

H2 2026 UPDATE: TOP FRAUD TRENDS

Fraud in the Age of Continuous Trust

Evaluating risk when identities, communications and established relationships are compromised

TransUnion

CONTENTS

3 **Executive Summary**

4 **Authors and Contributors**

5 **Inside the Global Trust Landscape**

Synthetic identities are redefining trust

Communications have become the new fraud battleground

AI is enabling criminal networks to operate on an industrialised scale

23 **Regional Perspectives**

Africa Overview

28 **Shaping the Next Era of Digital Trust**

31 **About the Research**

Executive Summary

Business leaders globally estimate their organisations lost an average of 6.5% of revenue to fraud in the last year. Those losses are a symptom of a larger problem: Fraud is succeeding because trust has become easier to exploit and harder to establish. And because trust underpins growth, customer relationships, operating efficiency and brand reputation, fraud has evolved from an operational challenge into a strategic business risk.

For years, identity verification served as the foundation of digital trust: establish trust at onboarding, authenticate users and approve transactions. That foundation remains critical, but it's no longer enough.

Identity verification alone can't carry the weight of fraud prevention. Fraud increasingly exploits identities after they're verified, communications after they're delivered and relationships after they're established. The critical question is no longer simply, "Is this the right person?" It's, "Should this interaction be trusted?"

Fraud prevention must shift from verifying identity at isolated moments to assessing trust continuously. Organisations need to bring together identity, device, behavioural, communications and network signals to create a more complete view of risk. Connected intelligence helps organisations detect risk earlier, make more precise decisions and reduce unnecessary friction for legitimate customers.

This report is written for fraud, risk, identity, authentication, digital channel and customer experience leaders responsible for protecting growth and customer trust. Drawing on TransUnion's global intelligence, proprietary research and regional market perspectives, it explains where fraud risk is moving, why traditional fraud strategies are losing effectiveness and which capabilities organisations should prioritise to build a more resilient trust strategy across the customer lifecycle.

The next era of digital trust reaches beyond fraud prevention. It will shape how organisations acquire customers, protect relationships, reduce friction and make confident risk decisions. Organisations that succeed in the next decade will not simply detect fraud more effectively — they'll establish trust continuously as a foundation for sustainable growth.

Three themes define the next era of digital trust:

Trust is no longer established once; it's evaluated continuously.

Fraud increasingly emerges after trust has been granted at onboarding, requiring organisations to consistently assess identity, behaviour and intent across the customer lifecycle.

The landscape for fraud prevention expands into communications.

Brand impersonation, spoofed calls and social engineering influence consumer perception and behaviour before traditional fraud controls have an opportunity to intervene.

Fraud operates as a connected, industrialised ecosystem.

AI and automation allow criminal networks to create and refine attacks faster, target them precisely, personalise them convincingly and adapt rapidly to changing conditions.

Authors and Contributors

Authors



Brian Killeen

Vice President:
Product Management,
Fraud & Identity Solutions



Richard Tsai

Sr. Director:
Product Marketing,
Fraud & Identity Solutions

Contributors



Amritha Reddy

Sr. Director:
Africa Fraud & Identity Solutions



Glyn Cowlishaw

Director:
UK Fraud Solutions Specialists



Andrew Sigfrid

Sr. Director:
Canada Fraud & Identity Solutions



Manuel Pineros

Director:
Spain Business Development



Anurag Anand

Director:
India Fraud & Identity Solutions



Miguel Rivera

Sr. Director:
Latin America Fraud & Identity Solutions



Anurag Varma

Director:
Asia Pacific Fraud & Identity Solutions



Wallace Massola

Sr. Advisor:
Brazil Head of Fraud & Identity Solutions

Inside the Global Trust Landscape



As trust becomes easier to exploit, organisations are struggling to keep pace

Fraud has become one of the most significant business risks organisations face. Globally, 61% of business leaders ranked fraud among the risks with the greatest potential business impact, ahead of cybersecurity breaches, compliance, customer churn, operational cost and reputational risk. More concerning, 58% said they're very or extremely concerned fraud is evolving faster than their organisations' abilities to detect and prevent it.

This is being driven by a fundamental shift in how fraud operates. Many of the fastest-growing threats are designed not simply to steal money but to exploit trust. Synthetic identities are built to appear legitimate. Scams manipulate consumers into authorising fraudulent activity. AI enables attacks to become more adaptive, scalable and difficult to detect. Increasingly, fraud succeeds by leveraging trusted identities, communications and relationships.

Fraud is a strategic risk hiding in operational losses

Many organisations still experience fraud primarily as a financial and operational problem. The data suggests something broader. While 47% of business leaders said operational costs and direct financial losses had a significant or severe impact on their business over the past year, 45% pointed to brand reputation and 42% cited the ability to grow or scale. Fraud is increasingly influencing customer acquisition and experience, as well as long-term business performance.

Organisations recognise the risk, yet many remain least prepared for the threats reshaping the fraud landscape. More than half of business leaders (53%) identified synthetic identity fraud as the threat they feel least prepared to manage, making it the largest preparedness gap identified in this research.

Taken together, these findings point to a broader shift. The challenge organisations face is no longer simply detecting fraudulent activity after it occurs. It's understanding how trust is being exploited across identities, communications and customer interactions, then building the capabilities to respond.

The sections that follow examine three forces driving this shift: the rise of synthetic identities, the growing role of communications in fraud attacks and the industrialisation of fraud through AI and automation.

About the data

Unless otherwise noted, data cited throughout this report is drawn from commissioned business and consumer surveys, as well as insights derived from TransUnion's proprietary fraud, identity, credit and communications intelligence. For additional methodology details, see About the Research.

Synthetic identities are redefining trust

In an era of synthetic identities and mass-scale identity theft, identity is no longer a reliable anchor for trust. Across every region, fraudsters appear to be outpacing organisations' abilities to differentiate genuine identities from those manipulated or manufactured.

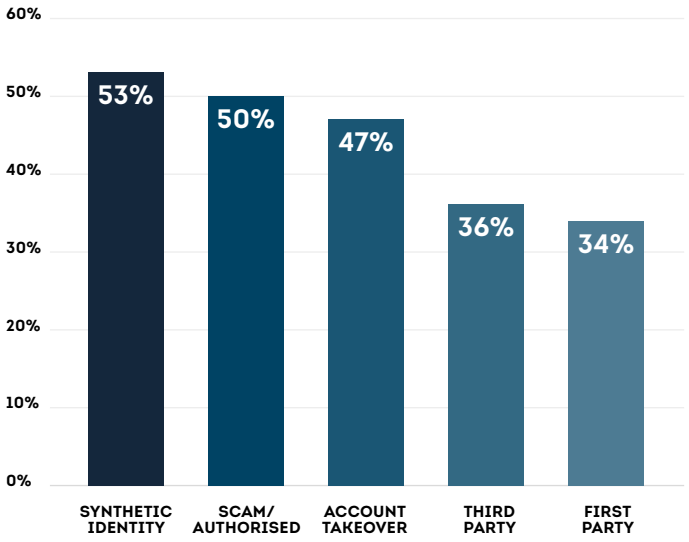
Synthetic identity fraud is outpacing organisations' detection capabilities

Organised fraud rings and bad actors are using exposed consumer information and AI to build credible identities and deepfake documents that can be used to attack businesses across industries and markets. Globally, 18% of business leaders said synthetic identity fraud was the leading cause of fraud losses for their organisations in the past year and 65% said they expect it to increase most for their businesses over the next two years.

Despite its impact, synthetic identity fraud is the top-ranked fraud type leaders believe they're least prepared to manage today (see Figure 1). Once synthetic identities slip past digital onboarding fraud controls, organisations face the challenge of discovering them before incurring fraud losses or facing regulatory compliance penalties, sanctions or legal actions.

Figure 1: Synthetic Identity Fraud Is the Threat Organisations Feel Least Prepared to Stop

Percentage of business leaders who said their organisations are least prepared to manage each fraud type



Source: TransUnion business fraud survey, June 2026

65%

of business leaders expect synthetic identity fraud to increase over the next two years

Source: TransUnion business fraud survey, June 2026

Synthetic identity exposure appears broader than many organisations realise

Synthetic identity fraud is a global, cross-sector problem. It's present in both mature credit economies and emerging digital markets. While there's little reporting of exposure and loss globally, awareness of the risk is growing as many organisations mistake synthetic identity fraud losses as first- or third-party fraud.

Regional observations reinforce the business impact leaders reported. For instance, business leaders in Hong Kong, India, Spain and the US were more likely than average to say synthetic identity fraud would increase the most of all fraud types for their organisations in the next two years. Data from the US and Canada, combined with observations from the UK and Latin America, suggest synthetic identity fraud may be more widespread than current reporting indicates. As organisations improve their visibility into synthetic identity activity, many may discover exposure has been underestimated, reinforcing the need to continuously evaluate trust beyond onboarding.

Synthetic Identity Fraud Risk Awareness Rising

US

Estimated US total lender exposure to synthetic identity fraud risk reached USD 2.4 billion at end of June 2026. Auto lending was hit hardest, with USD 1.5 billion in synthetic risk exposure, while other tradelines, including bank cards and personal lines of credit, showed lower levels of exposure. In the US, average synthetic fraud charge-off losses more than doubled from H1 2009 to H1 2026. Proprietary TransUnion research indicates non-financial services organisations like telecommunications also face risk from synthetic identities.

CANADA

In proprietary TransUnion research, synthetic fraud steadily increased in Canada between Q3 2021 and Q4 2023, accounting for more than 14% of onboarding credit losses, underscoring the growing challenge of identifying fabricated identities before they become established within the financial ecosystem.

UK

TransUnion found UK institutions are actively identifying large populations of suspected synthetic identities in proof-of-concept reviews. Many are finding synthetic identity fraud losses were originally written off as third-person impersonation or first-party default.

LATIN AMERICA

Synthetic identity concerns are increasingly associated with digital onboarding and credit acquisition. While many Latin American countries have national civilian registries, TransUnion found these measures are not preventing identity manipulation, document forgery and the use of AI to replicate identity documents like driver's licenses and passports.

Data breaches provide source material for more sophisticated synthetic identity fraud

Data breaches continuously feed the identity-based fraud supply chain. Cyber attacks aimed at organisations to obtain authentic identity information and credentials are exposing millions, if not billions, of individuals worldwide to potential fraud (see Figure 2). As AI enables faster, more targeted attacks, the threat synthetic identities pose to trust will only accelerate.

