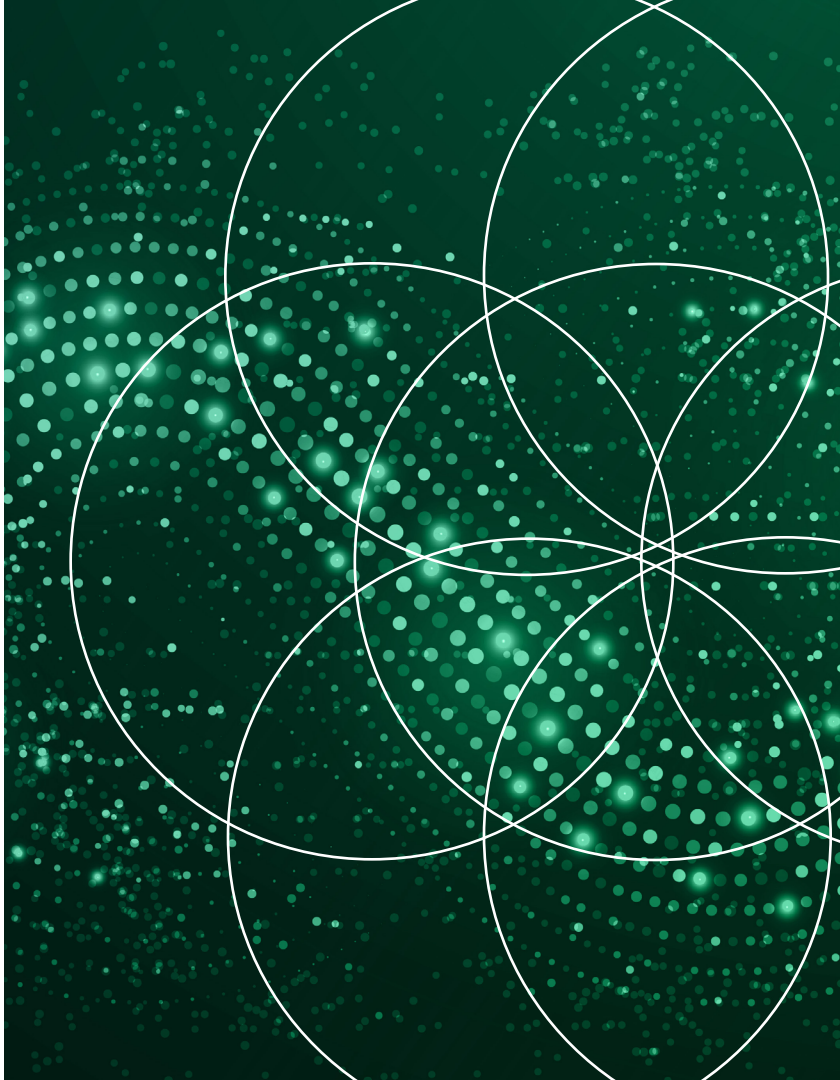
FORRESTER®

Rebuilding Trust In A High-Fraud Digital World

Exploring The Impact, Attributes, And Enterprise Actions Of Managing Consumer Trust Amid Rising Digital Fraud

Get started →

FORRESTER OPPORTUNITY SNAPSHOT:
A CUSTOM STUDY COMMISSIONED BY PROXIMUS GLOBAL | FEBRUARY 2026



Purpose, Scope, And Regional Considerations

Consumer trust has never been more integral, and in peril than ever before. With digital fraud on the rise, digital leaders need to act quickly and tactically safeguard their organizations against emerging AI vulnerabilities and eroding customer trust.

This report equips digital leaders at enterprises and technology providers who own user experience and digital safety to build trusted platforms that reduce fraud and protect customers effectively.

Regional Nuances

UNITED STATES

Nine percent of digital users encounter **daily fraud attempts**, as compared to 5% globally

FRANCE

Twenty-seven percent of digital users report **weekly fraud attempts**, as compared to 21% globally.

INDIA

Sixty-five percent report **an increase in fraud attempts this year**, as compared to 56% globally.

