromised identities increase risk of sophisticated fraud attacks

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

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

TransUnion

About the Research

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

How to apply these insights

Use this report as a strategic guide to:

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

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

Interpreting the data

Consumer survey findings

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

Digital fraud metrics

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

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

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

TransUnion

Contents

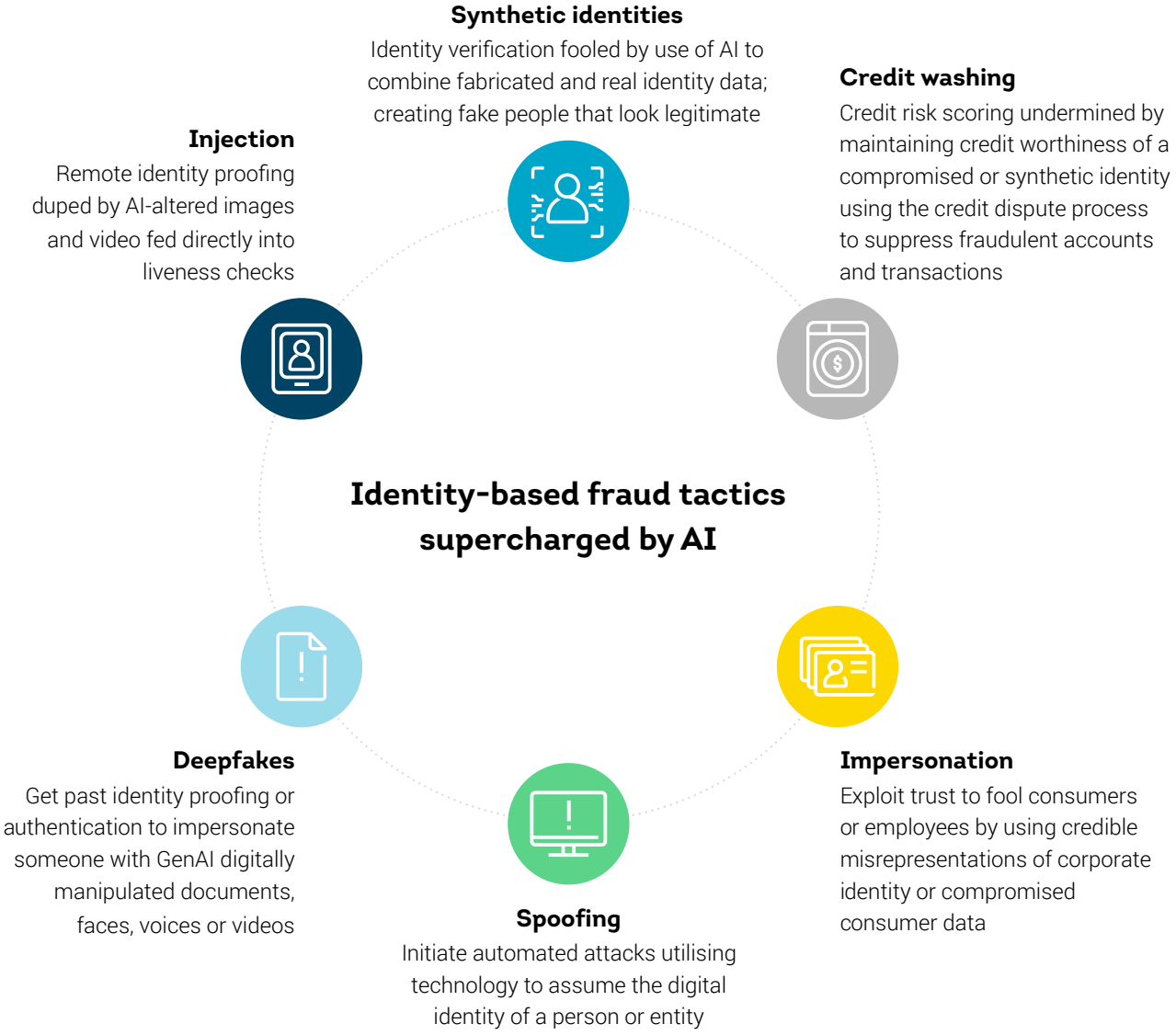
Are Your Customers Real?

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

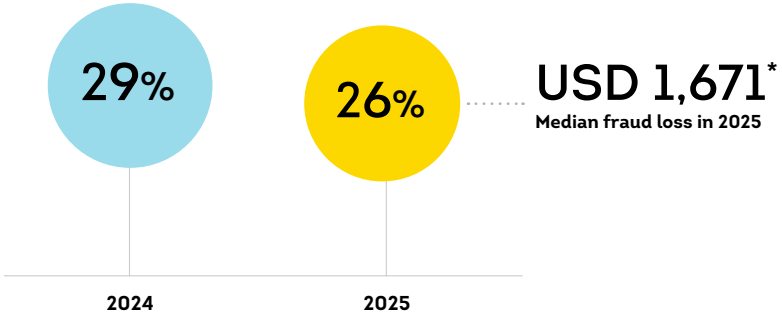
Gen Z most susceptible to losses from trust-based fraud schemes