Data breach reporting in the US highlights the scale of the identity data available to fraudsters for synthetic identity creation. Social Security numbers were exposed in 73% of US data breaches in H1 2026, while driver's licenses and state IDs were exposed in 34%. Cybercriminals also targeted information like medical histories (37% of US breaches) and checking or savings account numbers (34%). As more authentic identity data becomes available through breaches, fraudsters have greater ability to construct convincing synthetic identities, increasing the challenge of distinguishing legitimate consumers from fabricated ones and reinforcing the need for continuous trust at onboarding and beyond.

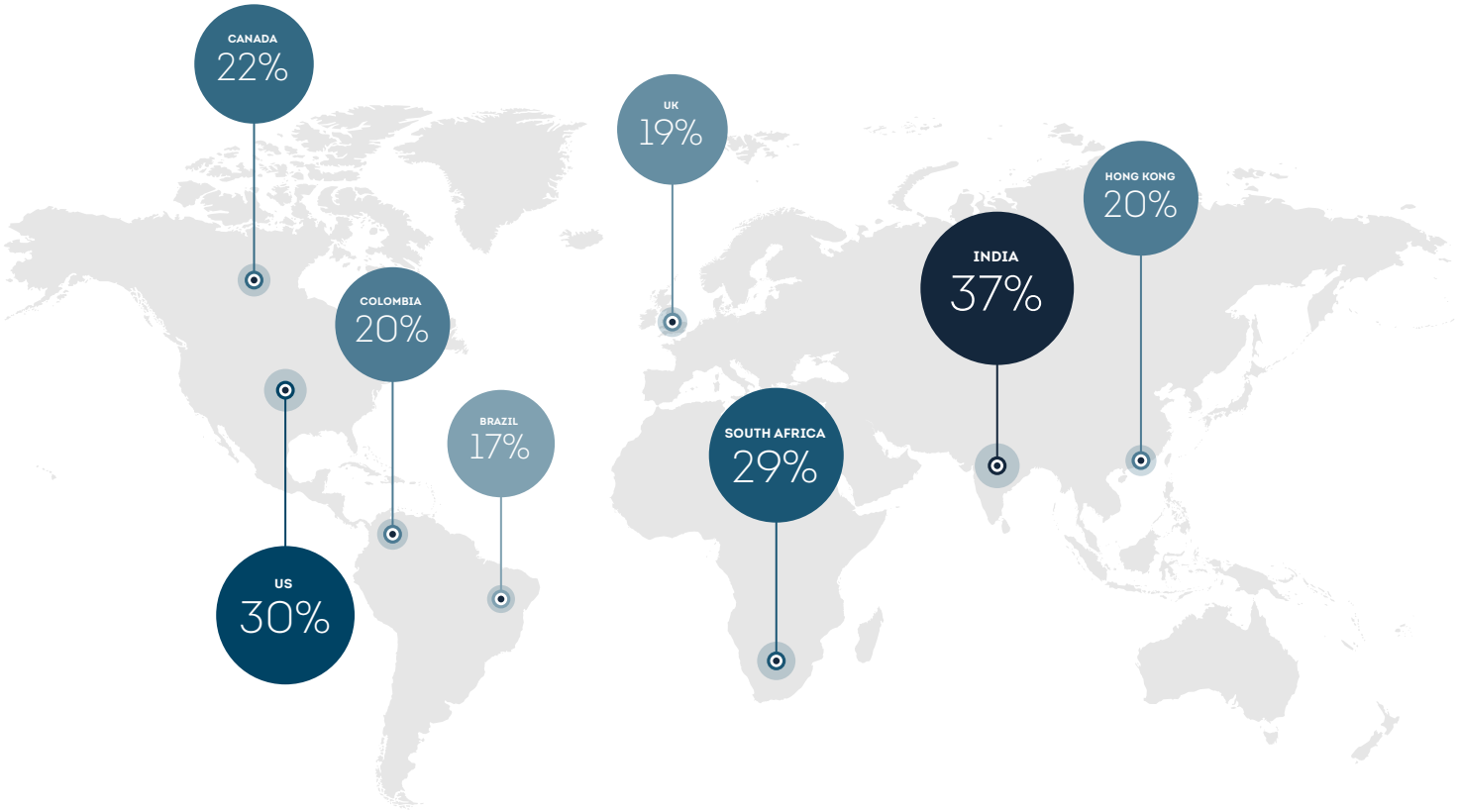
73%

of US data breaches exposed full Social Security numbers in H1 2026

Source: TransUnion global intelligence network

Figure 2: Consumers Worldwide Continue to Report Identity Exposure From Data Breaches

Percentage of consumers who said personal information or online account details were exposed in a data breach during a recent three-month period



Source: TransUnion consumer pulse survey, May and July 2026

Credit washing in the US extends identity risk of synthetics after they bust out

Criminals attack trusted processes to facilitate synthetic fraud. One strategy fraudsters employ to maintain synthetic identities over time is credit washing, a scheme that exploits the credit dispute process to remove legitimate negative information from a credit history by making false claims of identity theft.

Credit washing undermines credit risk scoring by suppressing derogatory information from credit score models. Consumer-initiated charge-off suppressions, have been shown to be closely correlated to credit washing. In the US, consumer-initiated charge-off suppressions grew at a compound annual growth rate of 29.2% from 2017 to 2026 (see Figure 3).

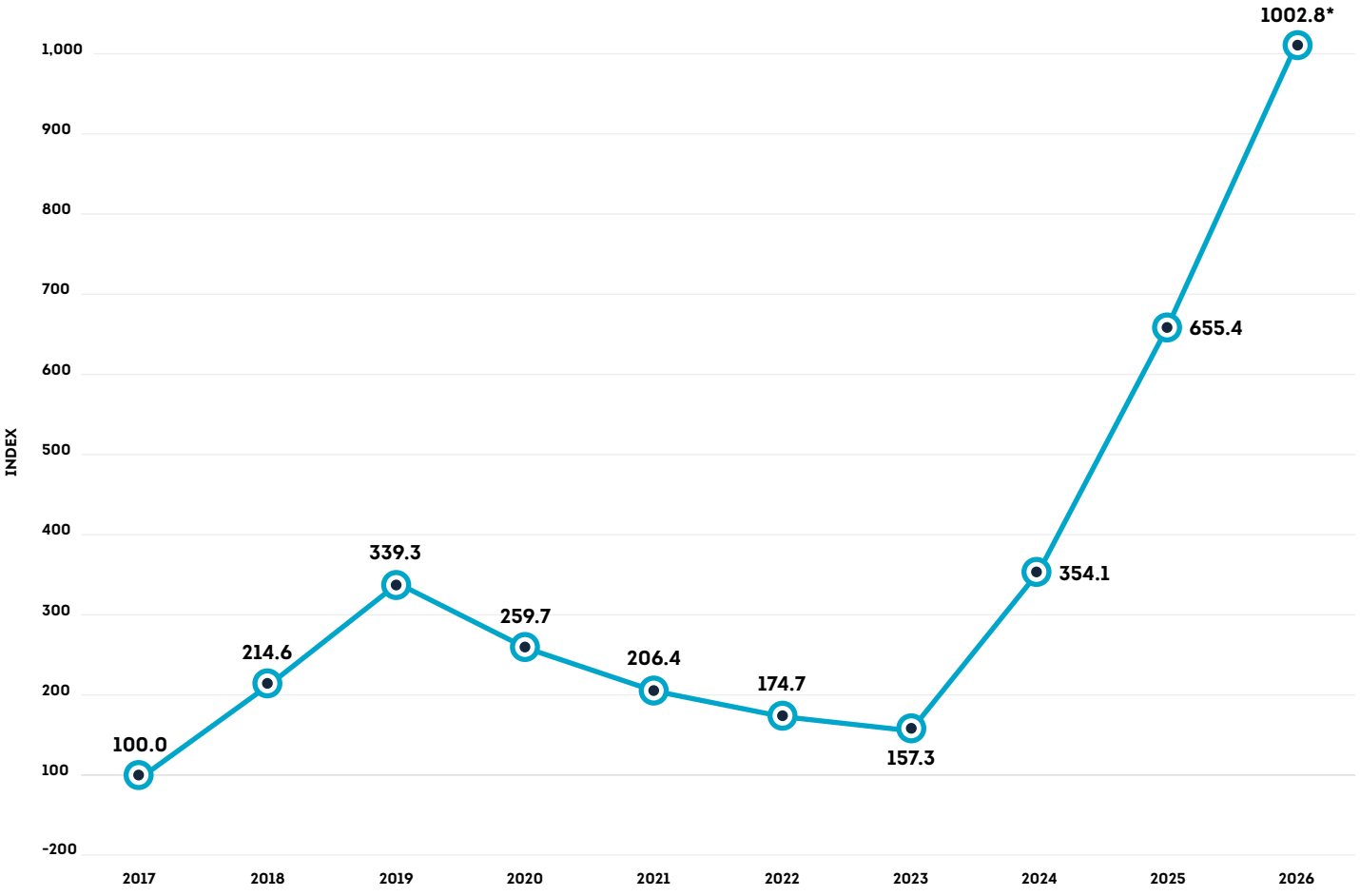
29.2%

compound annual growth rate of US consumer initiated charge-off suppressions from 2017 to 2026

Source: TransUnion global intelligence network

Figure 3: Rapid Growth in Charge-Off Suppressions May Extend the Lifespan of Synthetic Identities

Consumer-initiated charge-off suppressions annual growth indexed to 2017



2026 projected from H1 2026 actuals

Source: TransUnion global intelligence network

Identity risk extends far beyond account creation, becoming a lifecycle problem

Identity-based fraud attacks often arise before organisations have sufficient information to establish trust in new customers. While account creation is a critical trust-establishing event, most fraud exposure occurs after the customer relationship has already been established.

Different risk patterns appear across account creation, login and financial transaction activities, especially for AI-enabled fraud. For instance, AI can help fraudsters rapidly generate or modify identities, credentials and interactions to target the weakest controls across the customer lifecycle. While account creation often carries the highest percentage of suspected digital fraud of any lifecycle stage (see Figure 4), 81% of all suspected digital fraud in H1 2026 occurred during ongoing customer interactions (account login and financial transactions).