DEVELOPING MARKETS

In India, Brazil, and Indonesia, **messaging applications rank as the third most-trusted channe**l.

UNITED STATES AND UNITED KINGDOM

Overall **trust averages 42%**, below the global average of 47%.

Trust At Risk In The Digital Ecosystem

Customers increasingly integrate their lives within digital spaces, thus becoming more reliant on services from social platforms to healthcare applications. While these services improve convenience and productivity, they also expose users to rapidly escalating fraud across the digital ecosystem.

As fraud attempts grow, user trust in digital platforms continue to erode. Security and privacy rank as top user priorities, yet many perceive the ecosystem as failing to deliver, which creates a widening trust and accountability gap. The advent of AI has intensified these concerns, enabling more sophisticated fraud attempts and amplifying fears of misuse. Restoring trust now requires coordinated action across enterprises, platforms, and technology providers.

This study explores emerging fraud patterns, their impact on users and brands, and the actions organizations can take to strengthen trust and accountability across the digital journey.

Key Findings

Over half of users surveyed report higher frequency of fraud this year, with one in five facing weekly attempts. Among victims, the average monetary loss is around US$13,000.

Fraud breaks trust quickly. Only one in six users continued to engage with a brand after a fraud incident. In fact, 40% of fraud victims act on their experience by posting negative reviews on the brand.

Trust can be engineered with visible and layered security. Fraud alerts and multifactor authentication are top drivers for trust. Users favor clear security signals over invisible, seamless experiences.

Rising Digital Fraud Raises User Concern And Erodes Trust

Fraud attempts are on the rise globally: 87% of victims experienced fraud in the past year, while one in five users face at least one fraud attempt weekly.

The impact of a successful fraud attempt on the consumer is substantial across multiple factors. The top consequences are financial losses (73%), emotional distress (61%), and identity theft (56%). The average monetary loss in cases of financial fraud is US$13,037. Fraud also has a substantial impact on brands, affecting usage, customer loyalty, and reputation.

Consequently, 74% of users report an increasing concern about fraud, especially with more exposure to fraud attempts. More than 56% of users reported experiencing more fraud attempts in the past year, with markets such as India seeing an increase of almost 65% in reported attempts.

Fraud Experience And Brand Impact Funnel

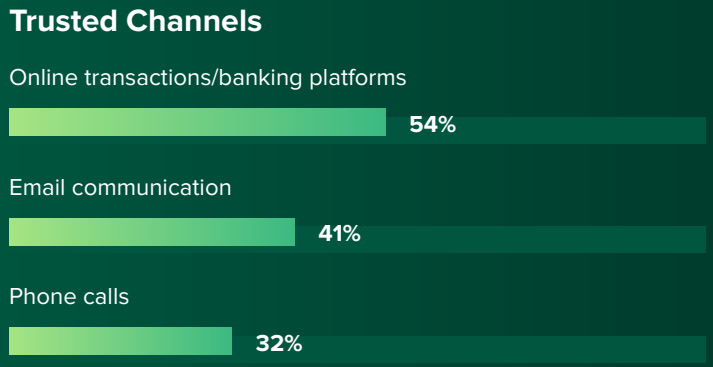
Base: 1,673 global digital users, aged 18 to 64 years
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

A Trust-Risk Mismatch Exists Across User Touchpoints

Trust exists even in the most vulnerable of channels. Users place their highest trust in official channels, such as online banking (54%) and emails (41%), yet these same channels are among the most exposed to fraud.

Across digital journey stages, payment or checkout is both the most trusted stage yet also most prone to fraud. It includes visible and additional security controls that augment trust, but it is also the point of value transfer, making it a target for fraudsters. This creates a mismatch between trust and risk across user touchpoints that enterprises need to address. In fact, users are currently filling this gap by trusting themselves more than digital services.

Meanwhile, recovery moments such as refunds and cancellations, are perceived with low trust — possibly due to opaque policies, resolution times, or a sense that the business may resist these requests.



