

Safety in numbers

Trust and safety trends, 2025



Safety in numbers

Trust and safety trends, 2025

It's a critical moment for leaders tasked with maintaining customer trust. Increasingly sophisticated and pervasive fraud attempts, misinformation and cyber attacks, as well as the proliferation of harmful user-generated content (UGC), all threaten to erode confidence. But at the same time, advancements in technology are equipping brands with more and more powerful methods of detection and deterrence. The situation is delicately poised.

To effectively navigate this complexity, leaders are right to look at the broader context, including how their peers are addressing these very challenges. Here, you'll find trust and safety insights from a survey of other leaders. Here, you'll find safety in numbers.



This report covers



Challenges facing leaders in maintaining safe and secure digital environments



Data and analysis of four core areas: Fraud detection, Know Your Customer (KYC), content moderation and ID verification



Limiting factors leaders are managing as they deliver effective trust and safety solutions

Methodology

TELUS Digital commissioned Ryan Strategic Advisory to conduct a custom global survey in the first quarter of 2025, which forms the basis of this report. The survey reflects the views of 819 enterprise customer experience (CX) decision-makers in the following regions: Western Europe, North America and Asia-Pacific. Interviews were conducted via telephone in the following languages: English, French, Italian, Japanese, Korean, Dutch or German (depending on the respondent's country of residence). The revenue mix for enterprise respondents ranged from \$10 million to over \$5 billion.

About Ryan Strategic Advisory

Ryan Strategic Advisory provides market insight, brand development initiatives, and actionable data for organizations in the customer experience services ecosystem. With two decades of experience, Ryan Strategic Advisory supports outsourcing operators, technology providers, industry associations, and economic development agencies.

About TELUS Digital

TELUS Digital partners with innovative brands to manage risk, reputation, security and safety. With more than 78,000 global team members and an established ecosystem of technology partners, we apply a fusion of human expertise and advanced technologies to safeguard trust. Our solutions include, but are not limited to, fraud detection, Know Your Customer (KYC), anti-money laundering (AML), content moderation, identity and access management, and a full suite of security services.

“

Even as enterprises face mounting economic challenges, maintaining a safe and secure environment for their customers remains a top priority, as the risks of not doing so are simply too high.

Ljubiša Velikić

Vice President of Trust and Safety
TELUS Digital



Threats to safe and secure digital environments

We asked: What is the biggest challenge your business faces in maintaining a safe and secure digital environment for your customers?



* Respondents could select more than one option from a provided list.

Note: Due to rounding, percentages may not add up to 100.

The top three challenges facing leaders today are: data breaches and cyber attacks (45%), compliance with government regulations and industry standards (44%), and managing third-party risks (supply chain vulnerabilities) (43%). These particular challenges cast light on the enormity of the task facing leaders today: To maintain customer trust, they must have knowledge that is both broad and deep. It's not enough to know about the diverse and evolving digital threats, they must also understand and adapt to differing regulations across markets and industries, and have a firm grasp of how their partners operate.

Not only is there a lot to know, there is much to do. It is clear that leaders are feeling overwhelmed and under-resourced, citing availability of human resources/technical expertise (39%) and keeping up with technological change (lack of budget) (32%) as significant challenges. What's more, 34%

identified internal threats as a major challenge, which affirms that the task of educating employees on matters of trust and safety is a continuous, concerted effort.



Leaders are facing pressure to tighten budgets while keeping pace with evolving compliance standards. These challenges are making it harder to access the technical talent needed to deliver and maintain effective solutions. CX providers are well positioned to ease those pressures by offering the expertise, people and technology to scale trust, safety and security operations as needed.

Peter Ryan
President and Principal Analyst
Ryan Strategic Advisory



In focus:

Fraud detection

Reliably preventing and detecting fraud minimizes financial loss and reputational damage. But for many, this is easier said than done.