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

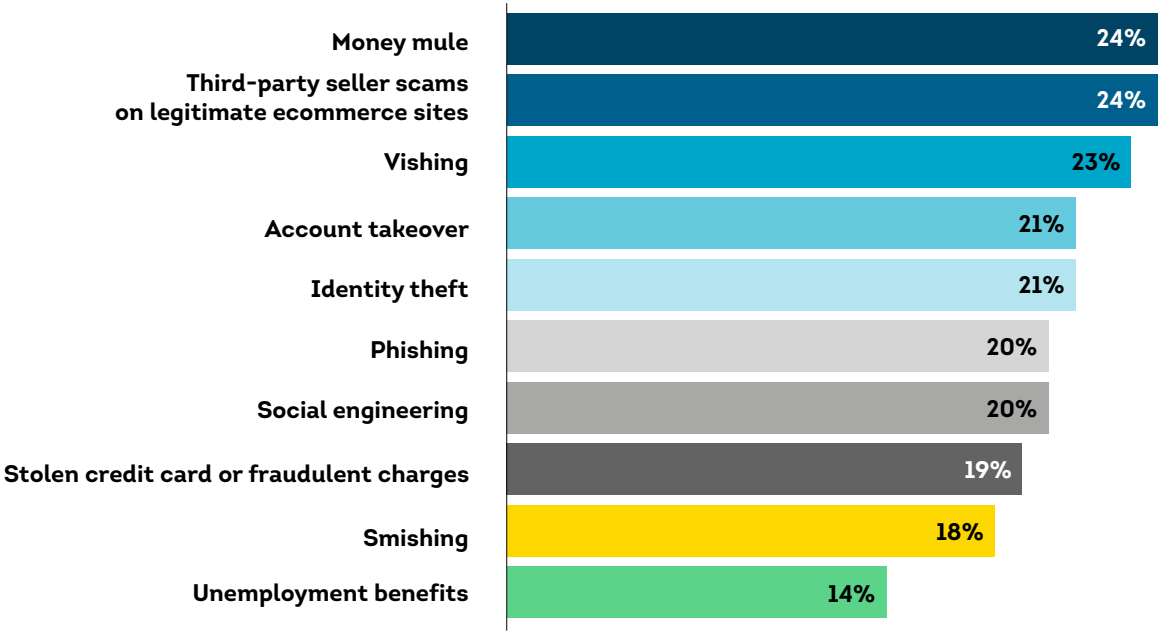


*USD conversion based on currency exchange value on Dec. 29, 2025

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

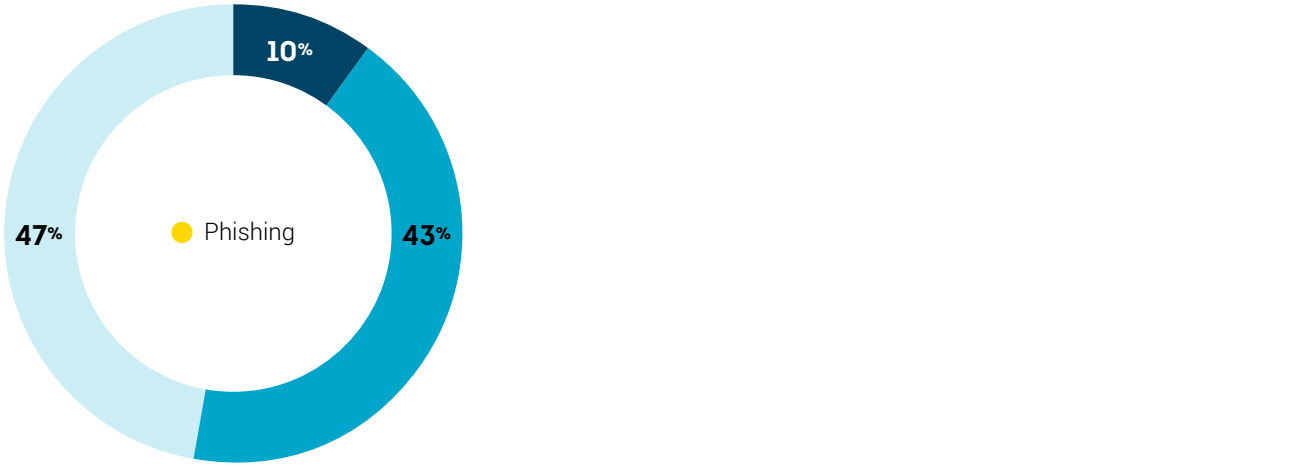
Identity-exposing scams dominate consumer reported fraud

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

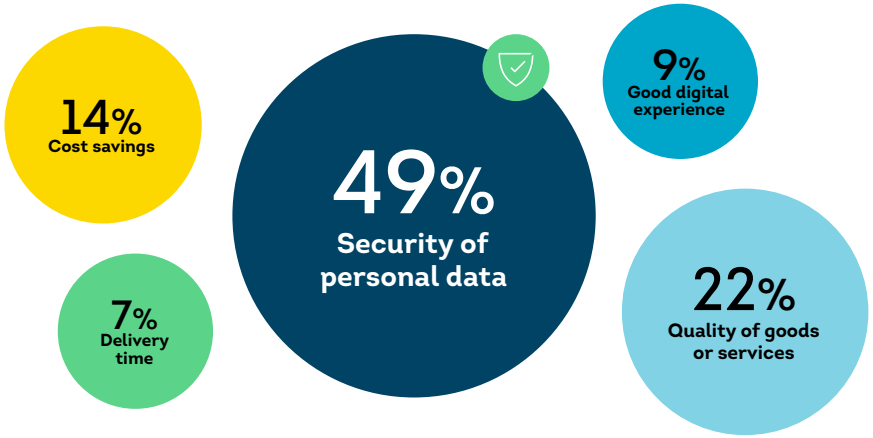
Safe and seamless online transactions drive consumer brand preference

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%.

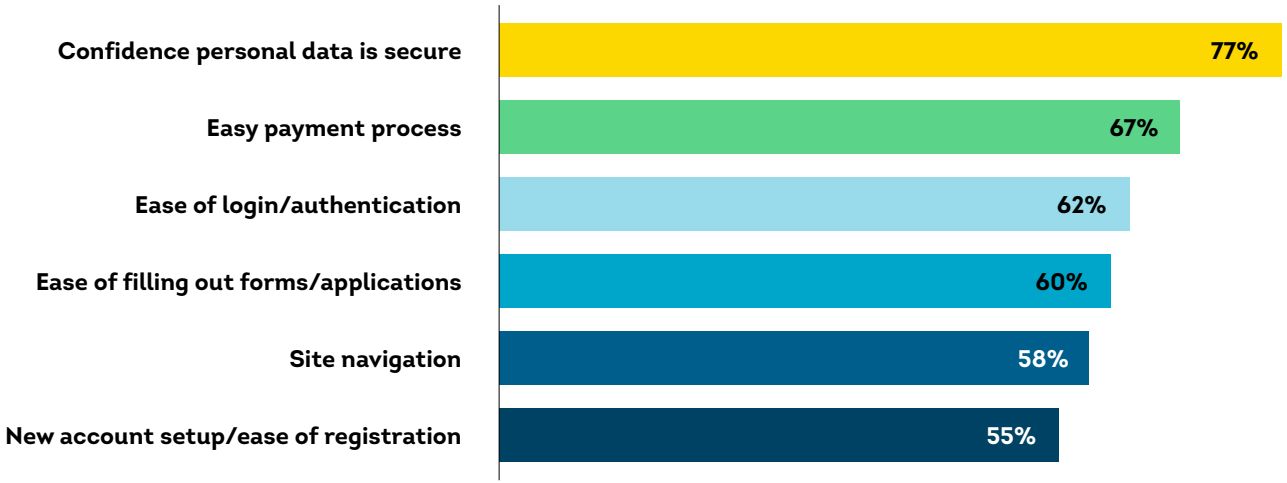
To gain more customers, organisations need to demonstrate trust when it comes to consumer data. About half (49%) of consumers ranked personal data security as the highest expectation or quality in preferred online companies. Not only that, over three-quarters (77%) said confidence their personal data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