Note: Showing sum of selected responses that ranked these channels within their top three
*Note: Showing top three fraud channels
Base: 498 global digital users aged 18 to 64 years who have been a fraud victim
*Base: 1,673 global digital users, aged 18 to 64 years
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Users Trust Themselves Despite Struggle To Independently Detect Fraud

Half of reported fraud attempts originate on social platforms, which are among the least trusted channels (19%), highlighting how fraudsters exploit scale, frictionless messaging, and weak identity controls. This suggests that many users struggle to reliably detect fraud — yet, they place greater trust in their own knowledge (57%) and perceived ability to recognize fraud (51%) than in digital services. This underscores a persistent trust gap and exposes a significant challenge in curtailing fraud at the most vulnerable channels.

Despite this, users place the onus for safety on telecommunications providers as well as on enterprises and governments, even when overall trust remains low. Enterprises are seen as accountable for traditional risks such as data breaches, while governments and providers are expected to address emerging threats like deepfakes. This reinforces the need for stronger protection delivered with minimal user friction.

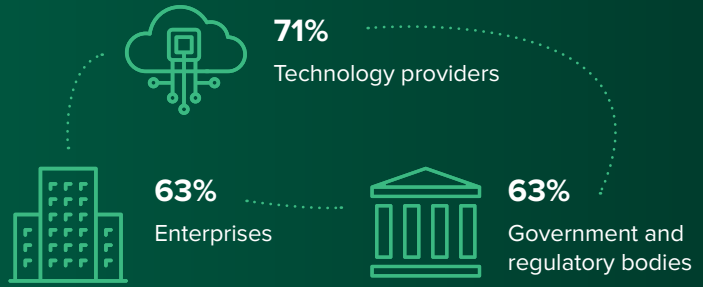
Consumer Trust: Self Vs. Digital Services*

57% Your own knowledge and awareness of digital safety and fraud

51% Your ability to recognize a fraud attempt

42% Digital services that I interact with will protect my personal data

Responsibility To Ensure Digital Safety



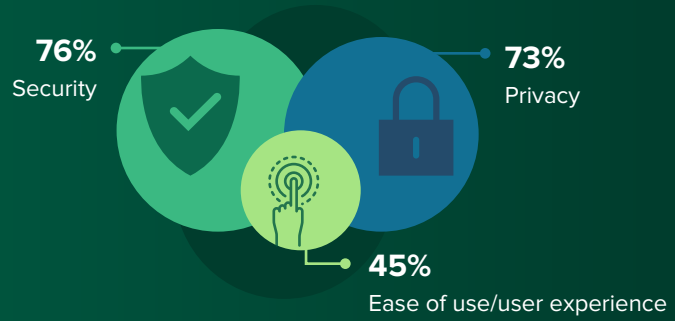
*Note: Showing top three sum for "Mostly trust" and "Completely trust" responses
Base: 1,673 global digital users, aged 18 to 64 years
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Users Prioritize Security And Privacy Ahead Of Convenience

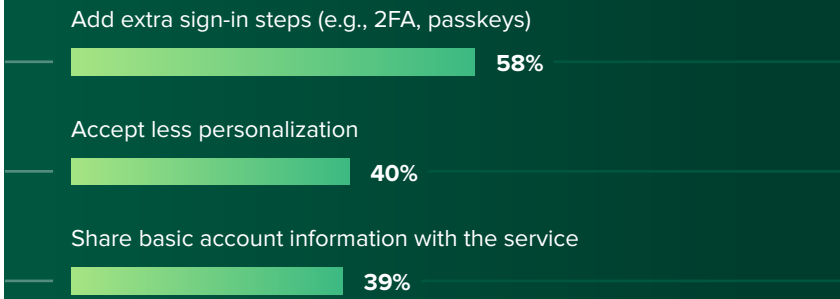
Digital users prioritize security (76%) and privacy (73%) over other elements of digital services, such as user experience (45%) and speed and performance (35%). They are willing to accept additional sign in steps (58%) but resist sharing personal and sensitive data, including device and application usage data (34%), browsing and transaction history (31%), and location access (29%), to improve these elements. This underscores the need to balance security and privacy.