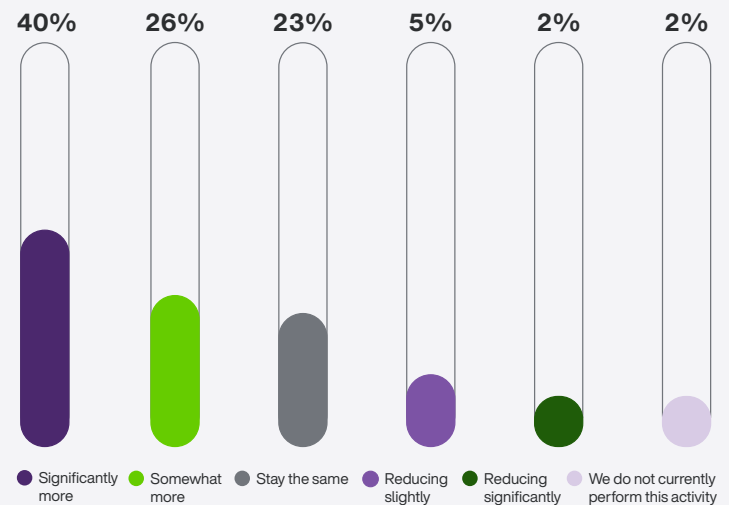
Challenging though it may be, leaders are responding. Two-thirds (66%) of those surveyed plan to invest more in fraud detection over the next 12 months. This investment aligns with the heightened prioritization of fraud detection, with 69% of respondents reporting that it has become a higher priority in the past year.

In terms of execution, to combat the sheer volume of fraudulent activity, leaders are turning to automation. In fact, 44% fend off fraud with technology alone, whereas hybrid human/technology approaches were most common for KYC, content moderation and ID verification.

Overall, the data indicates that fraud detection is at the forefront of trust and safety efforts, with leaders seeing it as an important way to minimize negative customer sentiment.

Investment

We asked: How will your company's investment in fraud detection services/solutions change in the next 12 months?

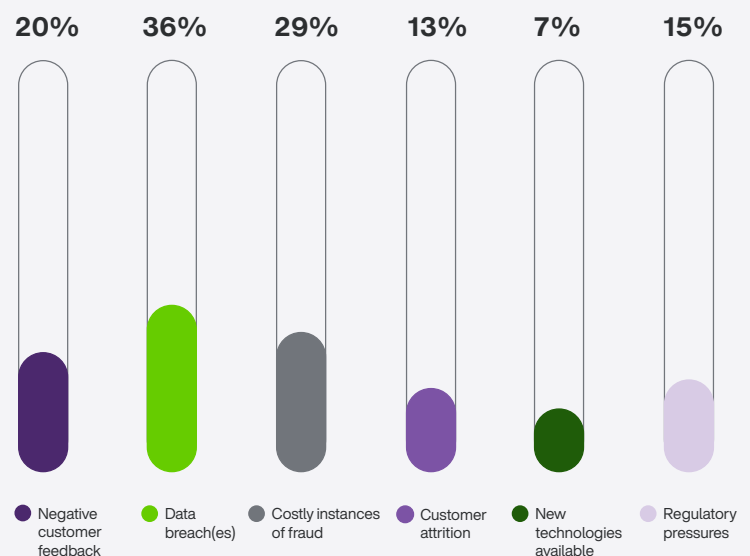


Prioritization

69% of respondents said fraud detection has become a higher priority in the past year as part of their CX delivery.

Motivation for prioritization

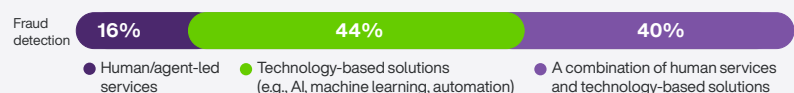
For those who said that fraud detection has become a higher priority, we asked why.



* Respondents could select more than one option from a provided list.

