2026 ANTI-FRAUD TECHNOLOGY BENCHMARKING REPORT

ACFE
Association of Certified Fraud Examiners

sas

TABLE OF CONTENTS

7%

Only **7%** of organizations are **more than moderately prepared to detect and/or prevent AI-POWERED FRAUD**.

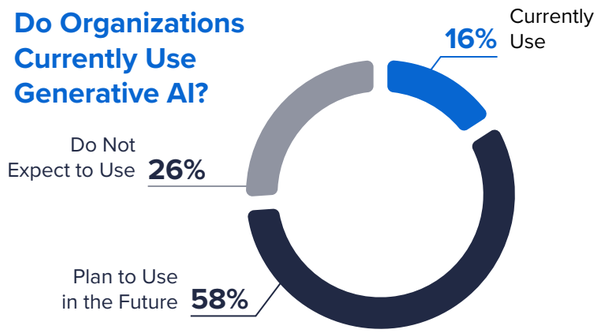
These schemes have increased the most over the past two years:

- **Deepfake Social Engineering**
- **Consumer Fraud/Scams**
- **Generative AI Document Fraud/Forgery**
- **Deepfake Digital Injection**

Generative AI in Anti-Fraud Programs

Accuracy of results or output was the **most important factor** in considering whether to implement generative AI as part of an anti-fraud program, with **86%** of organizations rating it important or very important.

Do Organizations Currently Use Generative AI?



Among organizations using generative AI, it is most commonly used for:

- **Phishing and Scam Detection (49%)**
- **Risk Identification/Assessment (46%)**
- **Report Writing (45%)**

One in four organizations (25%) now use **AI/Machine Learning in their anti-fraud data analysis initiatives,** up from 18% in 2024.

25%

28%

Another 28% of organizations **expect to adopt AI/Machine Learning** within the next two years.

82% say explainability or auditability is an important factor in **adopting generative AI, while 6% feel completely confident** explaining how AI/ML models make anti-fraud

82%
consider explainability important

75%
consider bias important

75% of respondents consider **AI models' bias or lack of fairness** an important factor for adopting the technology, but **only 18% of respondents' organizations test their AI models for bias or fairness.**

KEY FINDINGS

62%

QUANTUM COMPUTING/ QUANTUM AI

A majority of survey respondents **(62%)** expect quantum computing/quantum AI to materially impact fraud detection and prevention within five years.

Budget or financial restrictions are the most common challenge in implementing new anti-fraud technology, affecting **83%** of organizations.

83% of organizations

55% of organizations

More than half of organizations **(55%)** expect to **increase their budgets for anti-fraud technology** over the next two years.

Only 10% of organizations use cloud-native fraud detection platforms.

10%

Only **29%** of organizations automate routine fraud investigation tasks

29%

51%

About half of organizations (51%) either currently contribute or are willing to **contribute to data consortiums** to aid their anti-fraud efforts.

45%

Of the emerging technologies tracked in the report since 2022, **physical biometrics** usage in anti-fraud programs has **increased** the most, from **34%** to **45%**, making it the most adopted emerging technology.

INTRODUCTION

The utilization of technology by both organizations and the fraudsters who target them has become one of the defining characteristics of the anti-fraud profession in recent years. Anti-fraud professionals and organizational leaders must take steps to continually evaluate both long-standing and emerging technologies. The capabilities need to consider their potential impact as components of a comprehensive anti-fraud program, as well as a source of threats to defend against.

To help organizations and anti-fraud professionals in this endeavor, the ACFE and SAS have partnered to conduct a series of studies on the use of technology in anti-fraud programs by organizations throughout the world. This benchmarking report represents the fourth edition of this series, and for the first time incorporates information about how fraudsters are using technology to further their schemes. We have also expanded the breadth of technologies explored in the report, including more generative artificial intelligence (AI) tools and their applications, quantum computing, automation, and cloud computing. The findings of this study are valuable for anti-fraud professionals, the organizations that employ them, and others in the industry. The report provides insights into opportunities and vulnerabilities presented by technologies, benchmarking of anti-fraud programs' technology, and how to preparing for future technological developments with fraud resilience at the forefront.

The ACFE would like to thank SAS for their partnership and expertise in conducting this *Anti-Fraud Technology Benchmarking Report*, with special consideration for Stu Bradley, Senior Vice President - Risk, Fraud and Compliance Solutions.

METHODOLOGY

In October 2025, we sent a 30-question survey to 77,392 ACFE members. Respondents were asked to provide information about their organizations' use of various technologies as part of their anti-fraud initiatives, as well as fraudsters' use of technologies in perpetrating their schemes. Survey responses were collected anonymously. We received 713 survey responses that were usable for purposes of this report. This report provides a summary of respondents' answers to the survey questions, as well as select comments noted by respondents in relation to certain survey topics. (For data on participant demographics, including geographic region and industry, see Respondent Demographics section on page 38.)

The 2026 *Anti-Fraud Technology Benchmarking Report* was developed in partnership with SAS Explore the survey results with interactive charts based on various demographic categories, including industry and geographic region at sas.com/fraudsurvey. SAS.com/fraudsurvey.

HOW ARE ORGANIZATIONS USING DATA ANALYTICS IN THEIR ANTI-FRAUD INITIATIVES?

WHAT DATA ANALYSIS TECHNIQUES DO ORGANIZATIONS USE TO FIGHT FRAUD?

As in our prior studies, the vast majority (82%) of organizations noted the use of at least one type of data analytics technique as part of their anti-fraud programs. When looking at the specific types of techniques, most use cases remained relatively flat or saw a very minor decrease over the last two years. Exception reporting/anomaly detection and automated red flags/business rules analyses remain the most commonly used techniques, with roughly half of organizations in our study currently employing them.

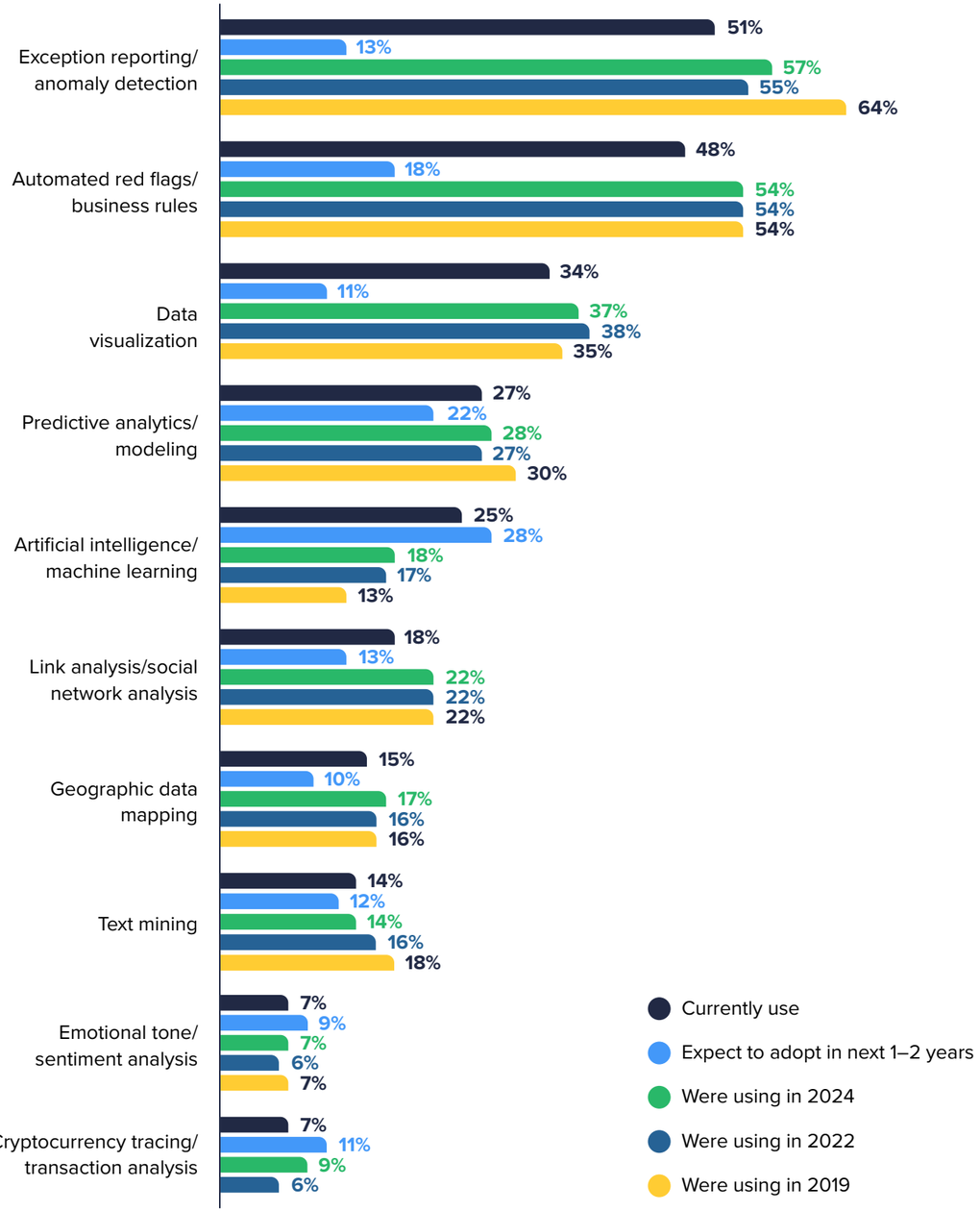
Not surprisingly, the primary exception, and the largest change observed, relates to the use of artificial intelligence and machine learning (AI/ML). The percentage of organizations incorporating this technology in their anti-fraud analytics programs grew from 18% in 2024 to 25% in 2026. This technology also has the highest percentage of organizations (28%) expecting to adopt it in the next one to two years, which would result in more than half of organizations employing AI/ML for anti-fraud analytics purposes by 2028.