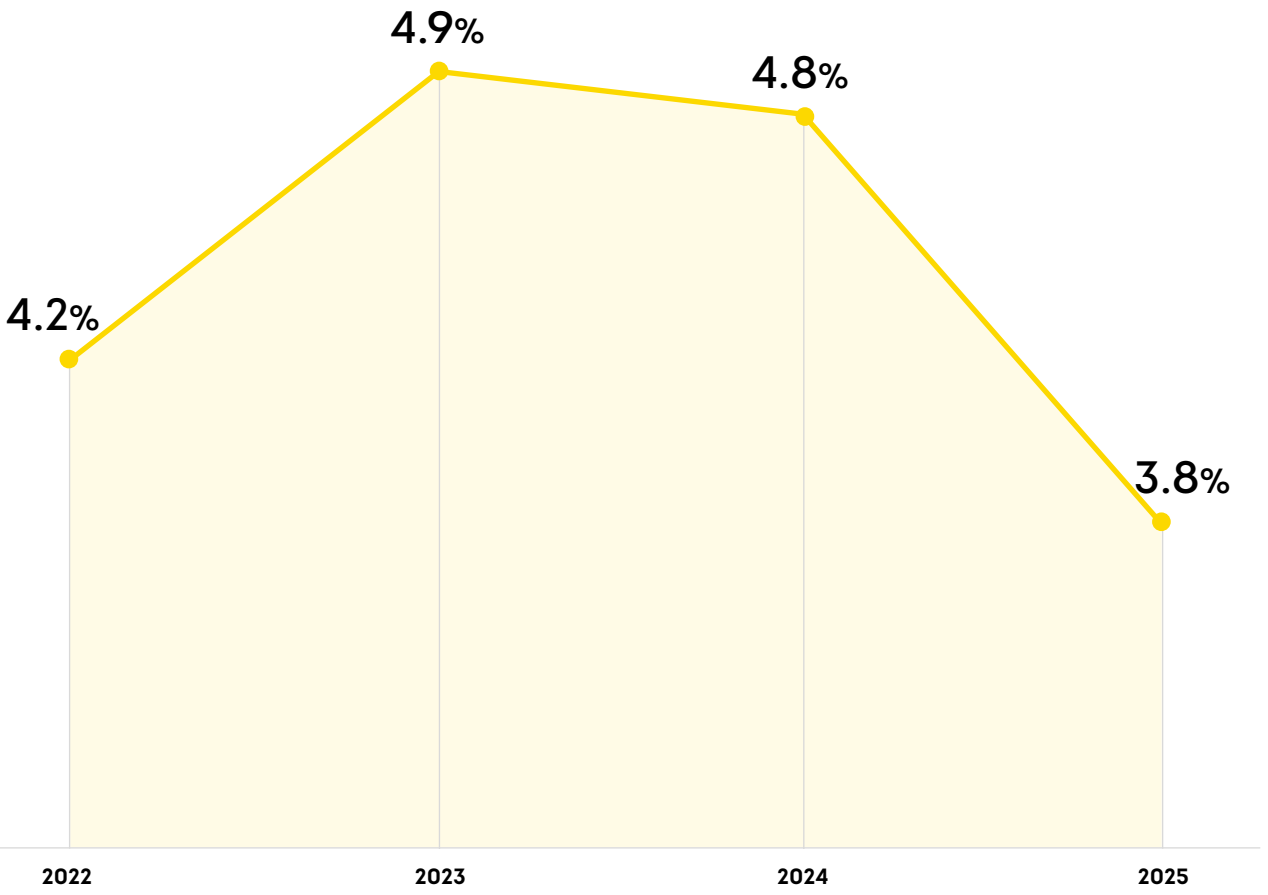
Digital Fraud Trends

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

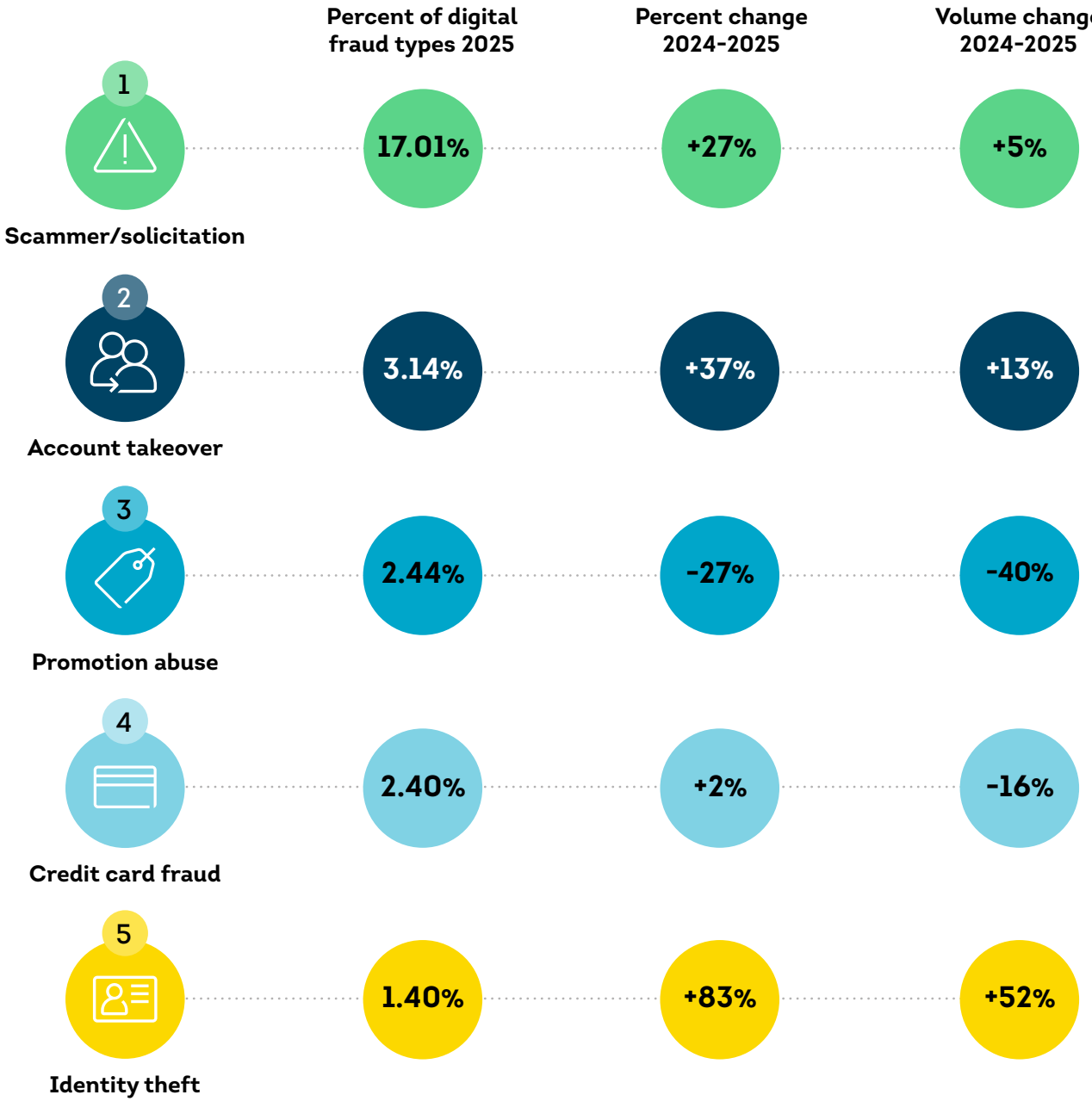
TransUnion

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

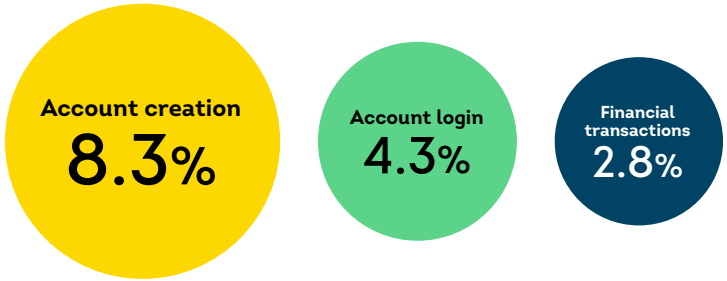
Account creation: Account signup, registration and loan origination

Account login: Login and failed login events

Financial transactions: Purchases, withdrawals and deposits

Fraud Risk in the Digital Consumer Lifecycle

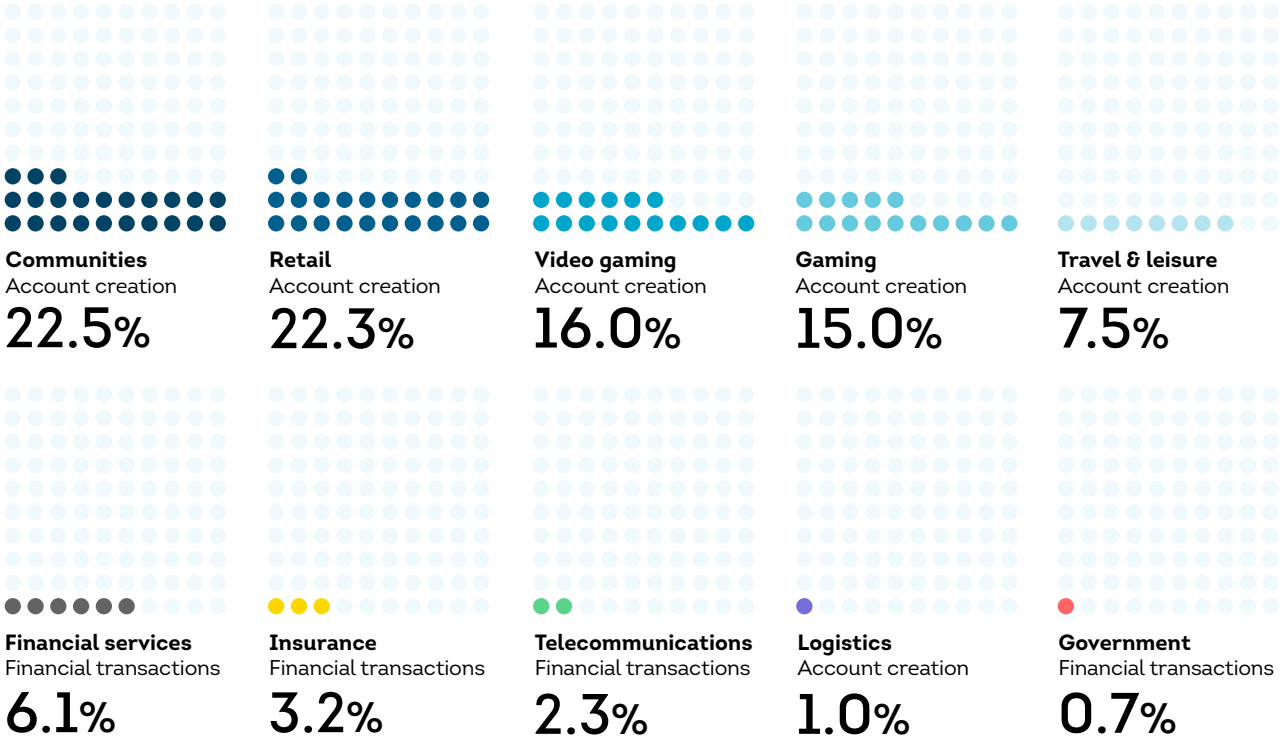