Approach

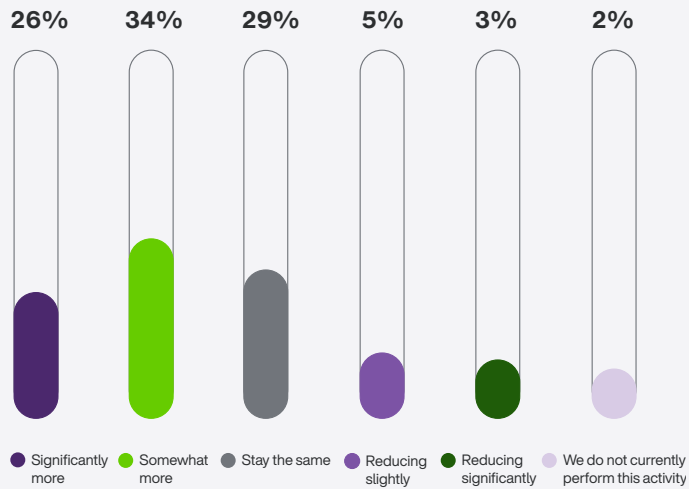
We asked: How does your company execute its fraud detection services/solutions?



Note: Due to rounding, percentages may not add up to 100.

Investment

We asked: How will your company's investment in KYC services/solutions change in the next 12 months?

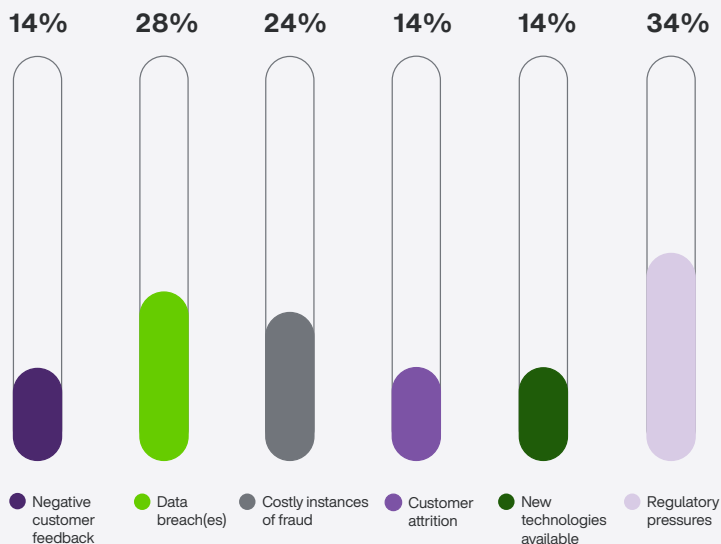


Prioritization

64% of respondents said KYC has become a higher priority in the past year as part of their CX delivery.

Motivation for prioritization

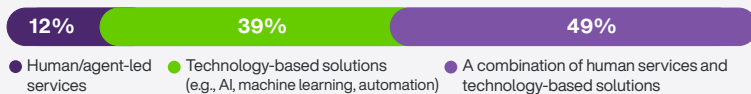
For those who said that KYC has become a higher priority, we asked why.



* Respondents could select more than one option from a provided list.

Approach

We asked: How does your company execute its KYC services/solutions?



Note: Due to rounding, percentages may not add up to 100.

In focus:

Know Your Customer

KYC programs play a fundamental role in evaluating customer risk profiles and monitoring to ensure their transactions align with expected behavior.

A substantial 60% of leaders plan to increase their investment in KYC in the next year, with 26% indicating “significantly more” investment. As was the case with fraud prevention, this aligns with prioritization data: 64% of respondents said KYC has become a higher priority in the past year.

Regulatory pressures were cited by just over one-third (34%) of respondents as a motivating factor to prioritize KYC. This can be traced back to the fact that 44% said compliance was the biggest challenge they faced in delivering a safe and secure environment for customers.