- **Only 34% of organizations use unstructured data in their data analytics programs.**
- **54% of organizations use both internal and external data sources in their data analytics programs.**

54%
of organizations

> **Data analytics makes anti-fraud initiatives faster, smarter, and more proactive, helping in detecting fraud early in real time, improving accuracy, reducing losses, and strengthening trust."**
>
> – Survey respondent

FIG. 1 What data analysis techniques do organizations use to fight fraud?



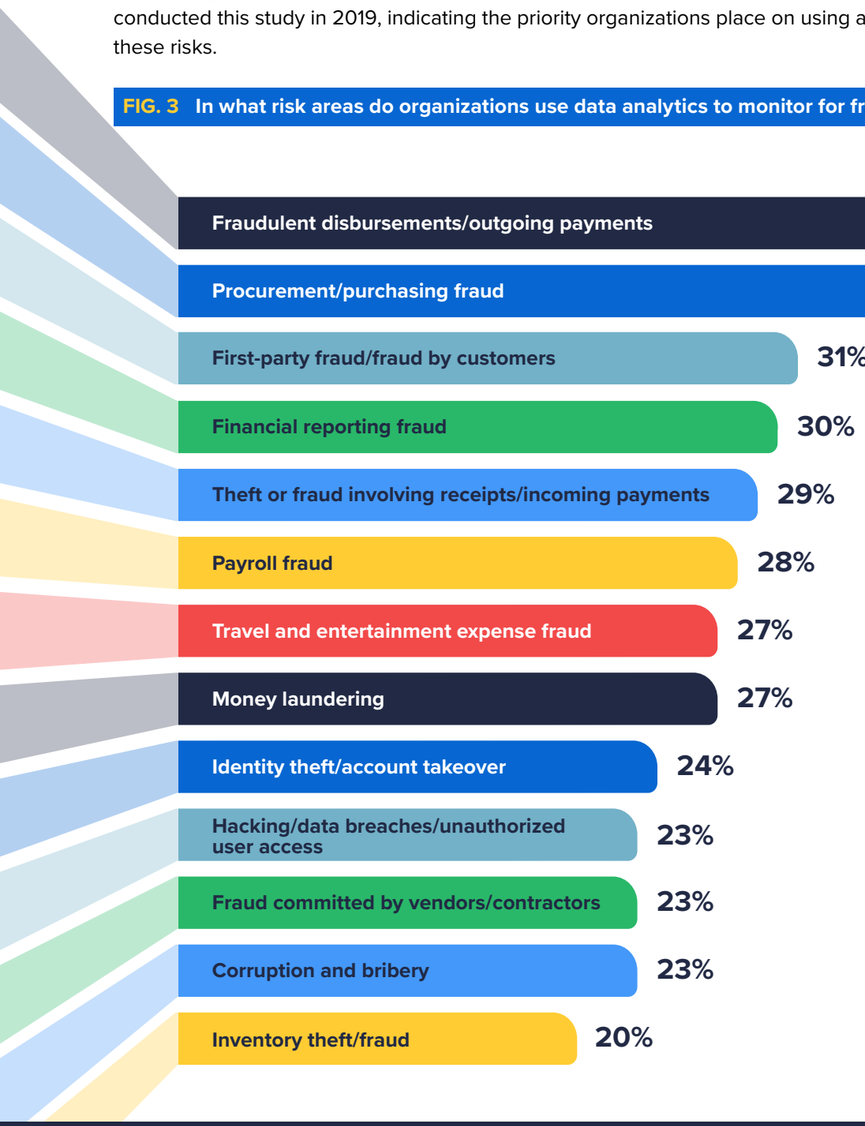
For each type of analytics noted in Figure 1, we asked respondents what program(s) their organization uses to deploy the related techniques. The responses indicate that many organizations are still relying on proprietary tools that are developed in-house for many components of their anti-fraud analytics programs. Dedicated analytics tools with a variety of applications, such as SAS, ACL, and Tableau, were noted by respondents in several categories. Both PowerBI and Excel were also noted in multiple categories, likely because many organizations either already have these tools as part of their primary tech stack for other professional functions or still rely on desktop capabilities for their analytics program.

FIG. 2 What are the most commonly used programs for each analytic technique?

IN WHAT RISK AREAS DO ORGANIZATIONS USE DATA ANALYTICS TO MONITOR FOR FRAUD?

Effectively fighting fraud generally requires a risk-based approach, so that organizations target their efforts, resources, and investments to the areas that present the greatest potential threats. We asked respondents in which risk areas their organizations currently use data analytics to monitor for fraud. The top risk areas noted are fraudulent disbursements/outgoing payments (43% of organizations) and procurement/purchasing fraud (39% of organizations). These have consistently been the top two risk areas for fraud analytics since we first conducted this study in 2019, indicating the priority organizations place on using analytics to detect fraud related to these risks.

FIG. 3 In what risk areas do organizations use data analytics to monitor for fraud?



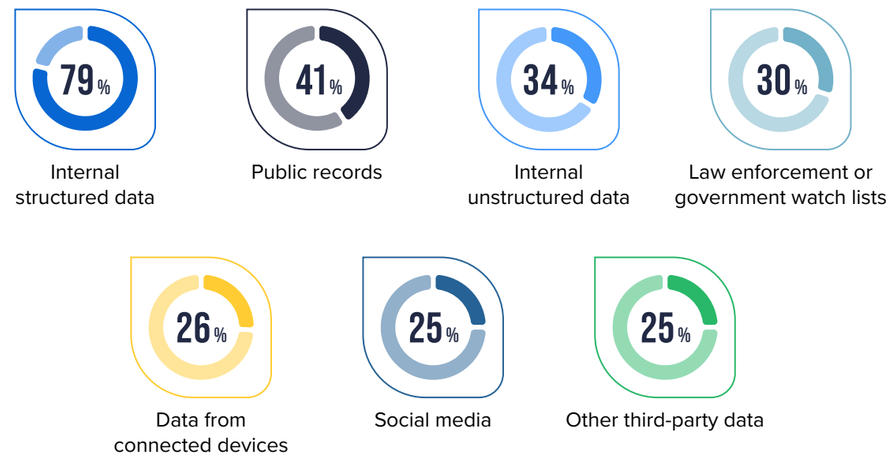
WHAT SOURCES OF DATA DO ORGANIZATIONS USE IN THEIR ANTI-FRAUD DATA ANALYTICS INITIATIVES?

The red flags of fraud can be found in a variety of data sources that originate both inside and outside the organization. As noted in Figure 4, most organizations' anti-fraud analytics programs (79%) use internal structured data—that is, data that exists in recognizable and predictable formats (e.g., data found in spreadsheets and databases). This is followed by data from public records, which is used by 41% of organizations in their anti-fraud analytics initiatives. Just over one third (34%) of organizations also incorporate internal unstructured data (i.e., data found outside of structured formats, such as text, images, or videos) into their anti-fraud analytics programs.

In addition, combining data from multiple sources can provide better visibility into potential risks and can result in earlier detection. Nearly two-thirds of respondents (64%) noted that their anti-fraud analytics initiatives incorporate more than one data source, and more than half (54%) use data from both internal and external sources.

> **"We work with unstructured data, which is 75% of the data universe, to understand human behavior and anticipate the intention to commit fraud and other unethical acts."**
>
> – Survey respondent

FIG. 4 What sources of data do organizations use in their anti-fraud data analytics initiatives?



HOW BENEFICIAL IS DATA ANALYTICS TO DIFFERENT AREAS OF ORGANIZATIONS' ANTI-FRAUD INITIATIVES?