Percentage of each attempted transaction type suspected to be digital fraud in 2025



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


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

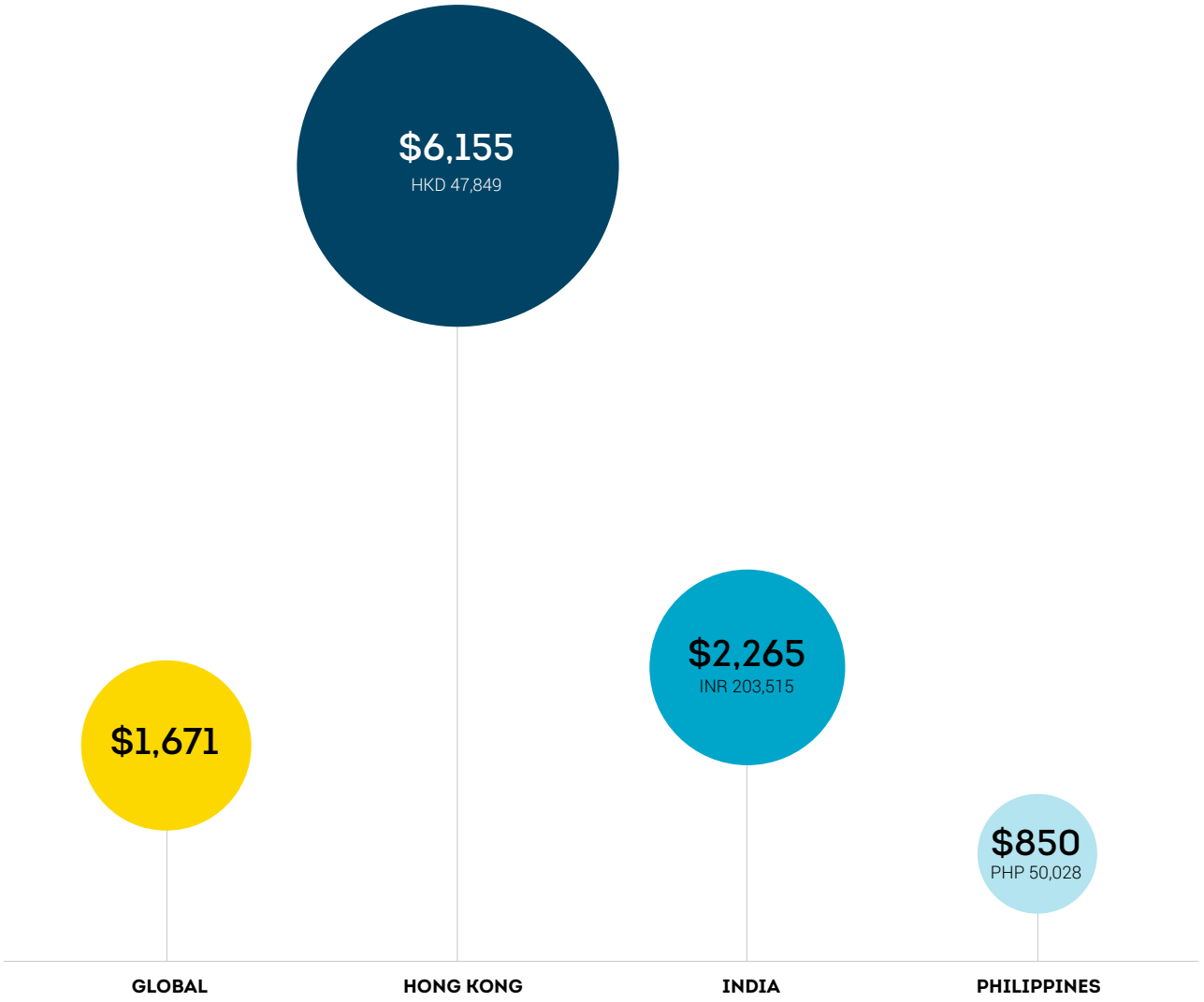
Indian consumers who said they lost money in the last year due to digital fraud reported a median loss of USD 2,265 (INR 203,515) in that period — 36% above the global median. They reported losing money in the past year due to schemes like phishing, vishing, smishing and third-party seller scams on legitimate 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