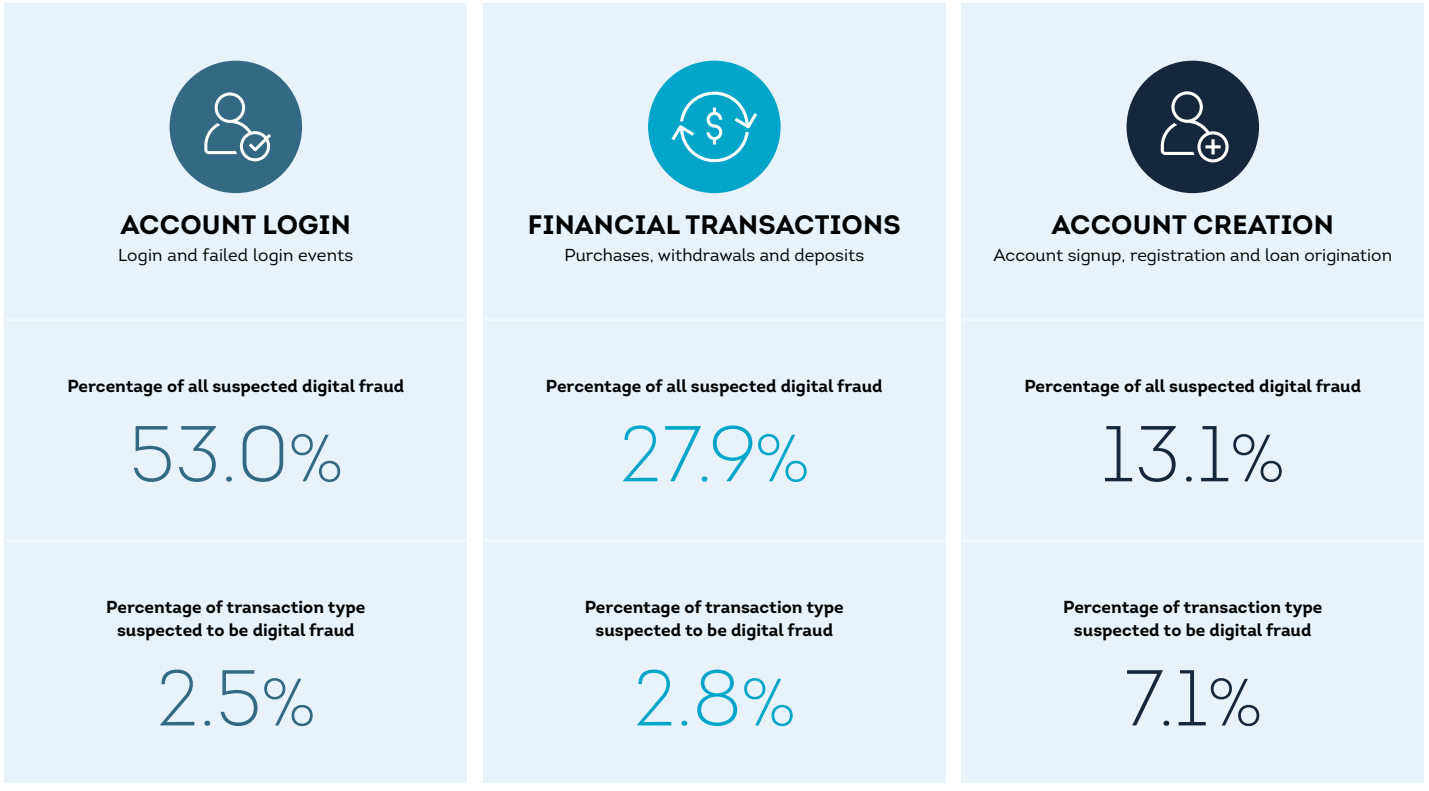
81%

of all suspected digital fraud occurred during ongoing customer interactions in H1 2026

Source: TransUnion global intelligence network

Figure 4: Most Suspected Digital Fraud Occurs After Account Creation

Digital fraud in the customer lifecycle in H1 2026



Source: TransUnion global intelligence network

Identity risk across the customer lifecycle poses a persistent threat across industries

As AI-driven digital fraud attacks expand, criminals increasingly look to exploit the weakest defences, moving across industries and organisations in search of the easiest targets. For example, a single synthetic identity may be used to obtain a buy now, pay later loan (BNPL) at a retailer, open a mobile phone account that includes a handset lease, secure a higher limit credit card at a bank and create an online betting account.

While the lifecycle stage where risk is concentrated varies by industry and business model (see Figure 5), organisations need to recognise closing gaps in identity assurance across the customer lifecycle is critical to reducing fraud losses.

For example:

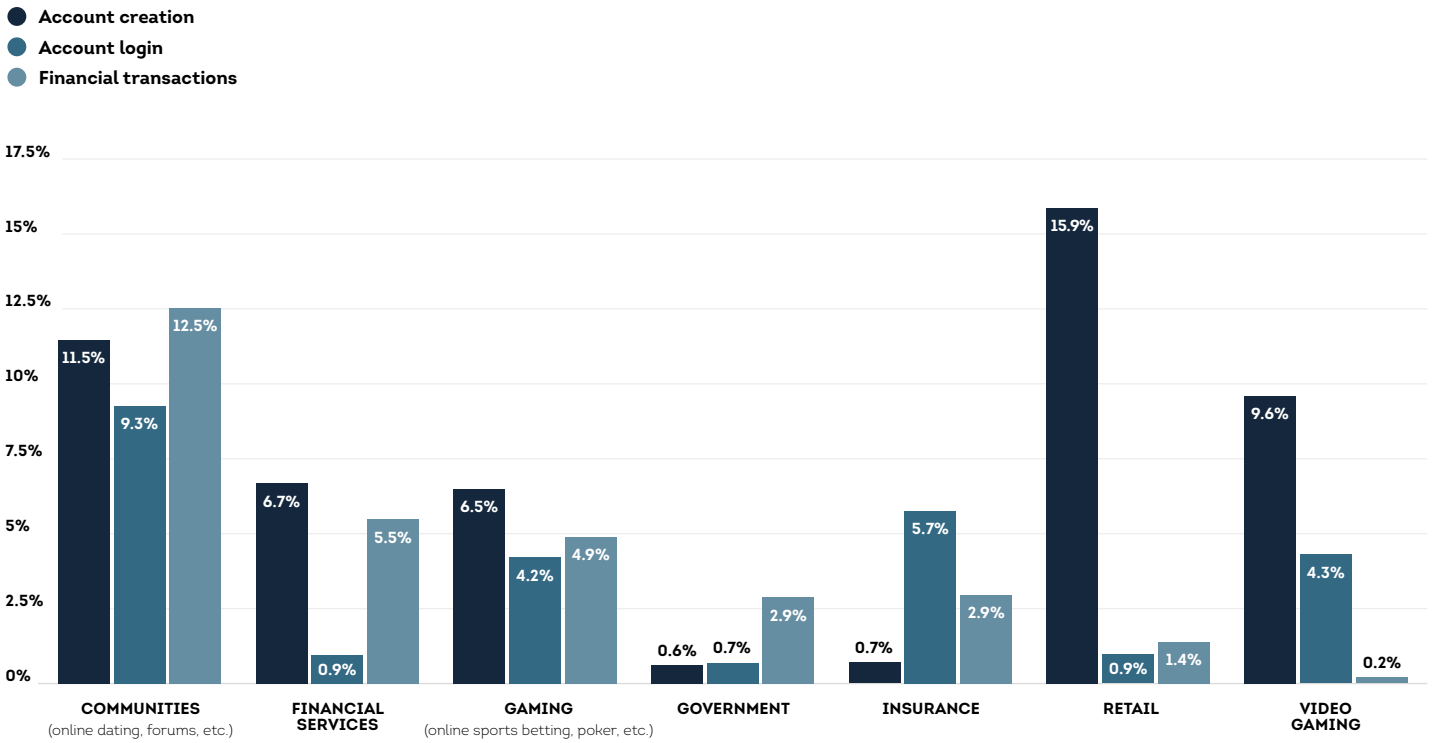
Retail shows extremely high account creation risk due to promotion abuse because accounts are often required to secure advertised discounts. Yet low-assurance identity verification is utilised to keep customer friction to a minimum in this extremely competitive industry.

Financial services experiences elevated account creation risk due to the immediate financial gain fraudsters seek. However, fraud risk associated with financial transactions (including deposits, withdrawals and payments) is higher than most industries, indicating identity assurance challenges persist well after a customer relationship has been established.

Gaming demonstrates elevated risk across multiple interaction points. Despite high-assurance identity verification, fraudsters target new accounts to commit bonus abuse. But risk persists throughout the customer lifecycle. For example, account login risk may arise when multiple individuals use the same account, while transaction risk may occur when a fraudster uses a stolen credit card to fund an account.

Figure 5: Fraud Risk Concentrates at Different Stages of the Customer Journey by Industry

Percentage of attempted transactions suspected to be digital fraud by customer journey stage in select industries in H1 2026



Source: TransUnion global intelligence network

RECOMMENDED ACTIONS

What this means for organisations

Identity assurance can no longer focus solely on onboarding. As synthetic identity fraud becomes more sophisticated and fraudsters exploit trusted accounts throughout the customer lifecycle, organisations need a broader approach to evaluating trust. The following actions can help reduce exposure while maintaining friction-right customer experiences.

1

Implement continuous trust, not one-time verification

Identity trust should be treated as an ongoing business process rather than a one-time onboarding decision. Organisations should continuously reassess trust as customer behaviours, credentials and risk signals evolve throughout the relationship.

2

Shift identity assurance to evolving risks

Prioritise identity intelligence where trust is most likely to change, not just where trust is initially established. While onboarding remains critical, organisations should strengthen identity assurance across login, account maintenance, payments and recovery journeys.

3

Connect identity intelligence across service channels

Shift investment from isolated verification tools toward connected identity intelligence that unifies identity signals across customer interactions to detect evolving fraud while reducing unnecessary friction for legitimate customers in every channel used to serve them.



Communications have become the new fraud battleground

Fraud increasingly begins before the traditional fraud event through brand impersonation, social engineering and trust manipulation. Communication channels have become an upstream fraud signal, often shaping consumer behaviour before traditional fraud controls can intervene.

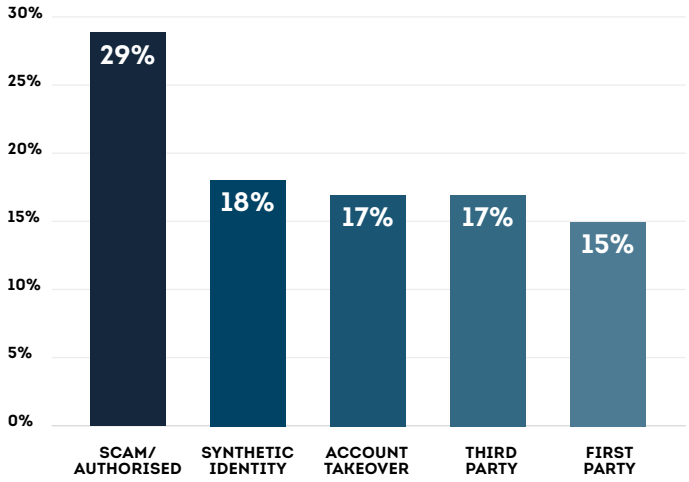
Scams emerge as the leading and fastest-growing source of fraud loss

Most consumers targeted by digital fraud have experienced scam emails, texts and phone calls. But awareness doesn't make these attacks any less effective. Business leaders reported scam/authorised fraud as the dominant cause of fraud loss for their organisations in the last year (see Figure 6).