Nearly half (49%) of respondents take a hybrid approach to KYC, leveraging human services and technology. This finding highlights the importance of tapping into human expertise when it comes to understanding nuanced regulations, as well as the advantages of automation to detect anomalies at scale.

In focus:

Content moderation

Content moderation is necessary to protect brands and the public. By identifying UGC that violates community guidelines, government regulations and intellectual property laws, content moderation creates safe digital spaces for people to interact.

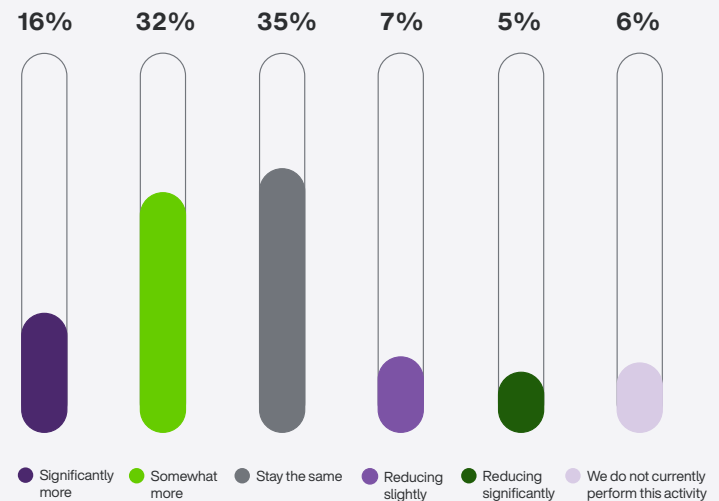
Nearly half (48%) of the surveyed leaders intend to invest more in content moderation this year. It is also interesting to note that only 6% of the 819 respondents do not currently perform content moderation. This highlights that content moderation is not specific to social media platforms, but rather it is a critical function for all digital platforms that support user interactions.

Relative to fraud detection, KYC and ID verification, a greater percentage (21%) of leaders execute their content moderation function through human-led services. This finding underscores the highly nuanced, dynamic world of content moderation and the value of a diverse and knowledgeable workforce. An optimized team has members fluent in relevant languages and who have an understanding of cultural, political and geographical contexts.

With that said, 44% deploy a hybrid model for content moderation, highlighting the advancements in AI and other technologies for this purpose, and that access to the right technology is essential in order to effectively scale operations and maintain trust.

Investment

We asked: How will your company's investment in content moderation services/solutions change in the next 12 months?

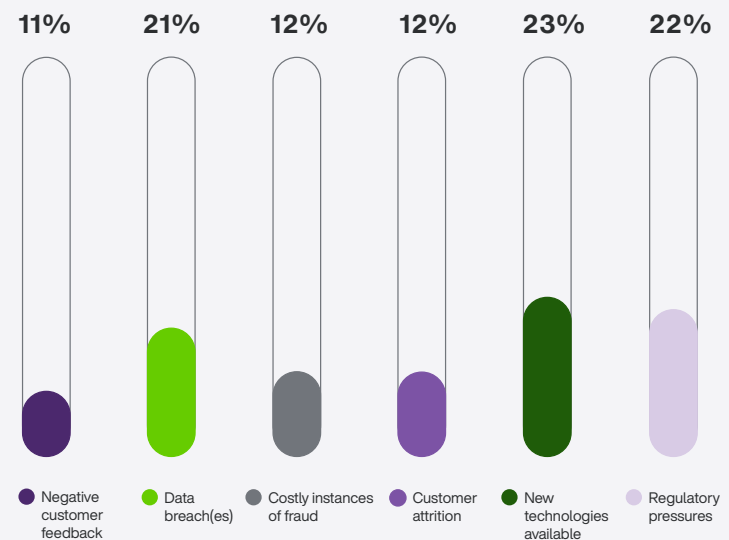


Prioritization

58% of respondents said content moderation has become a higher priority in the past year as part of their CX delivery.