About a third of users are willing to tolerate practical user experience and operational tradeoffs — such as less personalization and sharing basic account information — when these trade-offs result in greater security and privacy.

Important Aspects When Interacting With Digital Services



Acceptable Trade-Offs To Improve Top Priorities



Note: Showing top three sum for responses that ranked these aspects within their top three
*Note: Showing top three sum of responses for "Very willing" and "Extremely willing"
Base: 1,673 global digital users aged 18 to 64 years
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Fraud Has A Direct Impact On Brand Loyalty And Trust

Fraud victims lose trust quickly, driving immediate disengagement. After disengagement, victims move quickly into resolution mode, with more than half requesting refunds or contacting the brand to report the issue. This is when brands have an opportunity to stabilize the relationship by acknowledging the incident, responding quickly, and providing clear next steps.

Reputational damage often follows after victims attempt to resolve the issue by contacting the brand, with 43% proceeding to warn friends and family, and 38% posting negative feedback or reviews online. Regulatory risks also emerge, though they remain tail events: 23% file complaints with consumer protection authorities and 9% take legal action against the brand.

Ultimately, brand loyalty is fragile, with only 15% of fraud victims continuing to purchase from or engage with the brand after a fraud incident.

User Response To The Brand After Experiencing A Fraud Incident

Base: 498 global digital users aged 18 to 64 years who have been a fraud victim
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

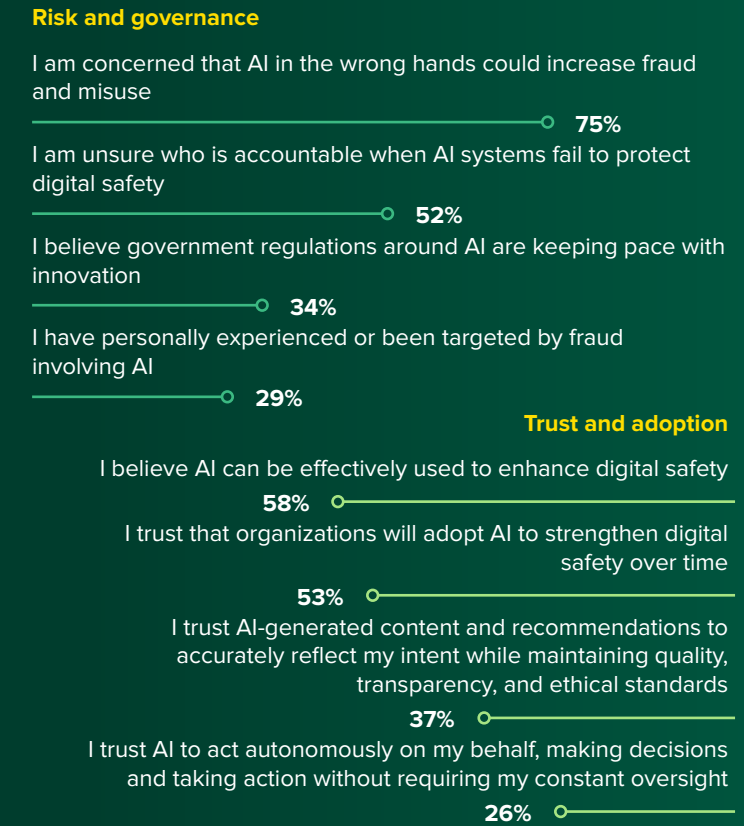
Users Believe AI Can Enhance Digital Safety, But Worry About Misuse And AI-Generated Outputs

Digital users are concerned about AI misuse increasing fraud (75%) and remain unsure on who is responsible when AI systems fail (52%). A significant 29% of users already report personal exposure to AI-related fraud. Among fraud victims, this rises to 39%, indicating growing use of AI in fraud attempts.