With sophisticated, AI-enabled impersonation scams, risk is only growing. Nearly half (48%) of business leaders reported scam/authorised fraud increased in the last year (see Figure 7), the highest by far compared to other fraud types.

Figure 6: Scam and Authorised Fraud Generate the Greatest Business Losses

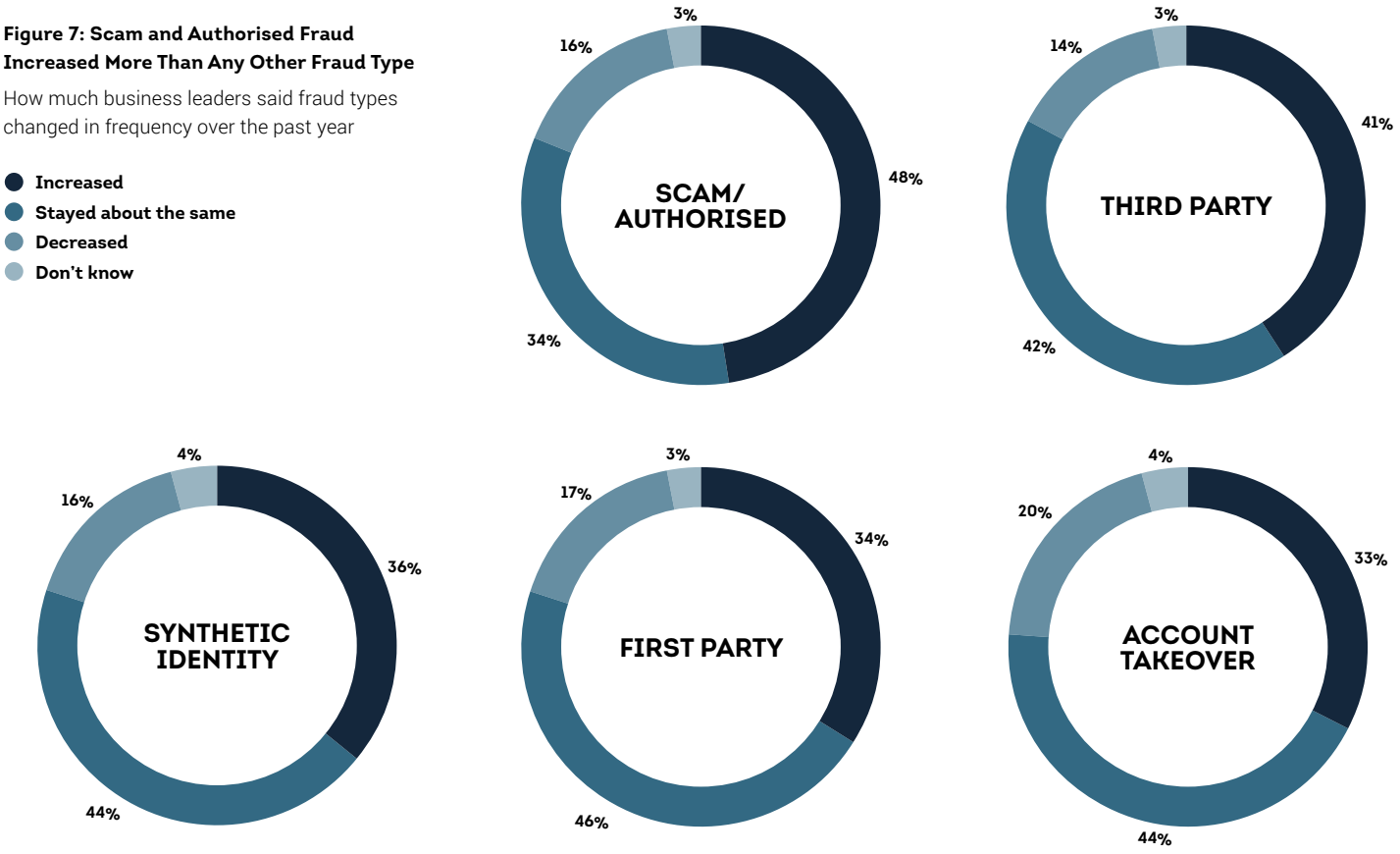
Percentage of business leaders who claimed these fraud types caused the most losses for their organisations in the past year



Source: TransUnion business fraud survey, June 2026

Figure 7: Scam and Authorised Fraud Increased More Than Any Other Fraud Type

How much business leaders said fraud types changed in frequency over the past year



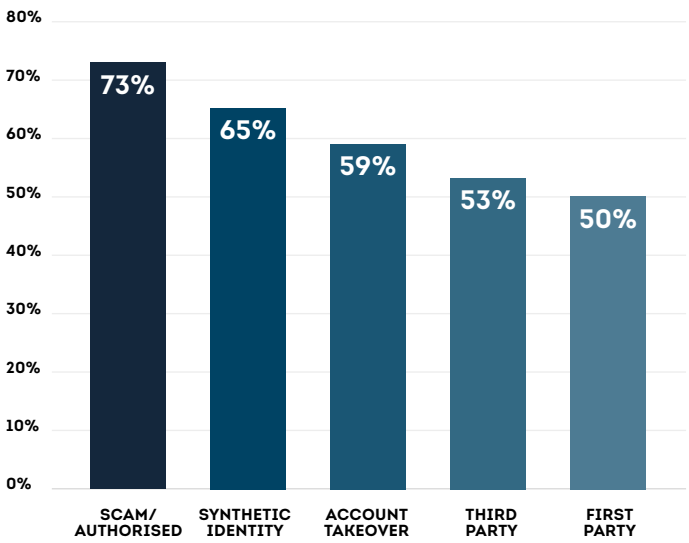
Source: TransUnion business fraud survey, June 2026

Enterprise impersonation is a leading indicator of future fraud attacks

Organisations should view communications risk as a fraud early warning signal, preceding identity-based attacks like account takeover (ATO), scam/authorised fraud and new account fraud. While many attacks end in immediate financial loss for consumers, more result in criminals successfully collecting data to be used later. More than half (56%) of scam victims who gave up personal or financial information said they didn't experience a financial loss.[1] At the same time, consumer scam losses declined dramatically year over year, a clear indication scammers are focused on stealing personal information rather than seeking immediate monetary theft.[2] Despite the drop in consumer fraud losses last year, scam/authorised fraud was the fraud type most business leaders expected to grow over the next two years (see Figure 8).

Figure 8: Organisations Expect Scam and Authorised Fraud to Grow Faster Than Any Other Fraud Type

Percentage of business leaders' top three fraud types they expect to grow the most in the next 24 months



Source: TransUnion business fraud survey, June 2026

34%

of consumers who reported being targeted by digital fraud said they experienced a smishing attack, more than any other scheme

Source: TransUnion consumer pulse survey; February, March, May, July and August 2026

Trusted communications are a common attack surface for impersonation scams

Consumers expect organisations to make legitimate communications easy to verify and fraudulent communications easy to identify. Criminals work to undermine that trust, and business impersonation has become a widespread tactic (see Figure 9). While many households have multiple digital devices, for most organisations globally, especially those in developing economies, trusted outbound digital communications are centred on a consumer's mobile phone. Yet brands don't control the path to the customer's device. Vulnerabilities in telecommunications network interoperability make mobile phones prime targets for impersonation scams involving spoofed calls and texts.

Fraudsters exploit vulnerabilities in phone networks to conceal their identities and spoof the phone numbers of trusted enterprises, including banks, healthcare providers and insurers. By posing as legitimate representatives, they can trick consumers into sharing one-time passcodes (OTPs), "verifying" personal information, resetting account credentials or redirecting payments as part of account takeover schemes.

Trusted outbound customer engagement is critical for servicing and growing relationships. Organisations typically rely on education to help protect customers from fraud — establishing clear policies and channels for when and why they'll contact customers, such as fraud alerts. However, given the scale and expected growth of losses from scam/authorised fraud, organisations need stronger ways to protect outbound customer engagement.

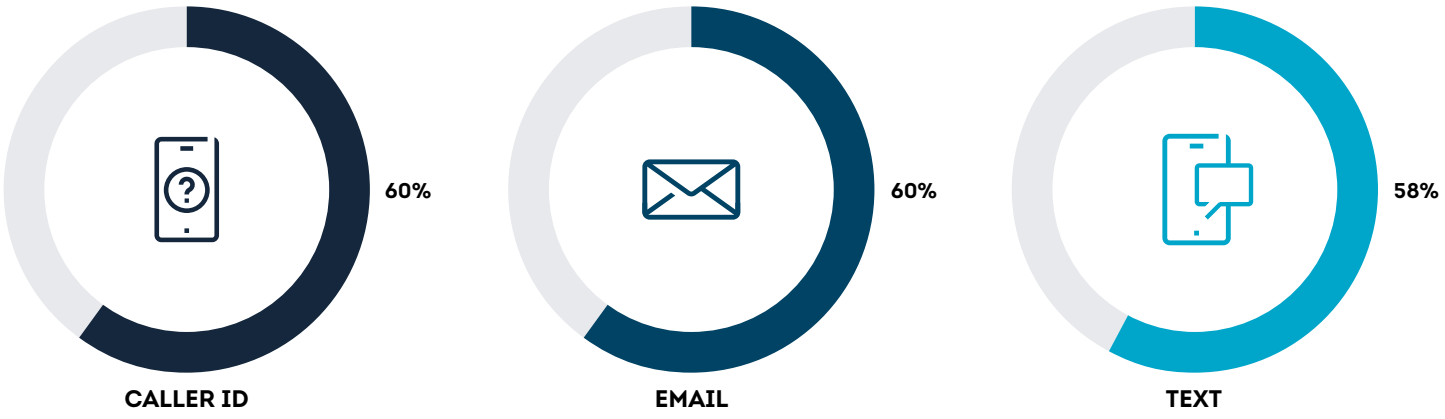
19.4%

of outbound business-to-consumer calls with US mobile carriers were spoofed in H1 2026

Source: TransUnion global intelligence network

Figure 9: Brand Impersonation Is Affecting Customers Across Every Major Communication Channel

Percentage of business leaders who said fraudsters spoofed their organisations on these channels in the last year



Source: TransUnion business fraud survey, June 2026

RECOMMENDED ACTION

What this means for organisations

As fraud increasingly originates through trusted communications channels, organisations must expand how they think about fraud prevention. The objective goes beyond simply authenticating users or approving transactions. It's about identifying manipulation before trust is compromised. This requires detecting fraud earlier using communications signals connected with identity, device and behavioural intelligence, and using that intelligence to protect and restore trusted customer engagement.