Consistently high adoption rates for data analytics in each edition of this benchmarking report illustrate the value of incorporating data analysis in anti-fraud programs. To contextualize that value, we asked survey respondents about the impact of data analytics in four key areas:

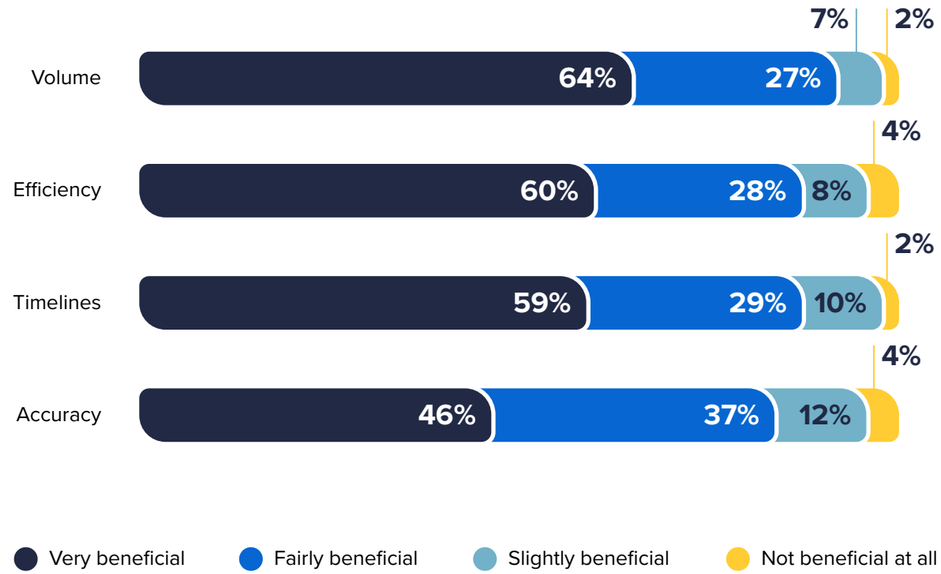
- **Volume**, or the ability to review more transactions or identify more cases of suspected fraud.
- **Timeliness**, or the ability to detect anomalies more quickly.
- **Efficiency**, or the ability to automate time-consuming tasks.
- **Accuracy**, or the ability to reduce false positive rates.

A significant majority of survey respondents indicated that incorporating data analytics into anti-fraud initiatives led to benefits in each of the above categories, as seen in Figure 5. At least 80% of respondents indicated that using data analytics was at least fairly beneficial for volume (91%), timeliness (88%), efficiency (88%) and accuracy (83%). The area in which the largest percentage of respondents indicated that data analytics were very beneficial was volume.

> **Data analytics has been highly beneficial in enhancing our anti-fraud initiatives by enabling broader transaction coverage, faster anomaly detection, and improved efficiency. It now serves as a key enabler of proactive and data-driven fraud risk management."**
>
> – Survey respondent

> **Data is only as good as what is put in. Many times, fraud is related to what is not put into the system (missing data)."**
>
> – Survey respondent

FIG. 5 How beneficial is data analytics to different areas of organizations' anti-fraud initiatives?



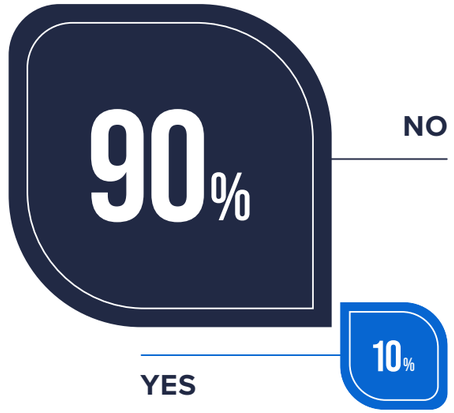
DATA ANALYTICS

WHAT OTHER TECHNOLOGIES ARE ORGANIZATIONS USING IN THEIR ANTI-FRAUD INITIATIVES?

ARE ORGANIZATIONS USING CLOUD-NATIVE FRAUD DETECTION PLATFORMS?

Many organizations have opted to utilize cloud-native platforms in recent years for a variety of operations, including fraud detection. Cloud computing can offer organizations the opportunity to handle massive data volumes and activity spikes while also enhancing security and cost efficiency. However, the use of cloud computing in anti-fraud programs appears relatively limited at this time, with **only 10% of respondents' organizations currently using cloud-native platforms for fraud detection purposes (see Figure 6)**.

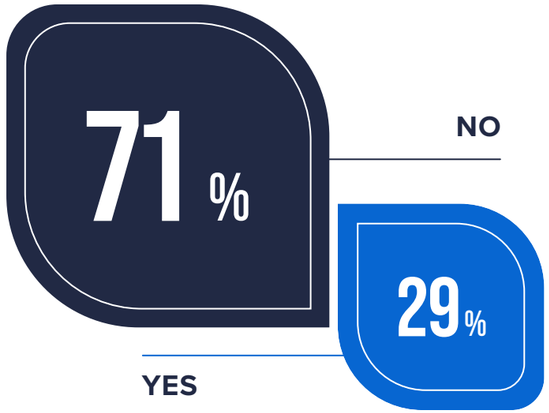
FIG. 6 Does your organization currently use any cloud-native fraud detection platforms?



ARE ORGANIZATIONS AUTOMATING ROUTINE FRAUD INVESTIGATION TASKS?

Many of the technologies in this report have features that allow organizations to automate routine fraud investigation tasks that previously would have required manual completion by employees or service providers. By automating tasks, anti-fraud functions can potentially operate more efficiently, with reduced labor costs and an increased scope of activity. As seen in Figure 7, 29% of survey respondents indicated that their organizations have adopted automation of tasks in their fraud investigations.

FIG. 7 Does your organization currently automate any routine fraud investigation tasks?



Automating routine investigation work is often the first step in the generative and agentic AI journey. When organizations do that well, they free investigators to focus on complex cases, improve detection strategies, and get ahead of emerging fraud threats."

– Stu Bradley,
Senior Vice President,
Risk, Fraud and Compliance Solutions, SAS

OTHER TECHNOLOGIES

WHAT EMERGING TECHNOLOGIES ARE ORGANIZATIONS USING TO FIGHT FRAUD?

As fraudsters continuously evolve their schemes and tactics by incorporating new technologies, organizations must also evaluate emerging technologies for anti-fraud applications to keep pace. We have asked respondents about which categories of emerging technologies their organizations either currently use or expect to adopt in each edition of this benchmarking report. For this edition, we updated the list of technologies to better capture the emerging technology landscape.

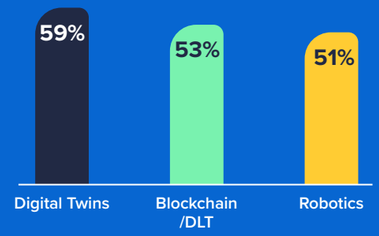
As in each of our previous editions, the emerging technology currently used by the most organizations is physical biometrics, which is used to identify individuals based on physical attributes such as fingerprints and facial or vocal features. Implementation of physical biometrics has grown from 34% in 2022, to 40% in 2024 and 45% in 2026.

The emerging technology expected to be adopted in the future by the most organizations was computer vision analysis, with 46% of organizations expected to incorporate this technology into their anti-fraud programs, followed by behavioral biometrics, synthetic data and blockchain/ distributed ledger technology, each expected to be incorporated by 37% of organizations.

Emerging technologies are transforming anti-fraud initiatives by shifting the focus from reactive detection to proactive prevention, enabling the firm to identify suspicious activity earlier, reduce losses, and strengthen trust."

– Survey respondent

MORE THAN HALF OF ORGANIZATIONS
DO NOT EXPECT TO EVER ADOPT...



Physical biometrics use unique, measurable biological characteristics—such as fingerprints, facial recognition, iris scans, or voice patterns—to verify a customer's identity.

Behavioral biometrics analyze patterns in how a person interacts with devices or systems—typing rhythm, mouse movement, swipe patterns, device orientation, or how they hold a phone.

Robotics or Robotic Process Automation (RPA) uses software "bots" to automate repetitive, rule-based tasks such as data capture, case triage, reporting, or workflow routing.