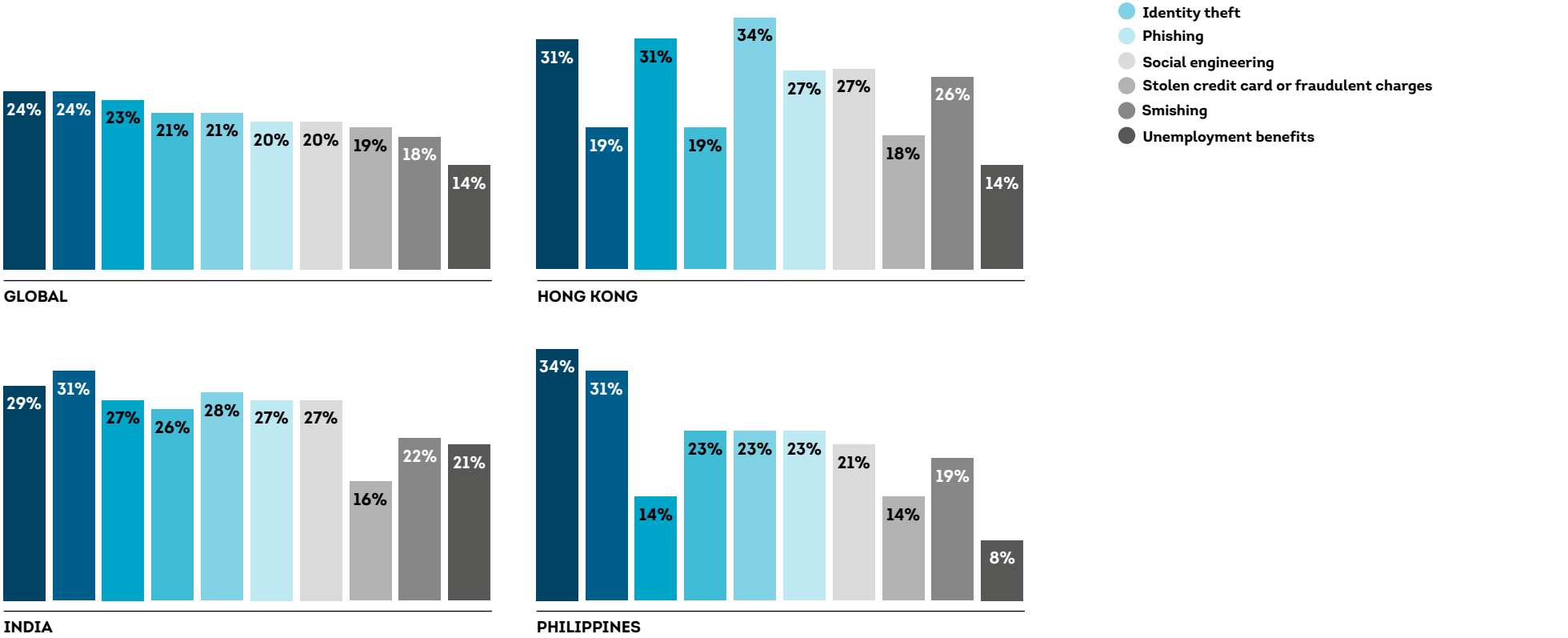
*USD conversion based on currency exchange value on Dec. 29, 2025
**The global median is the average of the 18 countries surveyed

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

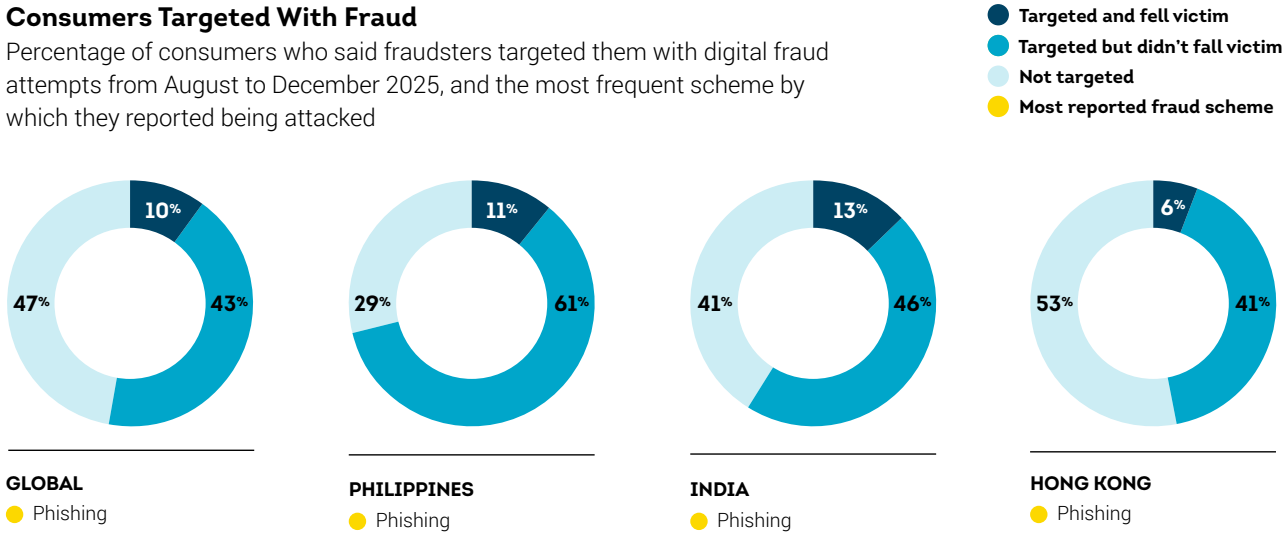
Indian consumers reported higher than global targeting and victimisation when asked if they were targeted by digital fraud attempts in the last three months, with 59% saying they were targeted and 13% of them reporting they fell victim. Among those who said they were targeted, phishing was the most reported 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