1

Detect fraud earlier using communication risk signals

Use impersonation or spoofing signals earlier, creating opportunities to disrupt fraud before downstream controls are tested.

2

Connect communication risk signals with identity intelligence

Incorporate communications-based risk signals alongside identity, device and behavioural intelligence to create a more dynamic and predictive view of customer trust.

3

Combat scams to restore trust and improve customer engagement

Invest in capabilities that restore trusted engagement outside organisational boundaries, block bad actor attempts to compromise credentials and enable coordinated responses across the broader fraud ecosystem.



AI is enabling criminal networks to operate on an industrialised scale

Traditional measures of digital fraud no longer capture the full scope of the threat as criminal networks effectively exploit trust to avoid or pass traditional controls. AI has changed the fundamental economics of fraud. It allows fraudsters to automate activities that historically required significant human effort (e.g., creating identities and content, targeting attacks and interacting with victims), improving the precision, scale and adaptiveness of attacks. It has enabled criminals to raise their attack success rates with unprecedented speed and scale to the point of industrialising the full fraud value chain. In fact, 42% of the business leaders said the increasing scale and/or sophistication of fraud is putting significant to severe pressure on their organisations.

The fraud value chain is built on trust organisations grant digital identities and consumers give to brands (see Figure 10). From identity production pipelines to long-term investments in synthetic identities as infrastructure assets, AI is reshaping the fraud value chain. It lowers the cost of executing sophisticated schemes and enables criminals to exploit legitimate business processes across industries, steal assets and launder proceeds into hard-to-trace assets.

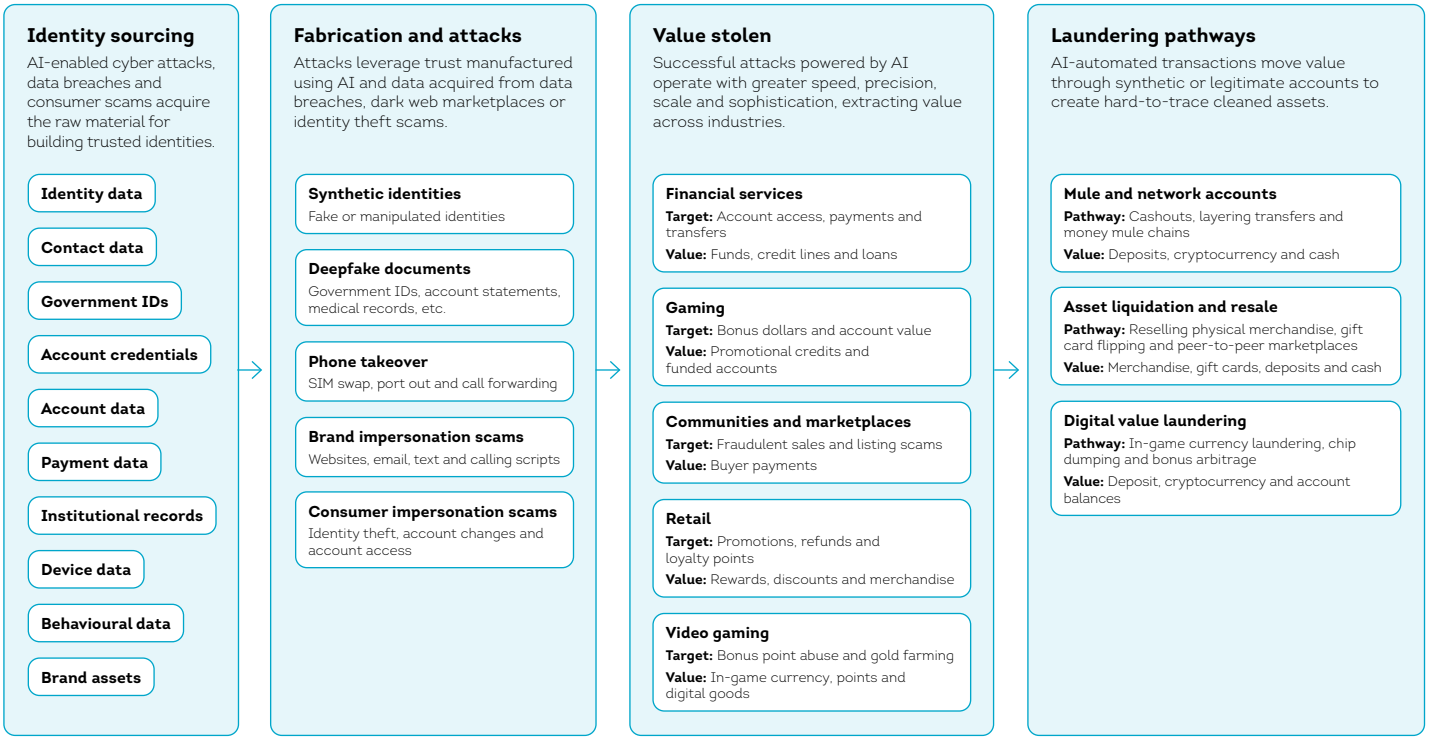
42%

of business leaders said increasing scale and/or sophistication of fraud is putting significant to severe pressure on their organisations

Source: TransUnion business fraud survey, June 2026

Figure 10: How Industrialised Fraud Converts Identity Data Into Financial Value

Illustration of how AI supports every stage of the industrialised fraud value chain



Fraudsters exploit digital trust by adapting to fraud prevention environments

Industrialised fraud operations increasingly target digital interactions where trust is established and value can ultimately be extracted. However, fraudsters do not attack every step of the customer lifecycle equally (see Figure 11).

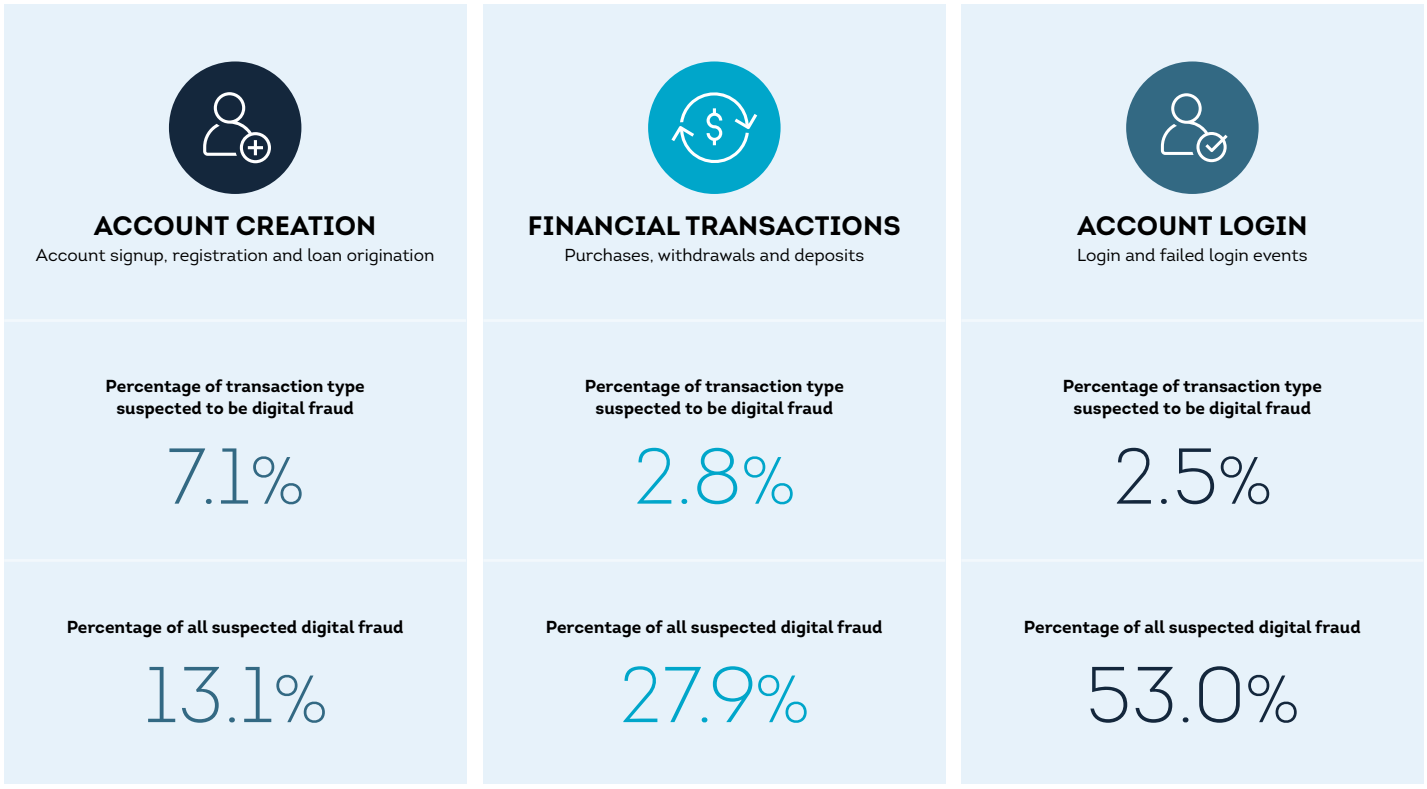
Organisations have invested heavily in strong customer authentication controls over the past decade, making simple credential-based attacks less accessible to fraudsters. Yet as login controls have improved, fraudsters have adapted. They increasingly target secondary authentication workflows like account recovery and service requests with adversary-in-the-middle attacks. The industrialisation of AI has made these attacks more efficient and scalable, reducing the need for the high-volume attack campaigns traditionally associated with primary authentication workflows.

Examining three specific digital trust points highlights the risks organisations face:

- **Account creation** carries the highest risk despite lower relative volume
- **Financial transaction** activity carries the second-highest overall risk because it represents the point where attacks are monetised
- **Account login** represents most of the activity but comparatively lower risk

Figure 11: Account Creation Carries the Highest Fraud Risk, While Logins Drive Most Fraud Activity

Digital fraud in the customer lifecycle in H1 2026



Source: TransUnion global intelligence network

Why digital account creation remains a high-risk touchpoint

Account creation represents only 4.9% of transaction volume but has the highest suspected fraud rate at 7.1% (see Figure 12). AI reduces the effort required to create synthetic identities, complete application forms, generate deepfake documents and automate the entire onboarding process.