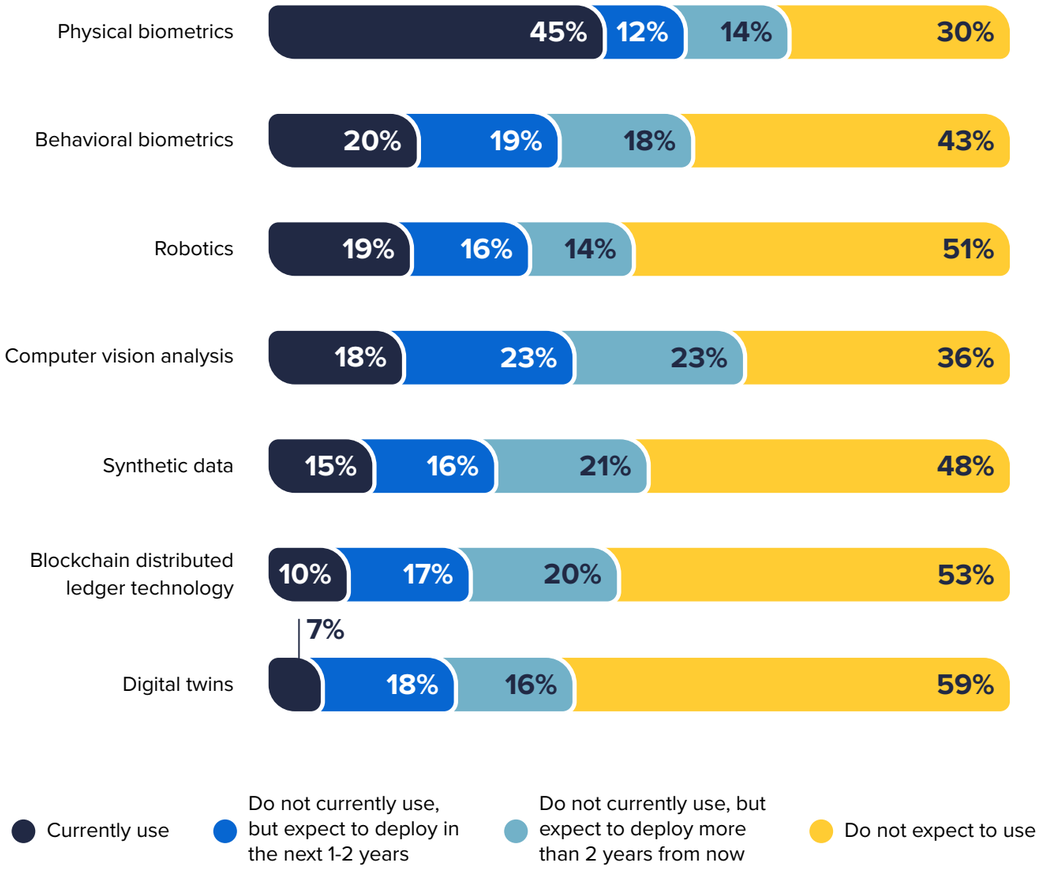
Computer vision uses AI to analyze images or video and extract meaningful patterns, classifications, or anomalies.

Synthetic data is artificially generated data that mimics real customer or transaction data without exposing sensitive details.

Blockchain and other forms of distributed ledgers record transactions across a decentralized network, creating an immutable, transparent, and tamper-evident audit trail.

A digital twin is a virtual replica of a system, process, or customer environment that behaves like the real thing using real-time or simulated data.

FIG. 8 What emerging technologies are organizations using to fight fraud?



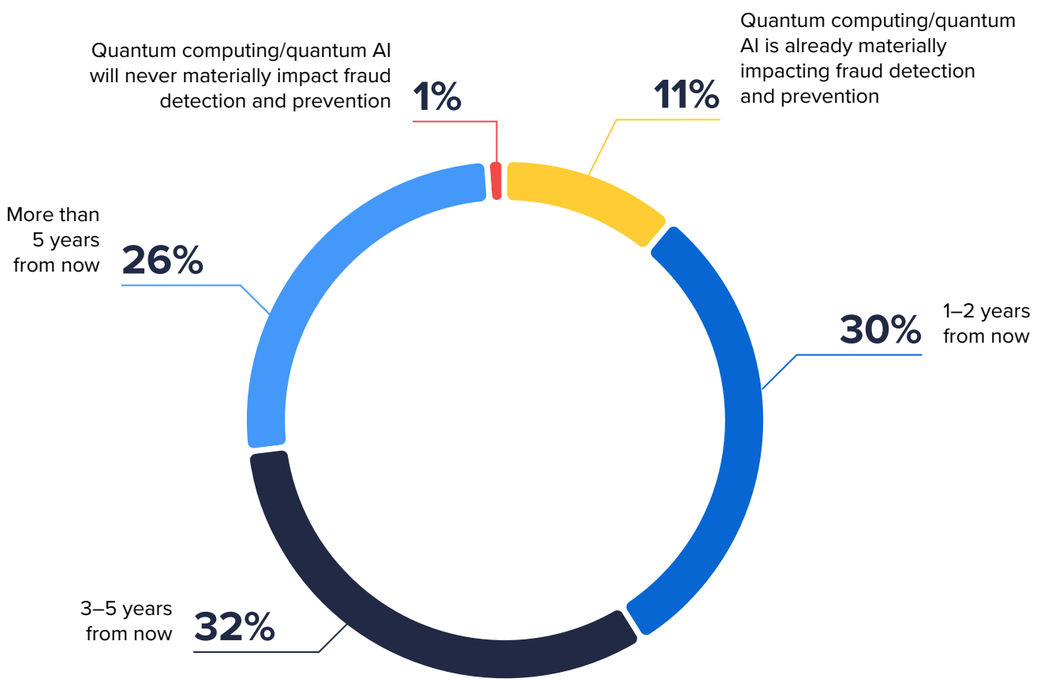
QUANTUM COMPUTING'S IMPACT ON FRAUD DETECTION AND PREVENTION

Quantum computing, which is based on quantum mechanics principles in physics, is one of the most advanced forms of technology ever developed. This technology has gone from being theoretical to tangible, as experimental development of quantum computing hardware has led to supercomputers capable of solving incredibly complex mathematical problems that would take classical computers hundreds or thousands of years to solve.

As the technology advances and becomes more practical, it both poses risks to cryptographic security measures and opportunities for enhancements, strengthening cryptographic security and safeguarding against quantum-enabled cyber threats that could compromise financial systems.

As seen in Figure 9, 11% of our survey respondents believe quantum computing and quantum AI is already materially impacting fraud detection and prevention, and 30% expect it to have a material impact in the next 1 to 2 years. Conversely, only 1% of respondents don't believe it will ever do so.

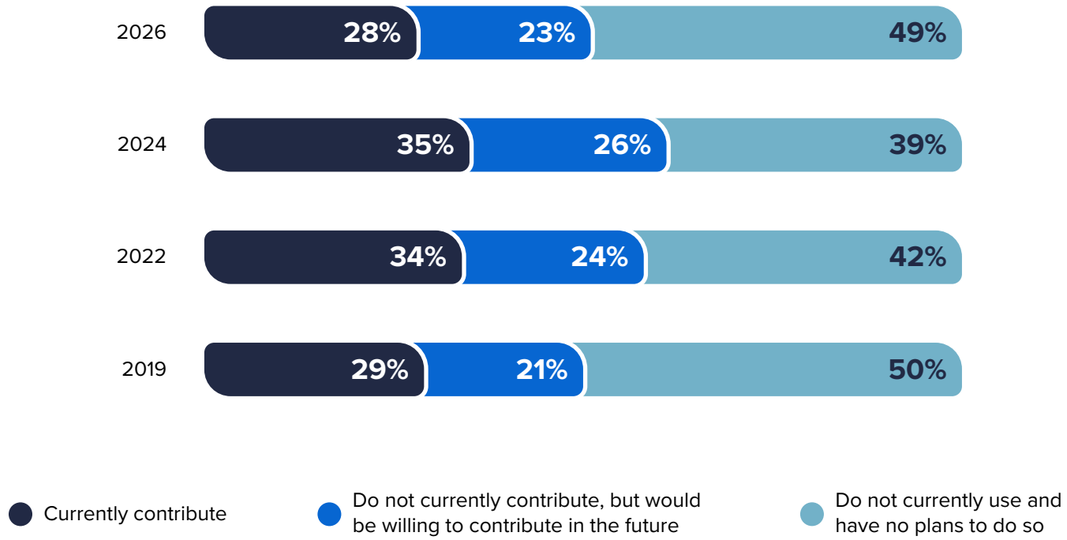
FIG. 9 How soon do you expect quantum computing or quantum AI to materially impact fraud detection and prevention?



ARE ORGANIZATIONS CONTRIBUTING TO DATA-SHARING CONSORTIUMS TO HELP PREVENT OR DETECT FRAUD?

Data sharing consortiums enable organizations to gain insight from data beyond what they collect and maintain on their own, which can provide significant benefits in fraud prevention and detection. The larger data sets provided by a consortium enhance the ability to detect patterns that can be incorporated in monitoring systems, potentially helping organizations prevent fraud that has impacted other organizations before they experience it themselves. However, after gradual increases across each previous edition of this report, the percentage of organizations that contribute to data sharing consortiums decreased from 35% in 2024 to 28% in 2026. Additionally, fewer organizations would be willing to contribute to data sharing consortiums in the future.

FIG. 10 Are organizations contributing to data-sharing consortiums to help prevent or detect fraud?