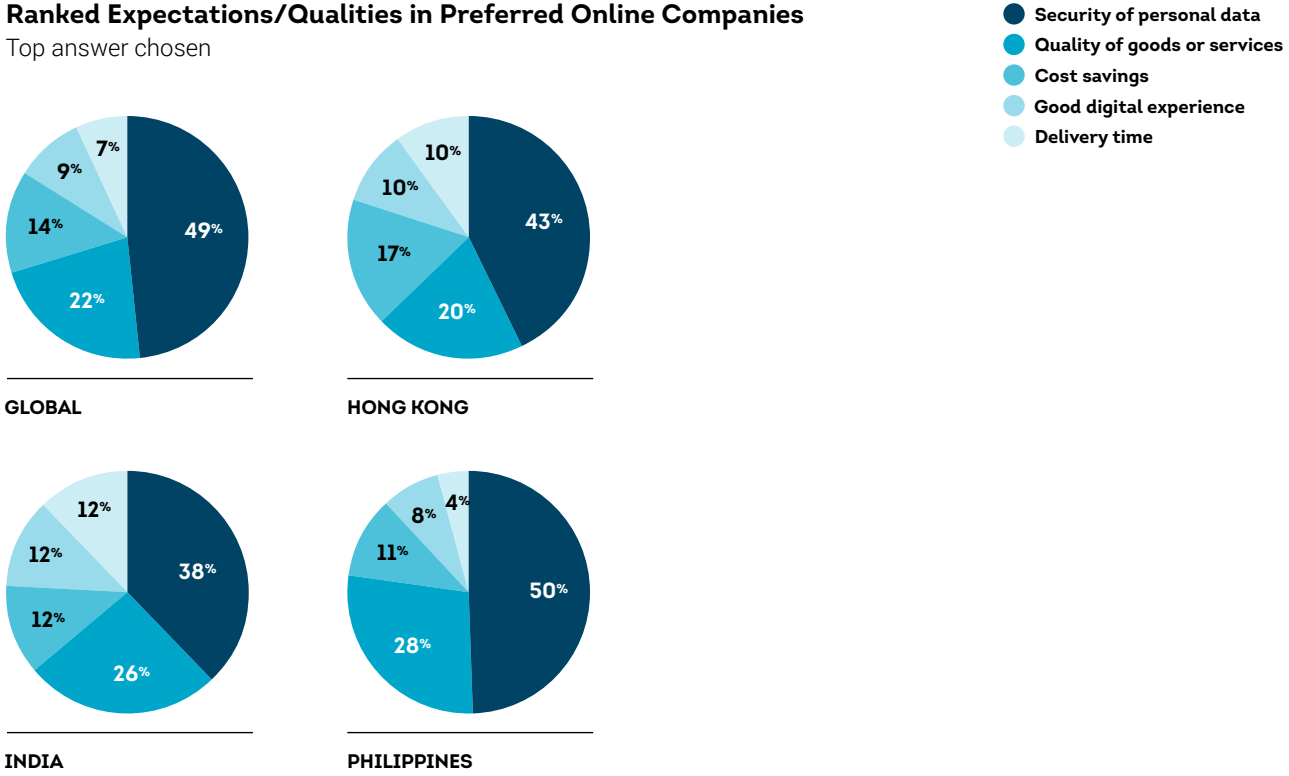
Security and convenience work together as core decision factors, highlighting a digital environment where trust and low friction are equally central to consumer choice. In India, security of personal data (38%) and quality of goods and services (26%) were the top expectations they consider when deciding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