Apart from concerns about misuse, trust in AI-generated outputs and in its autonomy is low: Only 37% of users trust AI-generated content and only 26% trust AI to act autonomously without oversight. This indicates that there is still a long way to go before users trust generative and agentic AI outputs.

Despite these concerns, more than half of users believe AI can enhance digital safety and expect organizations to adopt it. Hence, even with low trust in AI outputs and use, users still view AI as an enabler for improving digital safety.

Impact Of AI On Digital Safety



Note: Showing sum of selected responses for "Agree" and "Strongly agree"
Base: 1,673 global digital users aged 18 to 64 years, who have been fraud victim
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Building Trust At Scale With AI And Network-Enabled Security

Fewer than half of users trust platforms to protect their data (42%) or prevent fraud (40%), revealing a persistent trust gap. Confidence improves when security is active and visible — such as real-time fraud alerts, multifactor authentication, OTPs, and identity prompts. Telecommunications providers uniquely extend these protections beyond individual apps, delivering trusted, network-level signals that enhance cross-channel security and reduce fraud exposure.

AI- and machine learning-driven fraud detection (62% each), alongside solutions like global identity verification (58%) further complement these measures. Unlike over-the-top (OTT) only or app-layer approaches, network-powered security delivers continuous, multichannel protection that reinforces trust at critical identity and access moments.

Security Features That Improve User Trust

75%
Fraud detection alerts if unusual activity is detected on your account

71%
Multifactor authentication before confirming payments or logging in

69%
Trusted payment badges or secure checkout indicators

69%
Easy access to customer support in case of suspected fraud or errors

67%
Understanding a brand's protection strategy

67%
OTP delivered via multiple channels (e.g., SMS, email, app notifications)

65%
Identity confirmation prompts for new devices or locations

64%
Clear communication on how your data is stored and used

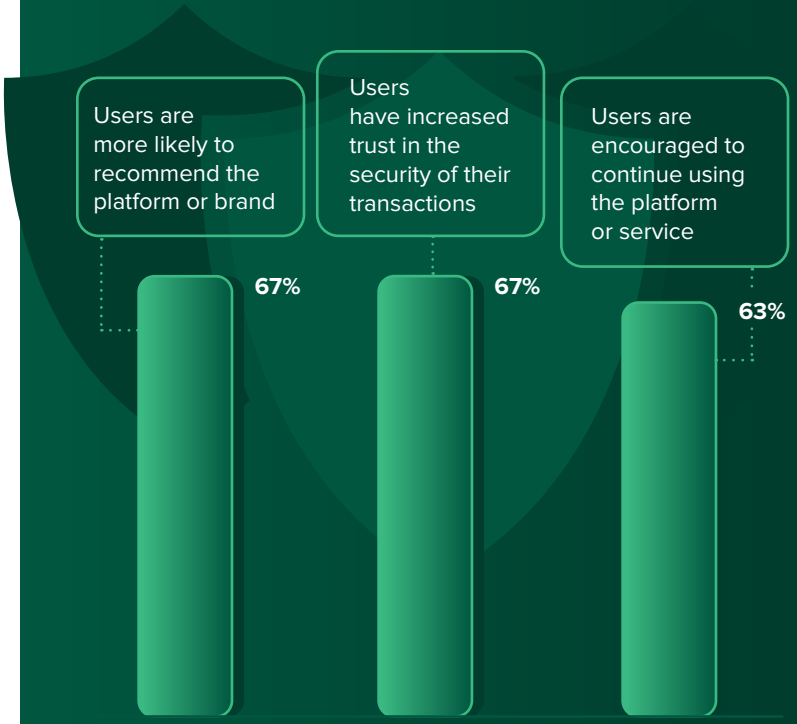
Note: Showing sum of top eight responses for "Important" and "Very important"
Base: 1,673 global digital users, aged 18 to 64 years
Source: Forrester's Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Trust Drives Consumer Loyalty, Advocacy, And Adoption

In the current digital landscape, trust is a critical driver of user engagement and platform adoption. Trust evokes positive user sentiments, primarily confidence (48%) and peace of mind (42%), which are essential for driving engagement and reducing adoption friction. Users who feel secure are more willing to try new features (61%), make purchases (61%), and share personal information (59%), behaviors that directly impact retention and growth.