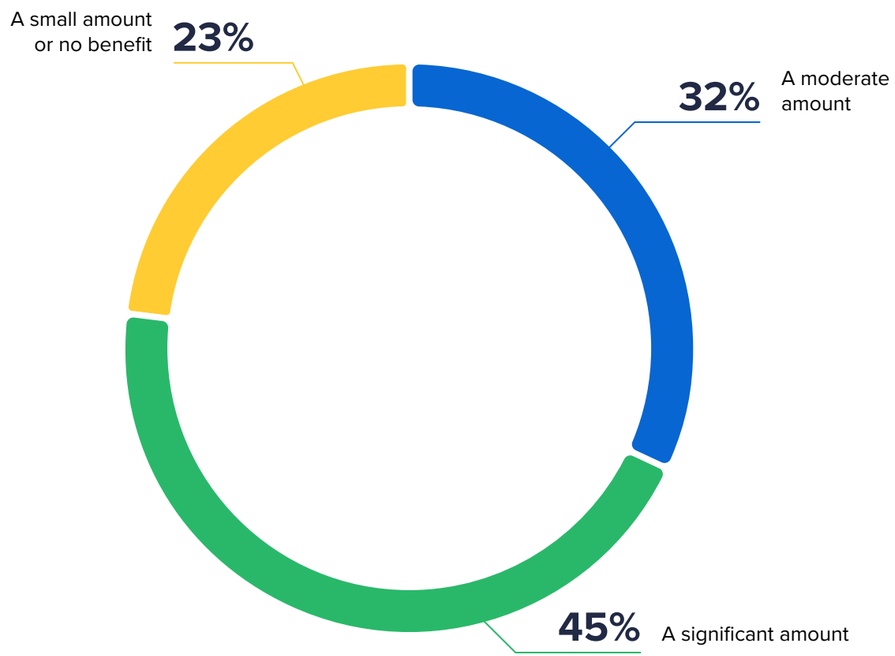
OTHER TECHNOLOGIES

HOW MUCH HAVE ORGANIZATIONS' ANTI-FRAUD PROGRAMS BENEFITED FROM DATA-SHARING CONSORTIUMS?

We asked respondents whose organizations do contribute to data sharing consortiums about the benefits of their participation. A majority of respondents indicated that their organizations have benefited, with almost half (45%) benefiting a significant amount, and just under a third (32%) benefiting a moderate amount.

> **Data sharing has increased the accuracy in reporting, which makes reports useful in confirming or [dispelling] fraud allegations"**
>
> – Survey respondent

FIG. 11 How much has your organization's anti-fraud program benefited from participating in a data-sharing consortium?

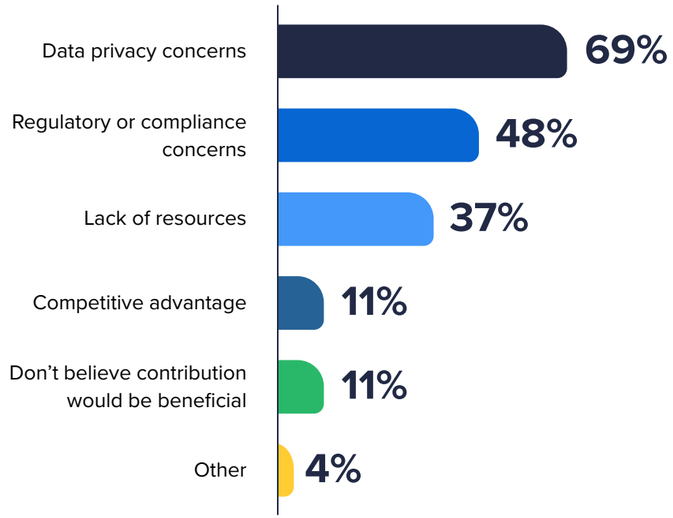


OTHER TECHNOLOGIES

WHY DON'T ORGANIZATIONS CONTRIBUTE TO DATA-SHARING CONSORTIUMS?

To understand why organizations would forgo the potential benefits of contributing to a data-sharing consortium, we asked respondents whose organizations don't currently or never expect to about their reasons for not contributing. The most common reason, cited by more than two-thirds of respondents (69%), was data privacy concerns, which was significantly ahead of the next most common reason, regulatory or compliance concerns (48%). Only 11% of respondents indicated that their organization does not participate in a consortium because they do not believe contributing would be beneficial.

FIG. 12 For which of the following reasons does your organization not contribute to a data-sharing consortium for purposes of detecting and preventing fraud?



Concerns about participating in a data-sharing consortium are reasonable, but many organizations have found a path they are comfortable with and are rewarded by more informed anti-fraud decisions. As risks are constantly evolving, data sharing consortium participation can be a big advantage compared to a perspective limited by only relying on the data your organization captures."

– Mason Wilder, CFE,
Research Director, ACFE

WHAT CHALLENGES DO ORGANIZATIONS FACE IN IMPLEMENTING NEW ANTI-FRAUD TECHNOLOGIES?

WHAT CHALLENGES DO ORGANIZATIONS FACE IN IMPLEMENTING NEW ANTI-FRAUD TECHNOLOGIES?

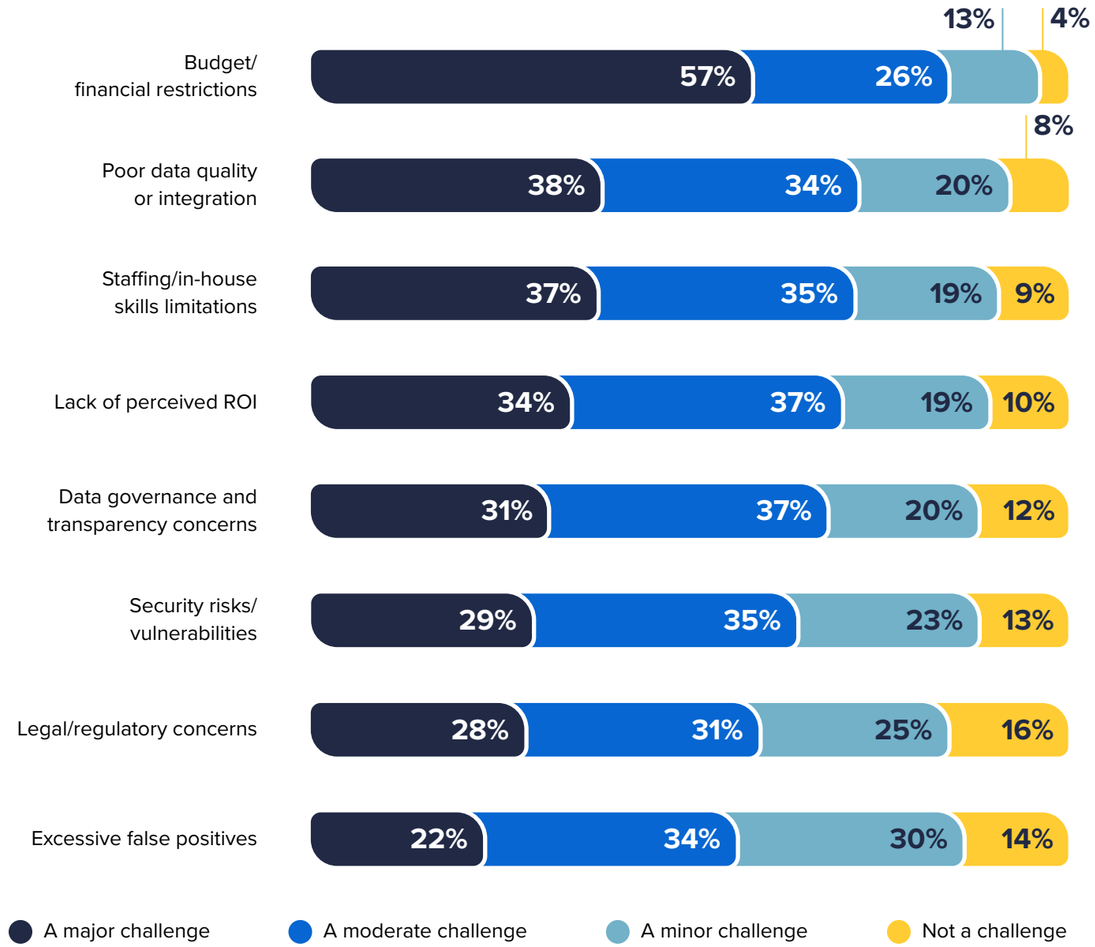
Onboarding and implementing new technology is never as simple as identifying a helpful tool and immediately plugging it into organizational operations. Organizations must weigh the potential benefits of the new technology against its cost, assess how it will integrate into current systems and processes, consider any legal or regulatory compliance impacts, and ensure staff are trained to use the technology effectively. Additionally, determining whether to become an early adopter of a new technology or wait for it to mature through several rounds of updates can be a difficult decision, as can deciding which provider of a technology to trust with important business operations.

To help anti-fraud professionals navigate these and other considerations, we asked survey respondents to rate the significance of common challenges associated with implementing new technologies. As with each previous edition of this benchmarking report, budget and financial restrictions were cited as a major challenge by the most respondents (57%), with a large margin separating it from the next most common major challenges of poor data quality/integration (38%) and staffing/in-house skills limitations (37%).

> **There are challenges around early adoption, leading to higher costs and a large number of false positives."**
>
> – Survey respondent

> **Rapidly changing technology and multiple options make it difficult to determine which is the best and most economical technology to use."**
>
> – Survey respondent

FIG. 13 What challenges do organizations face in implementing new anti-fraud technology?



CHALLENGES

HOW IS AI AFFECTING ORGANIZATIONS' ANTI-FRAUD PROGRAMS?