While fraudsters primarily open accounts to monetise stolen or synthetic identities, they also do so to support laundering pathways — cleaning illicit money and shielding their identities while conducting illegal activities. Some industries don't emphasise rigorous identity verification at account creation because it impedes conversions. Organisations often set controls at account creation relative to the value being offered to the consumer. A retailer probably won't ask a shopper to create an account to receive a 10% discount code in exchange for their email address, for example. While aligning value exchange to customer friction is a reasonable business decision, it may extend trust to a risky identity intended for fraudulent activity in the future.

Reducing this risk may require organisations to adopt identity assurance controls similar to regulated industries, including banks, lenders and gaming. These organisations must apply know your customer (KYC) and anti-money laundering (AML) regulatory compliance measures to account creation workflows to help stop money laundering activities and reduce pathways for late-stage fraud value chain activity.

Industrialised fraud can create thousands of new accounts using synthetic or stolen identities that appear legitimate. While traditional processes validate individual identity attributes, they're often evaluated in isolation, missing the trust signals that can uncover criminal networks and fraud rings.

Figure 12: Industries With Lower Identity Assurance Face Higher Account Creation Fraud Risk

Top five industries with the highest rate of suspected digital fraud at account creation in H1 2026

Industry	Account creation attempts suspected to be digital fraud	Identity verification approach
ALL INDUSTRIES	7.1%	
RETAIL	15.9%	Light identity verification to keep account creation as friction-free as possible
COMMUNITIES	11.5%	Light to strong identity verification to help protect community members depending on the perceived value of service
VIDEO GAMING	9.6%	Light identity verification to keep account creation as friction-free as possible
FINANCIAL SERVICES	6.7%	Strong identity verification to meet regulatory requirements and reduce credit risk
GAMING	6.5%	Strong identity verification to meet regulatory and geographic requirements

Source: TransUnion global intelligence network

Fraud attacks optimised for monetisation highlight late-stage lifecycle risk

While financial transactions and account login represent similar risk overall, with the exception of insurance and video gaming, financial transactions carry the highest observed fraud risk (see Figure 13). Industrialised fraud optimises for monetisation.

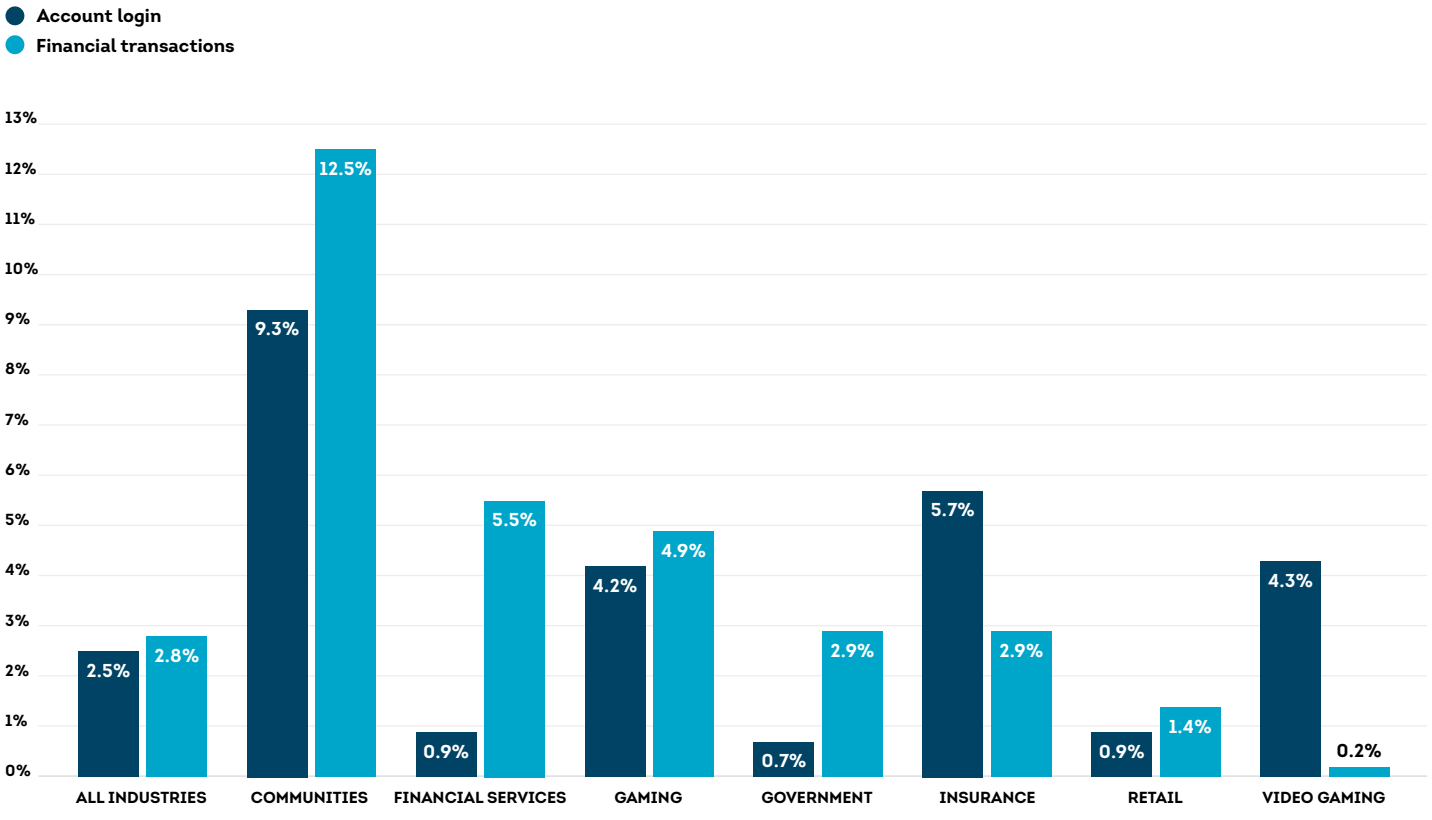
Risk in financial transactions supports this reality. AI can further enable monetisation by identifying targets, prioritising opportunities and automating activity designed to extract value from established accounts and industries where continuous authentication assessments are lighter.

While the financial services industry has made significant investments in account authentication and transaction monitoring, over-optimising the customer experience may leave financial transactions vulnerable. At the same time, communities and gaming both face elevated risk in financial transactions and account login.

For gaming, fraud risk is similar in both login and financial transactions. While most platforms have geo-fencing rules that don't allow users to access accounts in jurisdictions where gaming is illegal, ATO remains an issue because players maintain cash and bonus balances. While gaming follows AML regulations similar to financial services, an industry built on high-volume financial transactions will be a target. Communities operate on member trust, often with lower-friction account creation processes, which results in higher-than-average risk for account login and transactions. These platforms give criminals opportunities to execute at every stage of the fraud value chain depending on the community's business model. Supercharged with AI, communities are particularly vulnerable to synthetics, impersonation, purchase scams and asset liquidation.

Figure 13: Financial Transaction Fraud Often Rivals or Exceeds Login Fraud Risk

Percentage of transaction type suspected of digital fraud in select industries in H1 2026



Source: TransUnion global intelligence network

RECOMMENDED ACTIONS

What this means for organisations

Industrialised fraud is changing the economics of attack and defence. AI allows fraudsters to test, refine and scale attacks faster than many organisations can adapt their controls. As a result, risk increasingly shifts to the weakest point in the customer lifecycle rather than remaining concentrated at a single stage.

Fraud has become adaptive and industrialised. Therefore, fraud prevention must become adaptive and connected. Organisations that rely on static controls, disconnected signals and periodic updates may struggle to keep pace with rapidly evolving threats. Instead, they should continuously learn from emerging fraud patterns, connect intelligence across the customer lifecycle and automate decisions wherever possible.

1

Match the speed and scale of AI-enabled attacks

Assume fraud attacks will continue to become more efficient and build defences that can adapt at a similar pace.

2

Modernise decisioning with adaptive intelligence

Complement traditional controls with adaptive intelligence that continuously learns from emerging fraud signals and evolving attack techniques.

3

Build versatile and nimble fraud operations

Modernise fraud detection but also investigation, decisioning and response. Success will increasingly depend on combining trusted data, advanced analytics and automation to protect customers while maintaining friction-right experiences.



Regional Perspectives



Africa Overview



Africa's expanding digital economy gives more consumers access to mobile, financial and online services, yet increases their exposure to fraud. Across Africa, fraud risk now extends throughout the customer lifecycle, with account login emerging as the primary point of exposure. Fraudsters increasingly seek to take over legitimate accounts – where an established identity and trusted relationship can help them move with less scrutiny.

KEY TAKEAWAYS

Account login has become Africa's primary fraud battleground

94.3%

of suspected digital fraud volume for African clients in H1 2026 occurred during account login, highlighting the growing importance of protecting existing customer relationships

Financial services is Africa's highest risk sector

3.0%

of transactions with African financial services clients in H1 2026 were suspected of digital fraud (the highest rate among industries analysed in the region), reinforcing the need for layered identity, device and behavioural defences

Fraud attempts are driven through trusted communications

60%

of surveyed South African consumers said they were targeted by digital fraud in a recent three-month period, with many reporting being targeted through communication channels

Fraud expands beyond onboarding as communications and account access become key attack vectors across Africa

Digital trust in Africa is increasingly being challenged long after the onboarding process is complete. While organisations have traditionally focused on establishing trust once, by verifying identities at account opening, fraudsters are now shifting their attention to existing customer accounts. This changes the role of fraud prevention. Onboarding remains a critical control, but it cannot carry the full burden of protecting a relationship that exists across devices and channels.

Underscoring this shift, 2.7% of all account login transactions attempted among African clients in H1 2026 were suspected of digital fraud (see Figure 14). This is in line with 2.6% of all digital transactions in Africa being suspected digital fraud. Yet, the concentration of fraud activity was more revealing than the rate; nearly all of Africa's suspected digital fraud volume occurred at account login. Fraudsters are focusing on legitimate accounts that already carry trusted histories. Organisations should bolster account login authentication with device-based risk signals that pair account and device identity to better differentiate trusted customers from potential fraud attacks.