Trust also strengthens advocacy. With trust, users are more likely to recommend platforms to others and continue engagement over time. Platforms that prioritize transparency, reliability, and effective security measures will capture long-term competitive advantage in a crowded digital landscape.

Impact Of A Trusted Platform

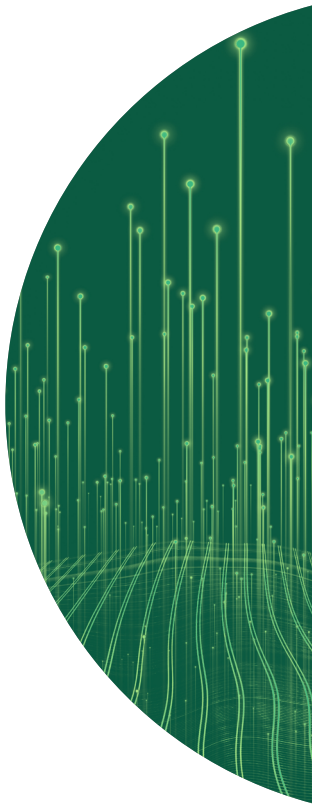


Note: Showing sum of selected responses for “Agree” and “Strongly agree”
Base: 1,673 global digital users, aged 18 to 64 years
Source: Forrester’s Q4 2025 Global Consumer Trust And Fraud Survey [E-66208]

Conclusion

Digital fraud is facing a rising trend, with significant consequences for victims and brands. Users are increasingly concerned about the misuse of AI to perpetrate fraud and face a paradox in which the touchpoints they trust most are among the most frequently targeted. A trust gap also persists, as users trust their own knowledge over digital services. For enterprises to be at the forefront of trust building, consider:

- Prioritizing the security of digital services while safeguarding user privacy, especially sensitive data.
- Making security and protection features visible to build user trust.
- Protecting brand loyalty by preventing fraud, and when incidents occur, acknowledge, respond quickly, and provide clear next steps to rebuild trust.
- Using AI to enhance digital safety with human oversight, transparent use, and proper governance.



Resources

Related Forrester Research:

The State Of Trust For US Health Insurers, 2024, Forrester Research, Inc., February 15, 2025

Related Resources

June 17, 2025, Generative AI In Customer IAM, AML, And Fraud Management, Webinar

Project Team:

Aneesh Ahuja, Market Impact Consultant

Alicia Choo, Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

Methodology

This Opportunity Snapshot was commissioned by Proximus Global. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 1,673 digital users from Brazil, France, Germany, India, Indonesia, the UAE, the United States, and the United Kingdom to gauge consumer trust and fraud experiences in the digital environment. Respondents represented digital users aged 18 to 64 across these eight territories. The custom survey began and was completed in December 2025.

Demographics

COUNTRY	
Brazil	12%
France	12%
Germany	12%
India	12%
Indonesia	13%
UAE	13%
United Kingdom	13%
United States	13%

EXPOSED TO FRAUD ATTEMPTS	
Exposed	59%
Not exposed	41%

DIGITAL SERVICES USED	
Dating applications	18%
E-commerce services	80%
Food delivery services	66%
Healthcare-related applications	39%
Maps or location-based services	67%
Online banking services	76%
Online chat and messaging services	65%
Online gaming platforms	50%
Payment services	76%
Social media platforms	83%
Transport/ ride-sharing/taxi services	46%

Note: Percentages may not total 100 due to rounding.

Demographics (Continued)

AGE (YEARS)	
18 to 24	**18%**
25 to 34	**21%**
35 to 44	**23%**
45 to 54	**20%**
55 to 64	**18%**

GENDER	
Male	**50%**
Female	**50%**

FRAUD PROFILE	
Experienced fraud	**30%**
Did not experience fraud	**70%**

Note: Percentages may not total 100 due to rounding.

FORRESTER®