HOW IS AI AFFECTING ORGANIZATIONS' ANTI-FRAUD PROGRAMS?

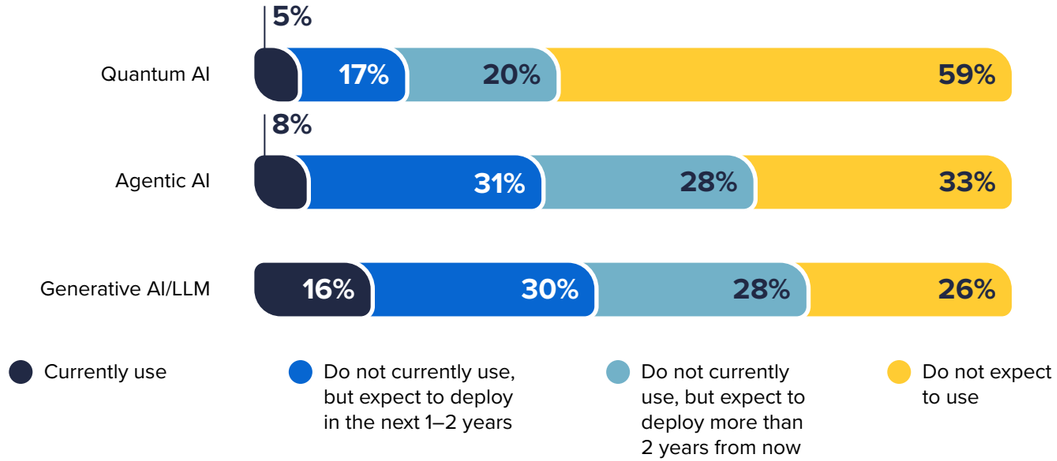
AI has had a significant impact on the anti-fraud profession over the last few decades, and its applicability to anti-fraud programs has been a prominent theme in each edition of this benchmarking report. Over the years, this report has tracked its integration from primarily featuring data analytics, to the much broader range of anti-fraud applications and artificial intelligence categories reflected in this edition of the report.

Generative AI in particular has seen rapid growth and adoption by individual users, as well as organizations, since the debut of ChatGPT 3 in late 2022, leading to significant investment in, and development of, this category of artificial intelligence. Anti-fraud professionals have now had some time to consider use cases for generative AI in the detection, investigation, and prevention of fraud. Data security was a limitation to adoption by critical industries like banking. Only recently has enterprise availability and adoption of computing capabilities through Graphic Processing Units by banks is now made the inhouse deployment of GenAI possible.

In addition to identifying effective and appropriate anti-fraud applications for the technology, organizations must navigate challenges related to AI, some of which are familiar hurdles that have been part of the implementation of other technologies, while others are unique to AI.

To provide a more in-depth perspective on the use of AI in anti-fraud programs, we explored the aforementioned considerations with several questions not featured in our previous anti-fraud technology benchmarking studies.

FIG. 14 Which of the following emerging types of AI does your organization expect to adopt in the next 1-2 years?



GenAI and LLMs create or interpret text, code, and patterns by learning from vast amounts of data. In fraud, they augment human analysts by interpreting signals, generating insights, or automating reasoning tasks.

Agentic AI refers to autonomous AI "agents" capable of taking actions, making decisions, and orchestrating workflows with minimal human intervention—going beyond prediction to execution.

Quantum AI combines quantum computing principles with AI algorithms to enable dramatically faster and more complex computation than classical systems (as this technology matures).

> **The biggest barrier to advanced AI adoption isn't interest—it's data readiness and governance. Until organizations trust their data and manage the full AI lifecycle, these technologies will stay experimental instead of delivering real value. Winners will be defined as those who embrace governance as an accelerator for innovation."**
>
> – Stu Bradley,
> Senior Vice President,
> Risk, Fraud and Compliance Solutions, SAS

> **The implementation [of generative AI] requires a balance the technology's power and addressing its risks by careful planning and human oversight and focus on upskilling employees."**
>
> – Survey respondent

> **We used artificial intelligence to draft certain parts of [a] report, primarily to more quickly locate legal grounds and regulations related to the violation, as well as to verify the traceability of transactions and correlate the roles of the organizations' employees."**
>
> – Survey respondent

> **[Our organization] is in an early adoption phase of generative AI for fraud analytics and communication. Use cases being piloted include narrative report generation, fraud typology pattern discovery, and staff awareness modules. Broader integration is planned post-regulatory clarity on explainability and data privacy."**
>
> – Survey respondent

ARTIFICIAL INTELLIGENCE

FOR WHICH ANTI-FRAUD APPLICATIONS DO ORGANIZATIONS CURRENTLY USE OR EXPECT TO USE GENERATIVE AI?

Generative artificial intelligence (AI) has been reshaping the technological landscape for a few years now. While our previous reports asked whether organizations expected to adopt generative AI, now that generative AI is becoming more widely considered for deployment in anti-fraud initiatives, we expanded our inquiries to include the current and expected anti-fraud applications for these tools.

Of the respondents whose organization currently use generative AI in their anti-fraud programs, almost half indicated that it is deployed for phishing and scam detection (49%), followed closely by risk identification/ assessment (46%) and report writing (45%).

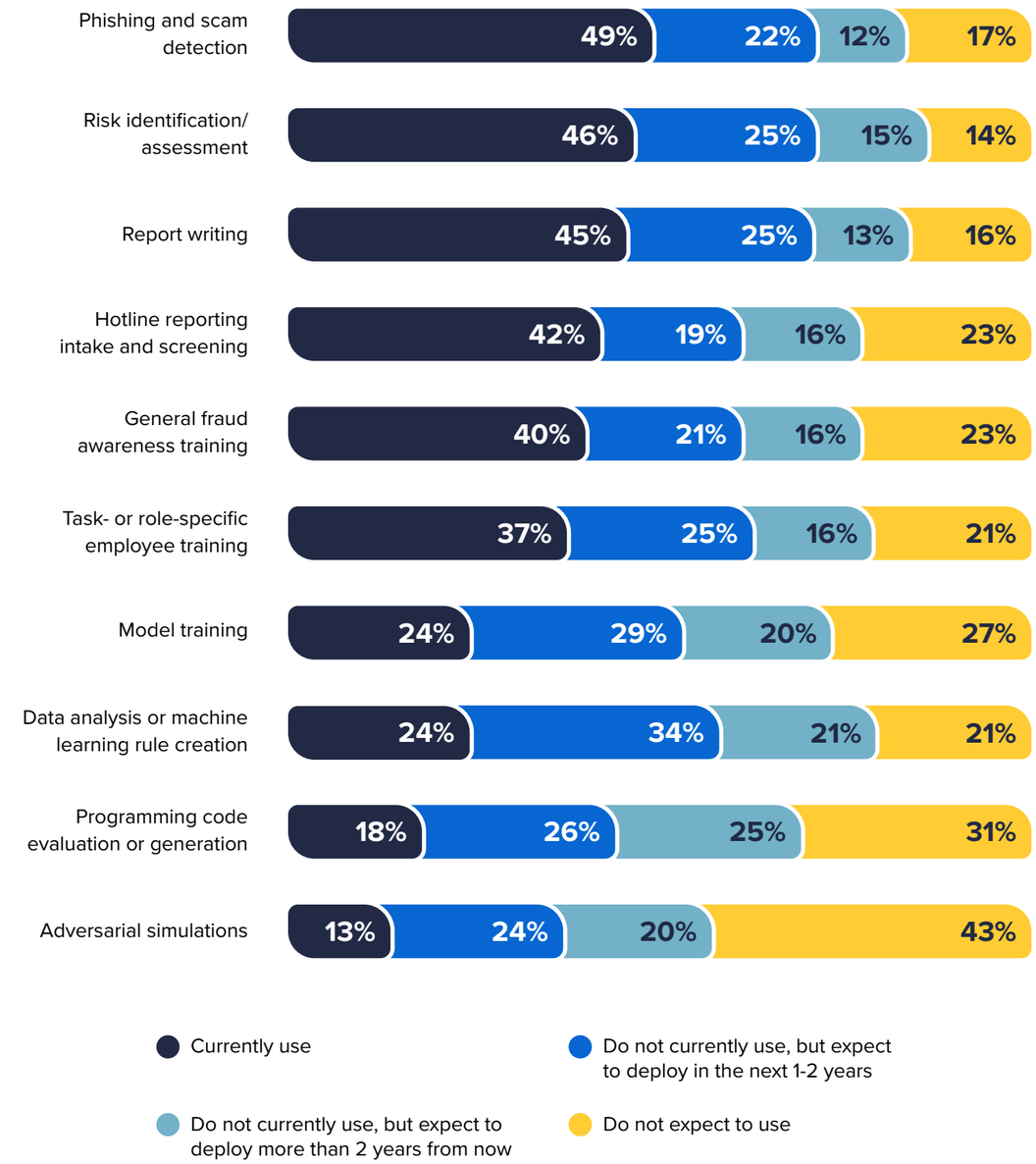
The applications of generative AI that are expected to be deployed by the most organizations in the future include rule creation for data analysis or machine learning (55%), programming code evaluation or generation (51%), and model training (49%).