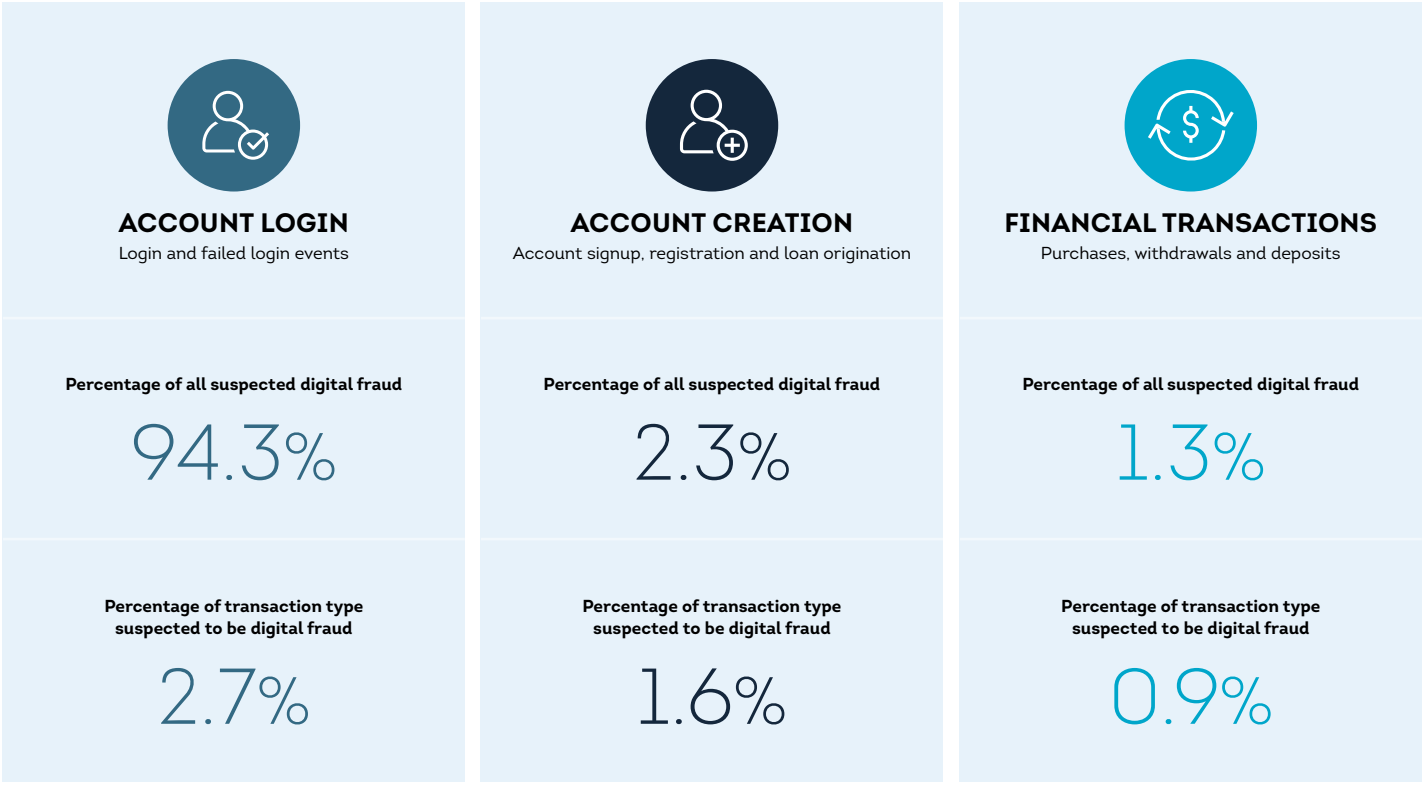
2.6%

of all digital transactions in Africa were suspected digital fraud in H1 2026

Source: TransUnion global intelligence network

Figure 14: Nearly All Suspected Digital Fraud in Africa Occurs During Account Access

Digital fraud in the customer lifecycle in H1 2026



Source: TransUnion global intelligence network

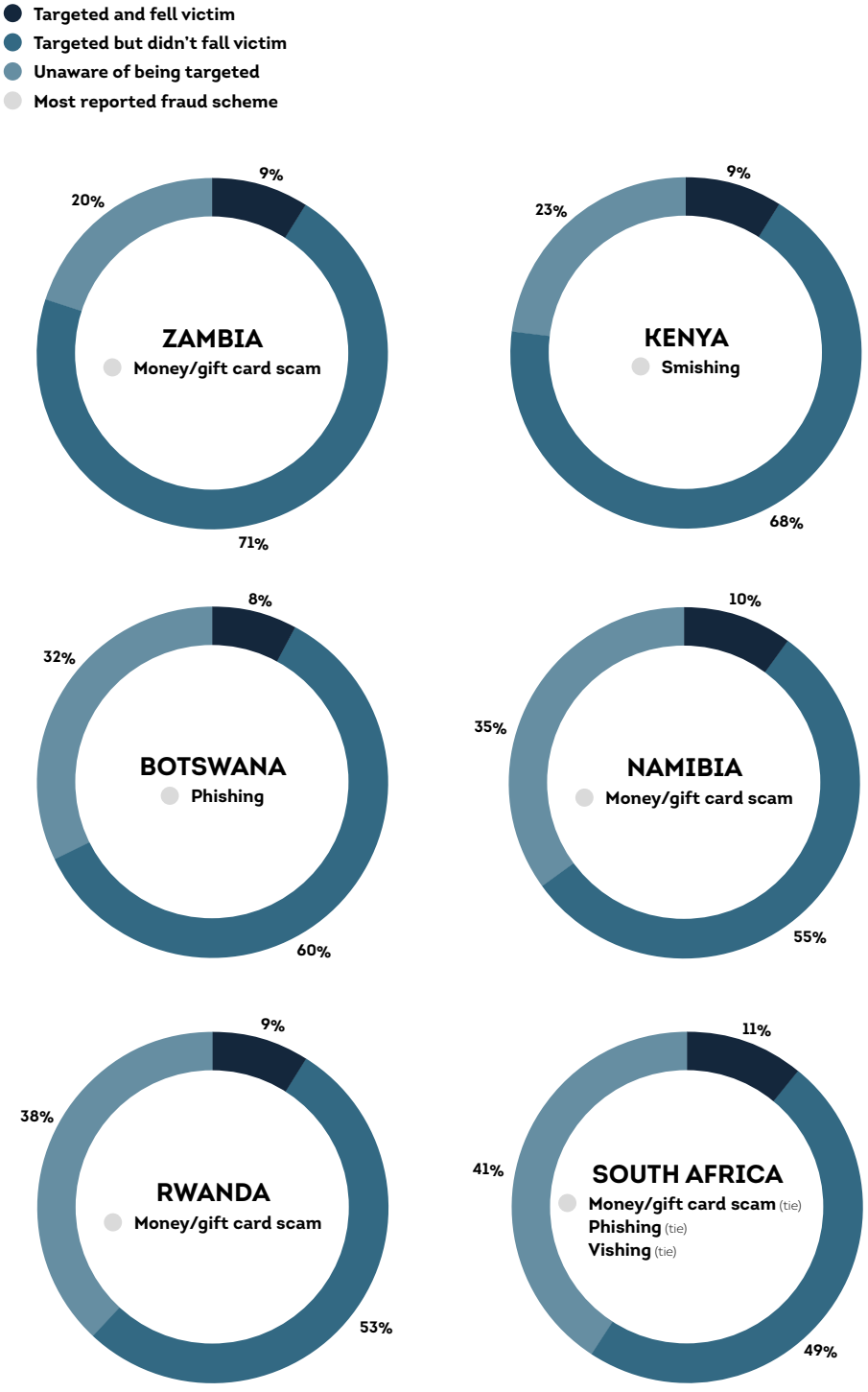
Fraud has shifted, putting customer trust at risk

Fraud often starts long before a financial transaction occurs. Across multiple African countries, significant proportions of consumers reported being targeted by fraudulent communications through email, online, phone call or text messaging fraud attempts in a recent three-month period (see Figure 15). Targeting was highest in Zambia and lowest in South Africa. The leading reported schemes varied by market, including smishing in Kenya, phishing in Botswana and money or gift card scams in several other countries. The variation matters because it shows a common business challenge expressed through different local tactics.

Trusted communications are often the first stage of account fraud. Criminals use familiar channels and convincing messages to create urgency, earn confidence or persuade a person to share information, approve an action or send funds. Businesses should therefore treat communications as part of the trust journey — not simply as marketing or service channels. Improve defences by connecting communication events with identity, device and account behaviour so elevated risk can be recognised before access becomes loss.

Figure 15: Consumer Digital Fraud Attempts Are Common Across African Markets

Percentage of consumers who said fraudsters targeted them with online, email, phone or text messaging fraud schemes in a recent three-month period — and the fraud scheme most reported



Source: TransUnion consumer pulse survey; March, May, July and August 2026

Financial services sit at the centre of African fraud risk

Financial institutions must protect high-value moments without creating unnecessary barriers for legitimate customers. Yet, financial services recorded the highest suspected digital fraud rate among industries analysed within Africa in H1 2026 at 3.0%. This reflects more than the value held by financial institutions. Digital banking, mobile money, lending and real-time payments — bringing together rapid movement of funds, remote customer interactions and digital onboarding — continue to expand across the continent.

That requires fraud controls proportionate to the interaction. Identity checks remain essential when an account is opened, but login, device change, account recovery and payment activity may require additional context. Linking identity to known devices, monitoring behavioural changes and applying real-time risk assessments in a layered strategy can help organisations distinguish a returning customer from a criminal using valid credentials. The objective isn't more friction everywhere. It's stronger verification where signals show risk is rising.

AI increasingly enabling sophisticated fraud across the continent

Fraud is no longer the work of isolated opportunists. Increasingly, TransUnion's African clients are observing fraudsters leveraging automation, AI-powered tools and organised criminal networks to scale attacks across multiple channels and markets simultaneously. Cybercrime has become an industrialised, borderless ecosystem, and a recent survey indicated AI enabled 55% of reported cybercrimes across Africa.[3] The combination of automated phishing campaigns, stolen credentials and sophisticated account takeover tactics allows fraudsters to operate with greater speed and efficiency than ever before.



Shaping the Next Era of Digital Trust

Across every region in this report, the same pattern emerges: Fraud is becoming more interconnected, increasingly adaptive and harder to contain within traditional organisational boundaries. AI, industrialised fraud networks, expanding digital ecosystems and evolving regulatory expectations are changing not only how fraud is perpetrated but how trust itself must be established and maintained. As fraud moves across identities, devices, communications, organisations and channels, no single signal or control will be sufficient on its own. The next phase of fraud prevention will be defined by how organisations establish trust across entire customer ecosystems rather than within isolated transactions. Exploring where the shift to establishing continuous trust across entire consumer ecosystems could take the market next.