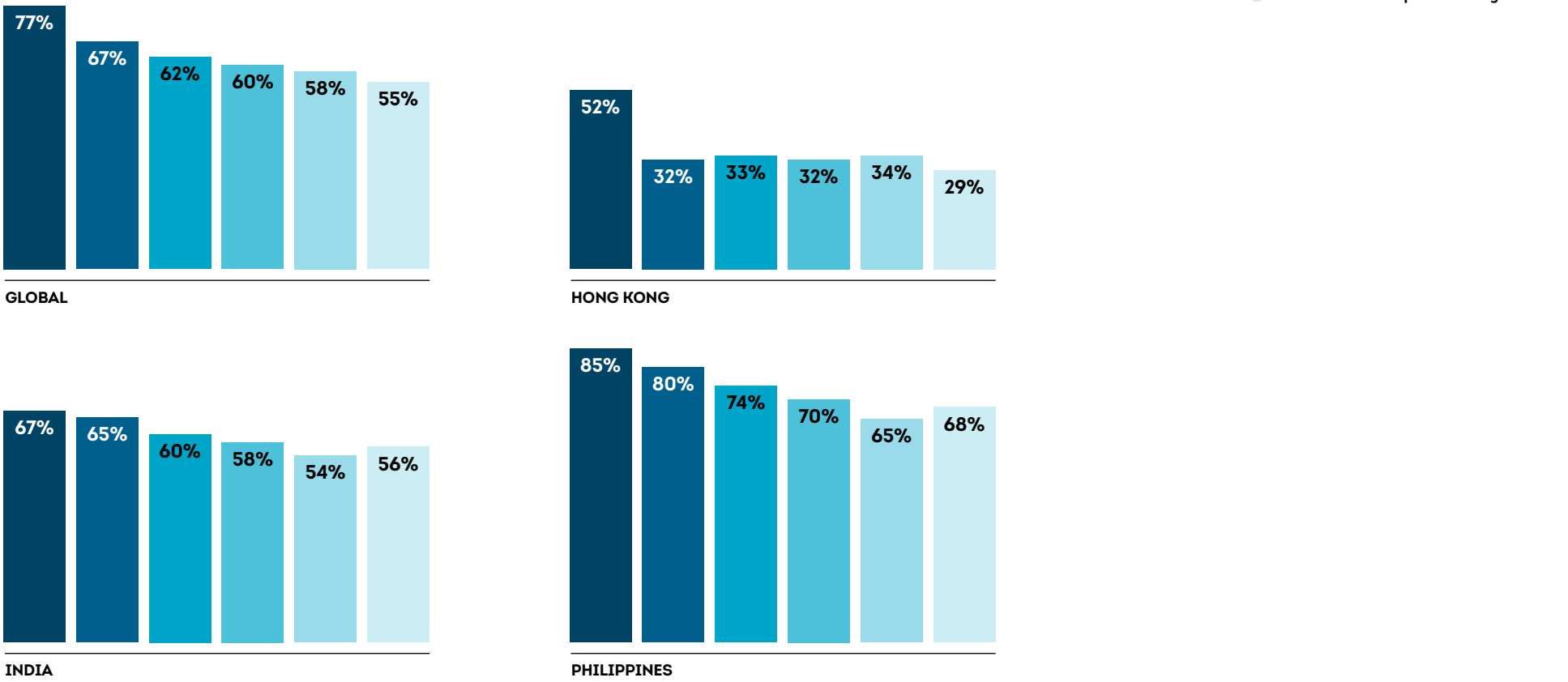


Source: TransUnion consumer survey

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

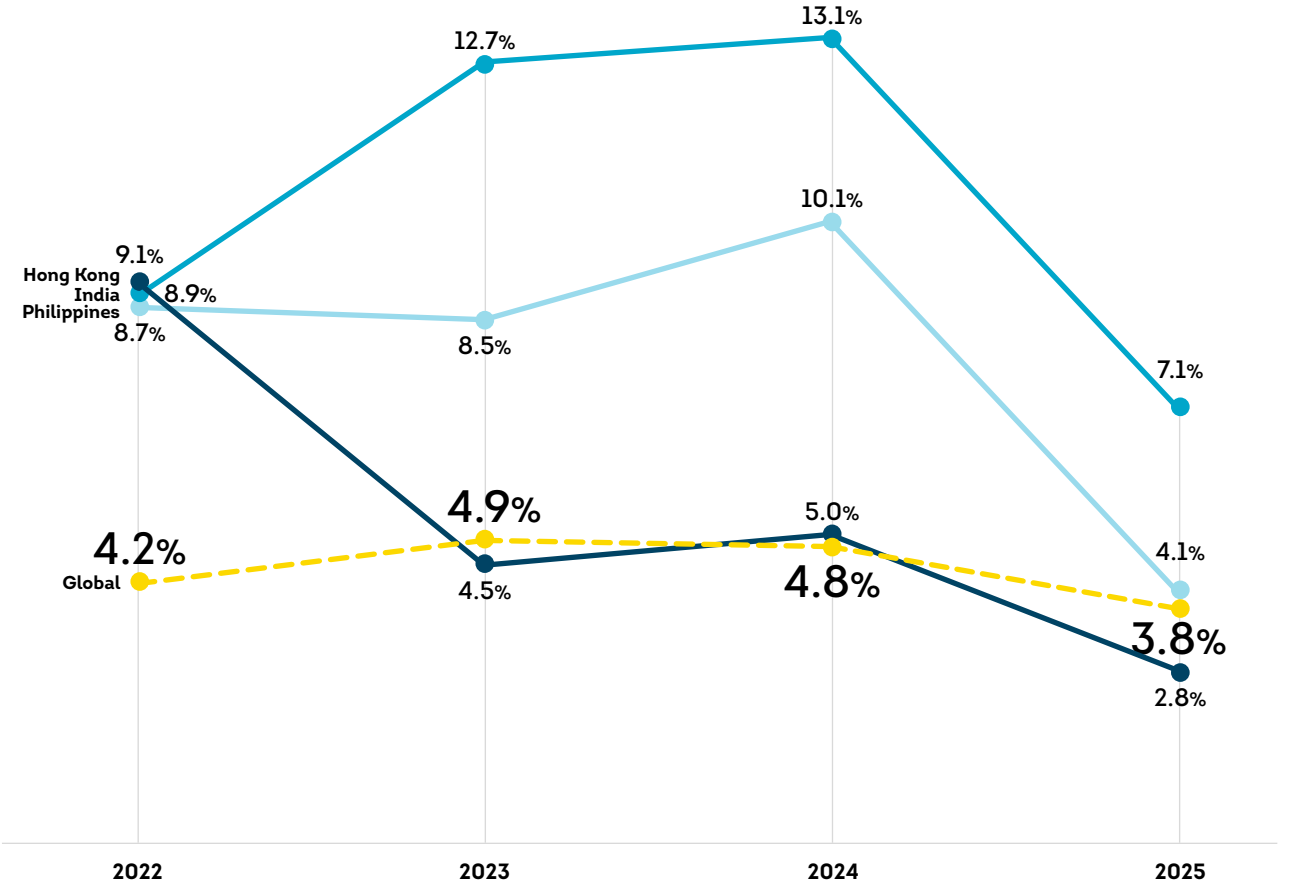
Even as suspected digital fraud attempts decreased across countries analysed in the region, the rate (5.9%) for those countries combined in 2025 still sat above the global rate.

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).

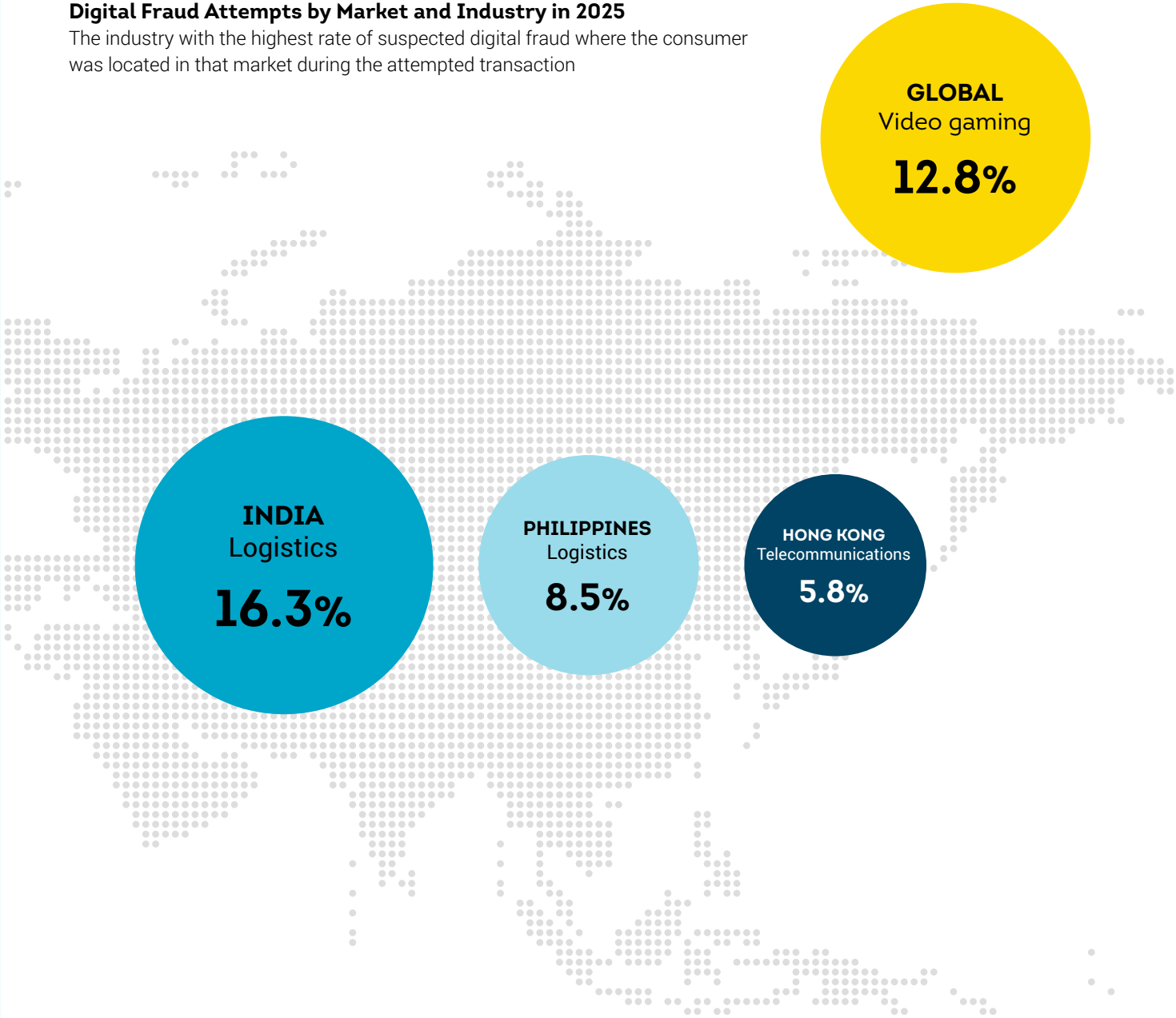
In Hong Kong, telecommunications recorded the highest level of suspected digital fraud attempts in 2025 at 5.8%, exceeding the global benchmark and outpacing sectors like communities and financial services.