At least 70% of respondents' organizations either currently use generative AI or expect to within two years for **phishing/scam detection, risk identification/ assessment and report writing.**

70%
of organizations

> **Anti-fraud use cases for generative AI are maturing quickly, with a lot of really sharp anti-fraud professionals creatively utilizing its capabilities and constantly iterating to improve results."**
>
> – Mason Wilder, CFE,
> Research Director, ACFE

FIG. 15 For which anti-fraud applications do organizations currently use or expect to use generative AI?



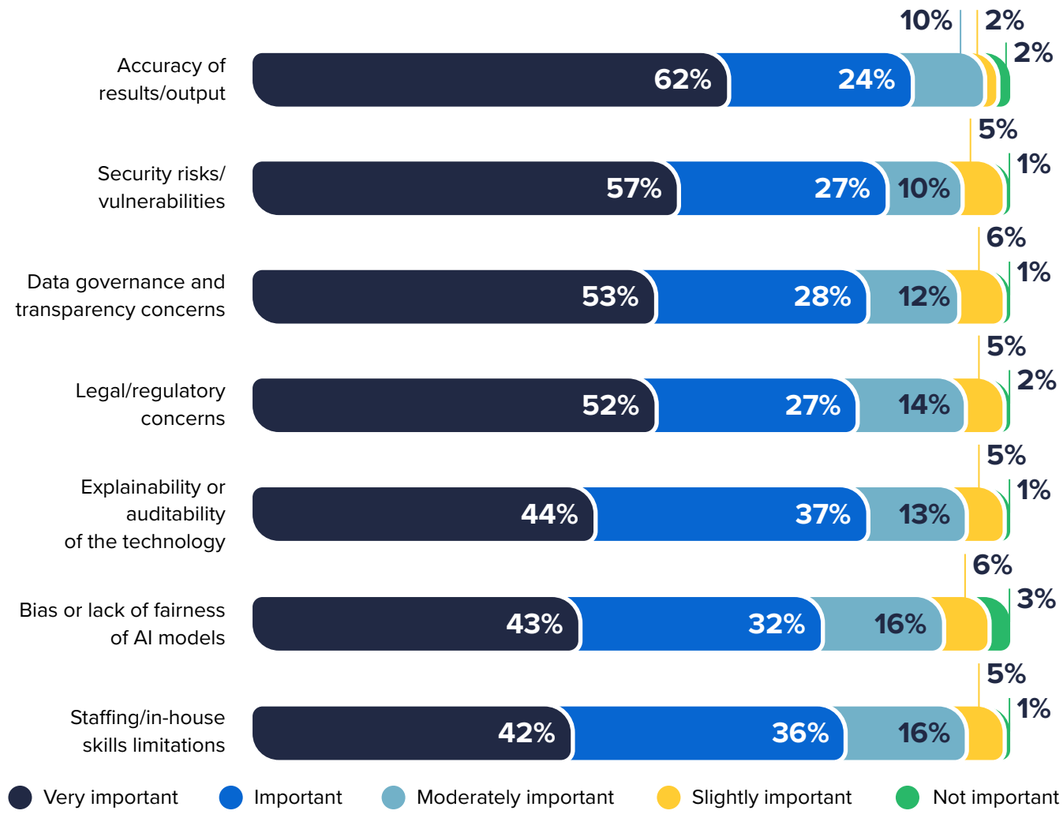
ARTIFICIAL INTELLIGENCE

HOW IMPORTANT ARE DIFFERENT FACTORS WHEN DECIDING WHETHER TO IMPLEMENT GENERATIVE AI AS PART OF AN ANTI-FRAUD PROGRAM?

Since generative AI is one of the fastest-growing technologies and is expected to be adopted by a majority of the organizations in our study (see Figure 8 on page 18), we asked respondents about the importance of different factors for organizations to consider when deciding whether to incorporate this technology into their anti-fraud programs. Several of the factors mirror the challenges featured in Figure 15 on page 30, while others are unique to generative AI.

Each of the factors in Figure 16 were considered important or very important by at least three-fourths of respondents' organizations, with accuracy of results/output (62%) and security risks/vulnerabilities (57%) rated as very important by the most respondents.

FIG. 16 How important are different factors when deciding whether to implement generative AI as part of an anti-fraud program?



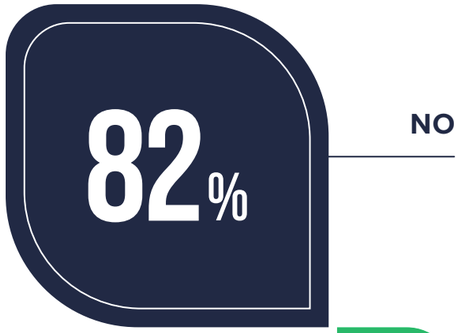
DOES YOUR ORGANIZATION ADDRESS FACTORS RELATED TO AI ADOPTION?

In the interest of adding context to the factors featured in Figure 16 that are especially relevant for AI compared to other technologies, we asked respondents follow-up questions about both bias or lack of fairness in AI models and the explainability of how AI/machine learning models make anti-fraud decisions. Responses to these questions suggest that opportunities exist for many organizations to more effectively address concerns related to bias and explainability of AI models.

As seen in Figure 17, fewer than 1 in 5 organizations (18%) test their AI models for fairness or bias; such testing can reduce the likelihood that these models produce skewed or inaccurate results that cause compliance or liability issues for the organizations that use them.

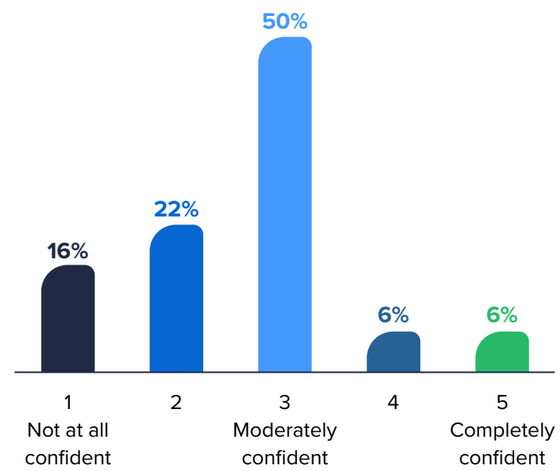
Additionally, any inquiries that organizations face based on the results of their AI models can be complicated or worsened if the organizations are unable to explain how those models arrived at decisions impacting fraud prevention and detection. Our study indicates that confidence in explaining how AI/ML models make anti-fraud decisions. As seen in Figure 18, survey respondents were much more likely to feel not at all confident in their ability to explain how AI/machine learning models make anti-fraud decisions (16%) than they were to feel completely confident (6%), and only 12% of respondents felt more than moderately confident.

FIG. 17 Does your organization test AI fraud models for bias or fairness?



> **There's a growing gap between using AI and governing it. Organizations espouse accuracy as a top priority, but fewer than 1 in 5 organizations test models for bias. This leaves them exposed to significant compliance and reputational risk. Fairness, explainability, and governance must mature alongside fraud detection capabilities or innovation stalls.**
>
> – Stu Bradley,
> Senior Vice President,
> Risk, Fraud and Compliance Solutions, SAS

FIG. 18 How confident are you in your ability to explain how AI/ML models make anti-fraud decisions?



HOW ARE FRAUDSTERS USING AI?

The use of AI to commit fraud schemes has been one of the most prominent themes impacting the fraud risk landscape in recent years. AI tools used by fraudsters to carry out financial crimes range from easily accessible and user-friendly applications to sophisticated, purpose-built tools developed by mature criminal organizations. These tools have allowed fraudsters to enhance and/or automate fraud schemes targeting both organizations and individuals.

To get a sense of how the fraud landscape is being affected by fraudsters' use of AI, we asked respondents about how the volume of common AI-powered fraud schemes has changed over the previous two years, as well as how they expect the volume to change over the next two years. We also asked respondents to rate their organization's readiness to detect and prevent such schemes.

More than 50% of respondents indicated that each of the noted schemes has increased over the previous two years (see Figure 19), and at least two-thirds expect these schemes to increase over the next two years (see Figure 21). The AI-powered schemes most commonly cited as having increased significantly included deepfake social engineering (44%) and consumer fraud/scams (38%), while the schemes the most respondents expect to increase significantly in the future include generative AI document fraud/forgery (55%), deepfake social engineering (55%), and deepfake digital injection (54%).

Given that only 7% of respondents believe their organization is more than moderately prepared to detect and prevent AI-powered fraud (see Figure 20), addressing these fraud risks will be an important objective in the anti-fraud profession for years to come.

FIG. 19 How has the volume of the following types of AI-powered fraud schemes changed over the previous two years?