Motivation for prioritization

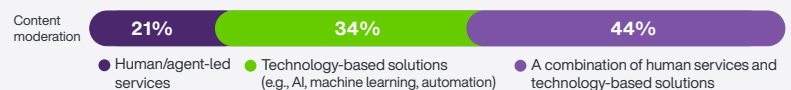
For those who said that content moderation has become a higher priority, we asked why.



* Respondents could select more than one option from a provided list.

Approach

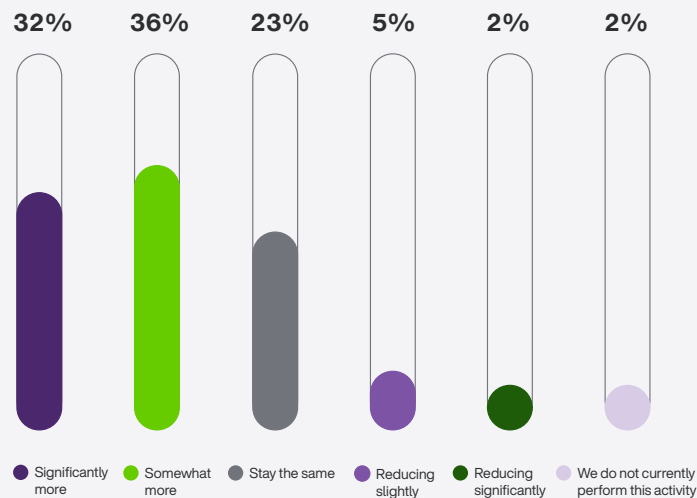
We asked: How does your company execute its content moderation services/solutions?



Note: Due to rounding, percentages may not add up to 100.

Investment

We asked: How will your company's investment in ID verification services/solutions change in the next 12 months?

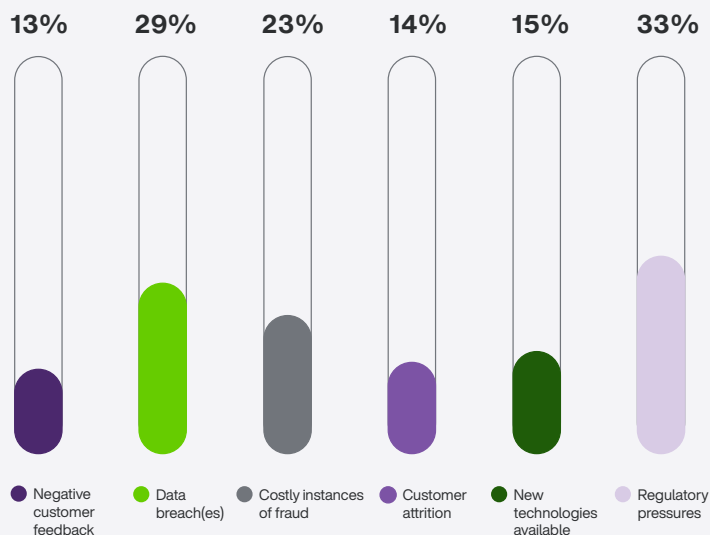


Prioritization

73% of respondents said ID verification has become a higher priority in the past year as part of their CX delivery.

Motivation for prioritization

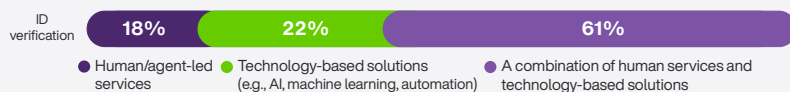
For those who said that ID verification has become a higher priority, we asked why.



* Respondents could select more than one option from a provided list.

Approach

We asked: How does your company execute its ID verification services/solutions?



Note: Due to rounding, percentages may not add up to 100.