1 Consumers protect themselves from digital risk with dedicated security apps

The next generation of identity protection will rely on AI-powered digital shields that will help consumers determine if interactions can be trusted before they act.

Market signals

Consumer mobile applications already evaluate caller identity, business reputation, scam labels and verified messaging.

How to prepare

Think beyond identity monitoring and post-event remediation, toward proactive consumer protection that detects manipulation early and helps them avoid irreversible actions.

2 The login will start to disappear

Passkeys, trusted devices, digital wallets and reusable credentials will make traditional logins less visible and less central.

Market signals

Passkeys are available across major technology ecosystems. Digital wallets and national identity systems, including Apple Wallet, the EU Digital Identity Wallet, Aadhaar and Singpass, continue to expand.

How to prepare

Design authentication around continuously established identity across devices, credentials and interactions rather than at a single login.

3 Fraud defence becomes a network – not a product

Collective intelligence will reveal relationships, patterns and threats no organisation can identify alone.

Market signals

Data-sharing networks, such as Cifas[4], Stop Scams UK[5] and Singapore's Anti-Scam Centre,[6] demonstrate this shift. US regulations also support information sharing.[7]

How to prepare

Determine where consortium intelligence, privacy-preserving collaboration and cross-industry partnerships can strengthen proprietary defences.

4 Proving identity will no longer be enough to establish digital trust

Confirming identity will remain essential, but it will not prove an interaction can be trusted.

Market signals

The growth of scams and authorised fraud demonstrates the limits of identity verification alone.

How to prepare

Connect identity verification with device, behavioural, communications and network intelligence across the customer lifecycle. Ask not only, "Is this the right person?" but also, "Should this interaction be trusted?"

5 Fraud intelligence will adopt a common operating language

The industry will adopt more consistent ways to describe fraud tactics, techniques and behaviours.

Market signals

MITRE's Fight Fraud Framework provides a behaviour-based taxonomy for financial fraud actors.[8]

How to prepare

Align fraud classifications with emerging frameworks and build data architectures that support interoperable, machine-readable fraud intelligence.

The connected future of fraud prevention

The most important lesson from the global fraud landscape isn't fraud has become more sophisticated. It's trust has become more valuable.

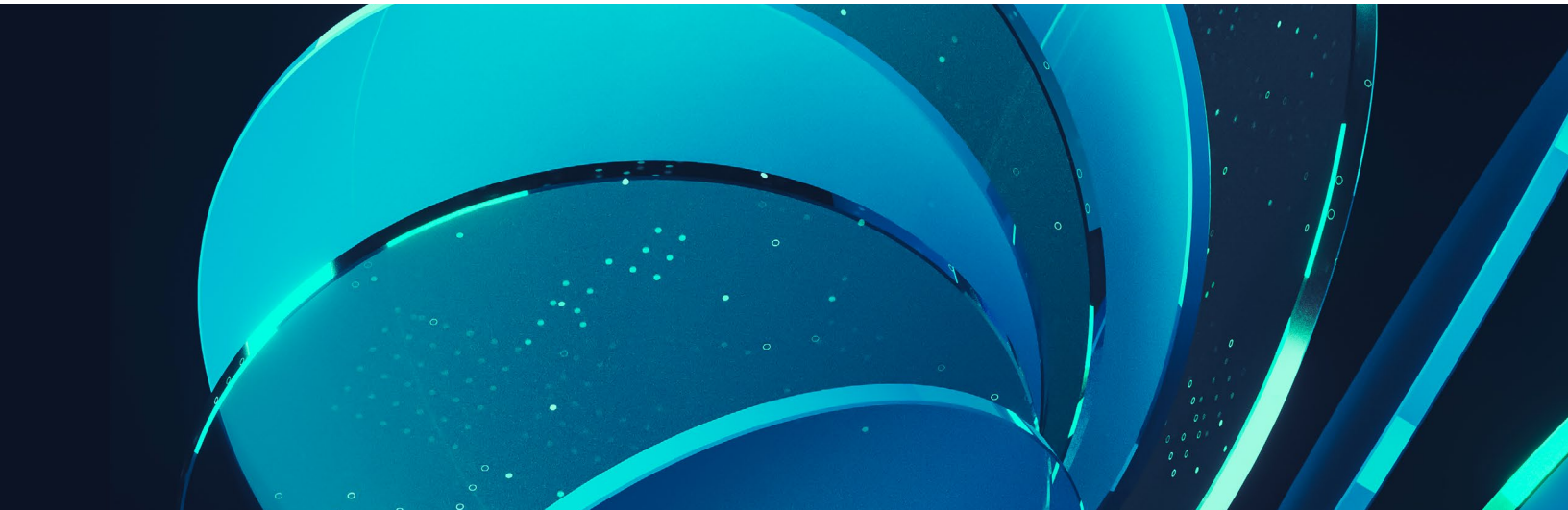
For decades, organisations treated trust as a point-in-time event established during onboarding, authentication or transaction approval. That model is increasingly disconnected from how digital fraud operates today.

Fraud now exploits identities after they're verified, communications after they're delivered and relationships after they're established. Organisations can no longer separate customer experience, risk management and fraud prevention into independent disciplines. They've become interconnected components of the same challenge: determining whether a digital interaction can be trusted.

Organisations that succeed won't necessarily be those that detect the most fraud. They'll be those that create the greatest confidence for customers, remove unnecessary friction and make better decisions through connected intelligence.

In the next era of digital commerce, trust will no longer be a control. It will be an asset. And increasingly, it will be a competitive advantage.

1,2 Javelin Group: 2026 Identity Fraud Study the Illusion of Progress, April 2026.
3 INTERPOL, INTERPOL African Cyberthreat Assessment 2026, August 2026.
4 Cifas.
5 Stop Scams UK.
6 Anti-Scam Centre Singapore.
7 US Department of Treasury's Financial Crimes Enforcement Network (FinCEN), USA PATRIOT Act Section 314(b) Fact Sheet, June 12, 2026.
8 MITRE's Center for Threat Informed Defense, Fight Fraud Framework, April 2026.



About the Research

This report combines findings from commissioned business and consumer surveys with insights derived from TransUnion's proprietary fraud, identity, credit and communications intelligence.

Business fraud survey

The business survey findings in this report are based on responses from 1,600 fraud and risk decision-makers at large, consumer-facing organisations across Brazil, Canada, Hong Kong, India, the Philippines, Spain, the United Kingdom and the United States.

The survey was conducted online from June 5–12, 2026, by TransUnion in partnership with third-party research provider Dynata. Respondents held managerial responsibility for fraud and/or risk and represented organisations with annual revenue exceeding BRL 300 million in Brazil, CAD 300 million in Canada, HKD 200 million in Hong Kong, INR 1 billion in India, PHP 1 billion in the Philippines, EUR 150 million in Spain, GBP 200 million in the United Kingdom and USD 200 million in the United States.

The survey was administered through an online research panel and completed across desktop, mobile and tablet devices.

Percentages may not total 100% due to rounding because some questions allowed multiple responses or "don't know" and "none of the above" responses were excluded.

Consumer pulse survey

Consumer survey findings in this report are based on responses from more than 13,500 adults age 18 and older across 19 markets worldwide.

The survey was conducted by TransUnion in partnership with third-party research provider Dynata using an online research panel. Fieldwork took place between Feb. 10 and Aug. 7, 2026 across Botswana, Brazil, Canada, Chile, Colombia, the Dominican Republic, Guatemala, Hong Kong, India, Kenya, Mexico, Namibia, the Philippines, Rwanda, South Africa, Spain, the United Kingdom, the United States and Zambia. Respondents completed the survey via desktop, mobile and tablet devices.

Survey questions were administered in Chinese (Hong Kong), English, French (Canada), Portuguese (Brazil) and Spanish (Colombia, the Dominican Republic, Guatemala and Spain). To help ensure representative results, quotas were used to balance responses across key demographic characteristics, including age, gender and income.

Percentages may not total 100% due to rounding or because some questions allowed multiple responses.

Data breaches

Data breach findings in this report are derived from TransUnion's proprietary breach database, maintained in partnership with the Identity Theft Resource Center (ITRC). The database tracks publicly reported US data exposure incidents using information from sources including state attorneys general, organisation disclosures, law firms and cybersecurity experts.

Each breach is evaluated using TransUnion TruEmpower™ Identity Threat Profile, which assesses exposed identity credentials, breach characteristics and associated consumer risk. Breaches are assigned a severity score on a scale of 1 to 10, where 1 represents the lowest level of risk and 10 represents the highest.

Reported percentages of exposed identity data are calculated only from breaches that disclosed compromised credential information and do not represent all reported data breaches.

Breach data is one of multiple risk signals used in the creation of TransUnion's Identity Safety Score — which helps assess an individual's overall identity risk profile and prioritise recommended protective actions.

Digital fraud

Digital fraud findings in this report are derived from TransUnion intelligence spanning billions of transactions across more than 40,000 websites and applications worldwide.

The suspected digital fraud rate represents the percentage of transactions identified by TransUnion clients as fraudulent or in violation of organisational policy. This includes transactions denied in real time due to fraud indicators or policy violations, as well as transactions later confirmed through customer or client investigation.

Country and regional analyses are based on transactions associated with clients operating in the applicable market. Global results reflect transaction activity across all countries represented within the TransUnion network and are not limited to the markets highlighted in this report.

When analysing transaction volume by customer journey stage, transactions classified as "other" were excluded. As a result, percentages across customer journey stages may not total 100%.

Outbound calls

Outbound call findings in this report are derived from mobile carrier data associated with calls to US consumers in which fraudsters impersonated legitimate financial institutions.

The reported spoofed call rate reflects instances in which caller identity information was falsified to appear as though calls originated from a trusted financial institution.

Because mobile carriers may attempt to reconnect unsuccessful calls multiple times, reported spoofed call volumes and rates may be slightly elevated.

Synthetic fraud

Synthetic fraud findings in this report are derived primarily from TransUnion's US consumer credit database, which contains credit information on approximately 400 million consumers across US states, territories and military installations in the US and abroad.

The database incorporates more than 50 years of consumer credit history. Synthetic fraud analyses included US credit activity recorded between Jan. 1, 2009 and June 30, 2026.

Lender exposure estimates were calculated using TransUnion's proprietary methodology designed to quantify potential lender losses associated with synthetic identity fraud.

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.

© Copyright 2026 TransUnion, its subsidiaries and/or affiliates. All Rights Reserved. | INT-AF-26-4909546

TransUnion