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.

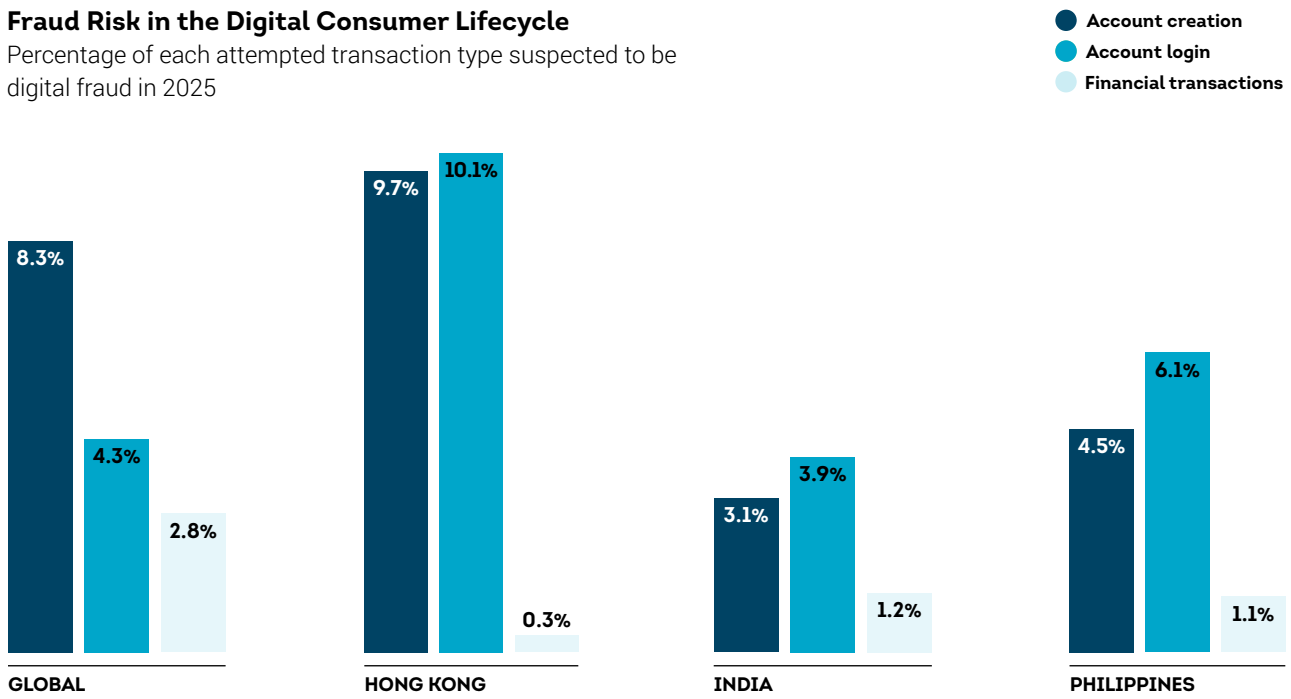
For transactions where the consumer was in India, fraud penetration across the digital consumer lifecycle was lower than global levels, with suspected digital fraud at account creation (3.1%), account login (3.9%) and financial transactions (1.2%) in 2025. Account creation suspected digital fraud was 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

Conclusion

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

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

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

Data Sourcing Methodology

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

Consumer survey

This online survey was conducted Nov. 20–Dec. 9, 2025 in Brazil (1000 respondents), Canada (999), Chile (499), Colombia (853), the Dominican Republic (415), Hong Kong (1000), India (950), Kenya (495), Mexico (500), Namibia (308), the Philippines (821), Puerto Rico (218), Rwanda (308), South Africa (1000), Spain (999), the UK (1000) and US (1000), and Zambia (365) by TransUnion in partnership with third-party research provider, Dynata. Adults 18 years of age and older were surveyed using an online research panel method across a combination of desktop, mobile and tablet devices. Survey questions were administered in Chinese (Hong Kong), English, French (Canada), Portuguese (Brazil) and Spanish (Colombia, the Dominican Republic, Mexico, Puerto Rico and Spain). To ensure Data Sourcing Methodology representation across resident demographics, the survey included quotas to balance responses across key demographics like age, gender and income. Please note some chart percentages may not add up to 100% due to rounding or multiple answers being accepted.

Digital fraud

TransUnion uses intelligence from billions of transactions originating from over 40,000 websites and apps. Suspected digital fraud attempts reflects those which TransUnion clients determined met one of the following conditions based on device risk indicators: 1) denial in real time due to fraudulent indicators, 2) denial in real time for corporate policy violations, 3) fraudulent upon client investigation, or 4) a corporate policy violation upon client investigation. The country and regional analyses examined transactions in which the consumer or suspected fraudster was located in a select country or region when conducting a transaction. Global statistics represent every country worldwide and not just the select countries and regions.

ABOUT TRANSUNION (NYSE: TRU)

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

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

TransUnion