In focus:

ID verification

While fraud detection, KYC and content moderation are core trust and safety functions, ID verification is more closely associated with information security (InfoSec). When executed effectively, InfoSec prevents unauthorized access to data or systems and protects against identity theft and other cyber crime.

More respondents (68%) are increasing their investment in ID verification than in any other domain. What's more, 73% said it has become a higher priority in the past year — once again making it the leading response.

The causes for investment in, and prioritization of, ID verification are clear. One-third (33%) cited regulatory pressures and 29% singled out data breach(es). Leaders have recognized the importance of maintaining compliance, and how doing so can both deter breaches and boost trust.

Finally, the majority of leaders (61%) operate a hybrid model for ID verification. While technology undoubtedly performs a critical function (as in the case with document scanning and biometric matching), human experts are needed to handle edge-cases and identify new fraud tactics that automated systems haven't yet been trained to recognize.

“

Customers expect that the companies they interact with will keep their private information safe and secure. In the presence of the evolving threat landscape, sophisticated and reliable ID verification is essential.

Michael Ringman

Chief Information Officer
TELUS Digital



Trust and safety program challenges

There's no getting around it: Cost is the primary challenge leaders are facing in running their trust and safety programs. That 27% of respondents identified cost as their greatest challenge suggests the need for cost-effective solutions. With what budget you do have, there is a heightened importance on scaling efficiently, potentially through partnerships with specialized providers.

Other challenges identified by leaders have a lot to do with a lack of expertise at their disposal. This was explicitly the case for 16% of respondents, but it can also be inferred by other responses. Technical complexity and integration with existing systems/architecture could become less daunting with the right personnel. A similar conclusion could also be drawn from the 10% who cited understanding/following regulations as their greatest challenge.

The challenges in earning and maintaining trust aren't static — they evolve alongside technology advancements and customer expectations. The data suggests that while cost is today's primary concern, the real challenge lies in developing and executing an agile and holistic strategy that can adapt to tomorrow's threats effectively and efficiently. Success will require leaders to find the right balance between developing internal capabilities and leveraging external expertise.

We asked: What is the greatest challenge your organization encounters in delivering effective trust and safety solutions across your digital channels?

Cost

27%

Technical complexity

21%

Integration with existing systems/architecture

20%

Lack of internal expertise

16%

Understanding/following regulations

10%

We do not currently perform any of these activities

6%

Note: Due to rounding, percentages may not add up to 100.

“

As organizations work to strengthen their approach to trust and safety, they need partners with deep expertise who also understand the complexities of implementing and scaling these solutions. It's increasingly clear that flexibility, experience, and the ability to manage end-to-end delivery are essential to helping enterprises stay resilient in a constantly evolving risk landscape.

Ljubiša Velikić

Vice President of Trust and Safety
TELUS Digital



There's safety in numbers

This report has equipped you with important information about how your peers are evolving their trust and safety operations. The charts, data and analysis have sought to show safety in numbers.

The truth is, customer trust has always been hard to earn and easy to lose. But if you ask leaders, you'll see that the nature of the challenge is different today. The pace of innovation, the specter of regulation, the array of threats and the cost of consequences are very real.

The good news is that you don't need to go it alone.

Brands partner with TELUS Digital to:

- Gain access to multilingual talent around the globe and at scale.
- Leverage a complete partner ecosystem of the latest and greatest technology.
- Minimize risk associated with technology investment.
- Keep up with an increasing volume of threats while managing cost.
- Benefit from earned expertise and understanding of local context.



20+

Years of experience



31

Countries of operation



>78K

Team members



650+

Global clients



120+

Awards



Solutions

Account Takeover Prevention
Ad Moderation
Anti-Money Laundering
Chargebacks
Content Labeling and Annotation
Content Moderation
Fraud Prevention and Detection
Identity Verification
KYC
Phishing Management
Transaction Monitoring

Looking to bolster your trust and safety program?

We can help.

telusdigital.com/contact/sales