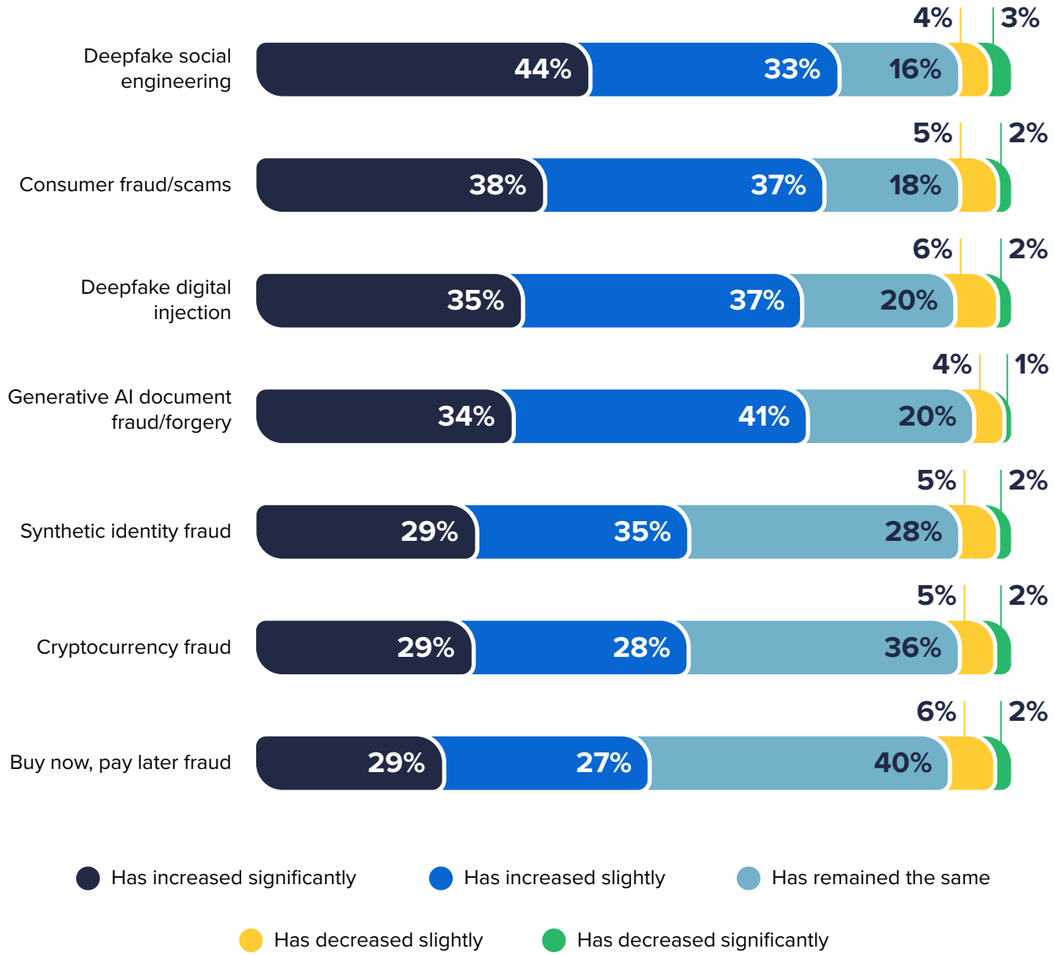


FIG. 20 How prepared do you believe your organization is to detect and/or prevent AI-powered fraud?

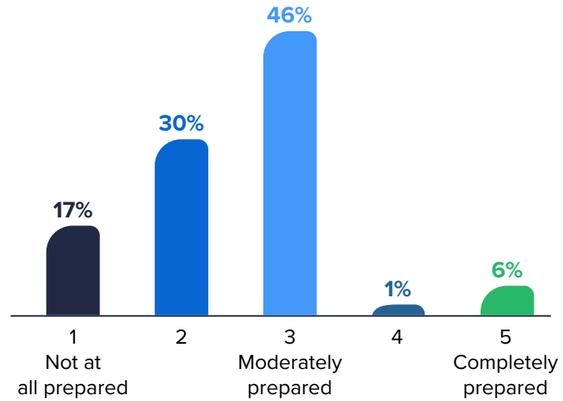
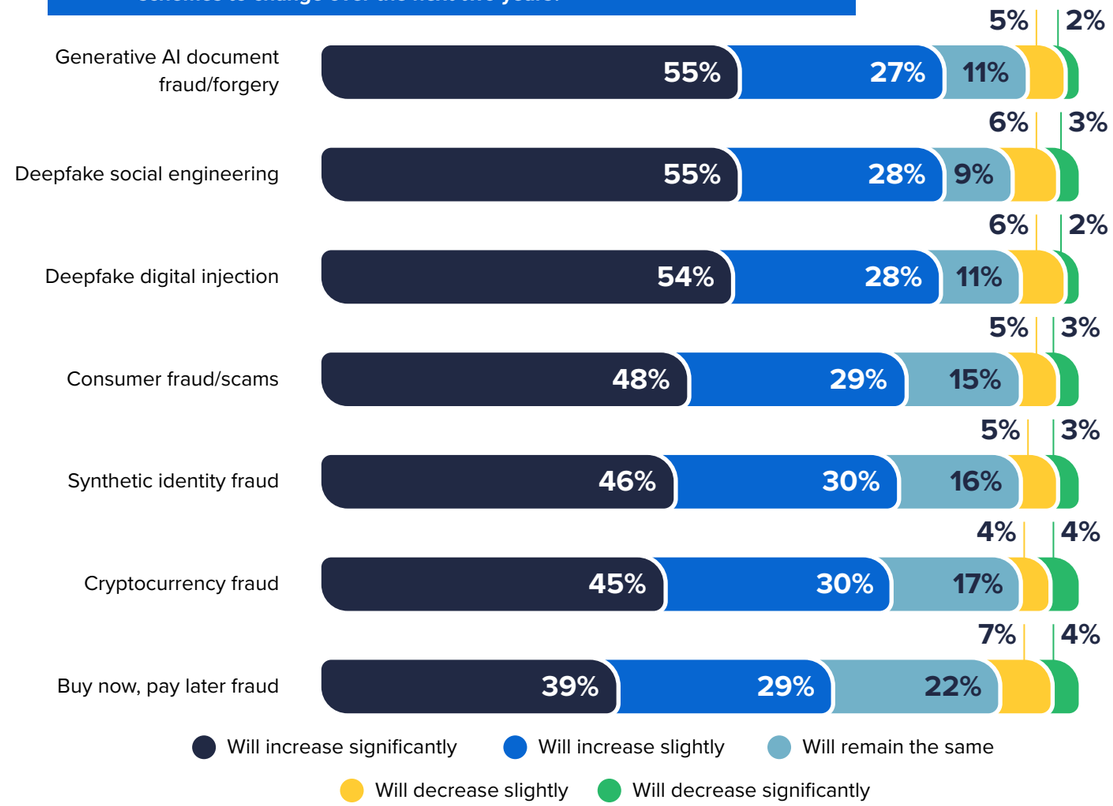


FIG. 21 How do you expect the volume of the following types of AI-powered fraud schemes to change over the next two years?



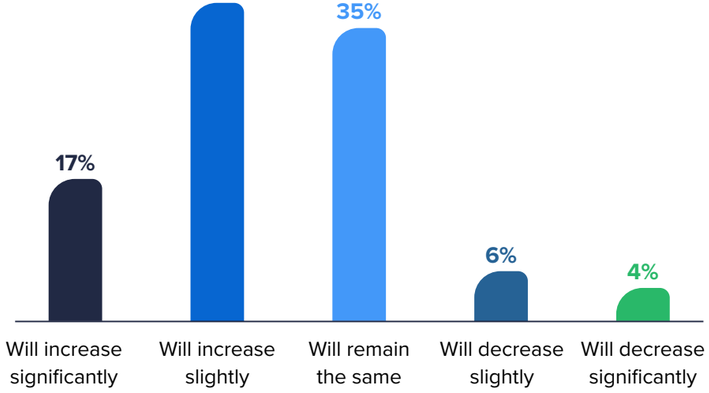
HOW ARE ORGANIZATIONS' ANTI-FRAUD TECHNOLOGY BUDGETS EXPECTED TO CHANGE IN THE NEXT TWO YEARS?

HOW ARE ORGANIZATIONS' ANTI-FRAUD TECHNOLOGY BUDGETS EXPECTED TO CHANGE IN THE NEXT TWO YEARS?

More than half of respondents (55%) indicated that they expect their organization's budget for anti-fraud technology to increase in the next two years, with 17% saying that increase would be significant. This finding is comparable to the results in our 2024 study, when 59% of respondents expected their organization's budget to increase, and 18% expected that increase to be significant.

These budget expectations are particularly interesting when considering that 83% of respondents noted budget and financial concerns as a major or moderate challenge when implementing new anti-fraud technologies at their organizations (see Figure 22). On the other end of the spectrum, 10% of respondents expect to see a budget decrease for anti-fraud technology, with 4% anticipating a significant reduction in funds available for these tools.

FIG. 22 How are organizations' anti-fraud technology budgets expected to change in the next two years?

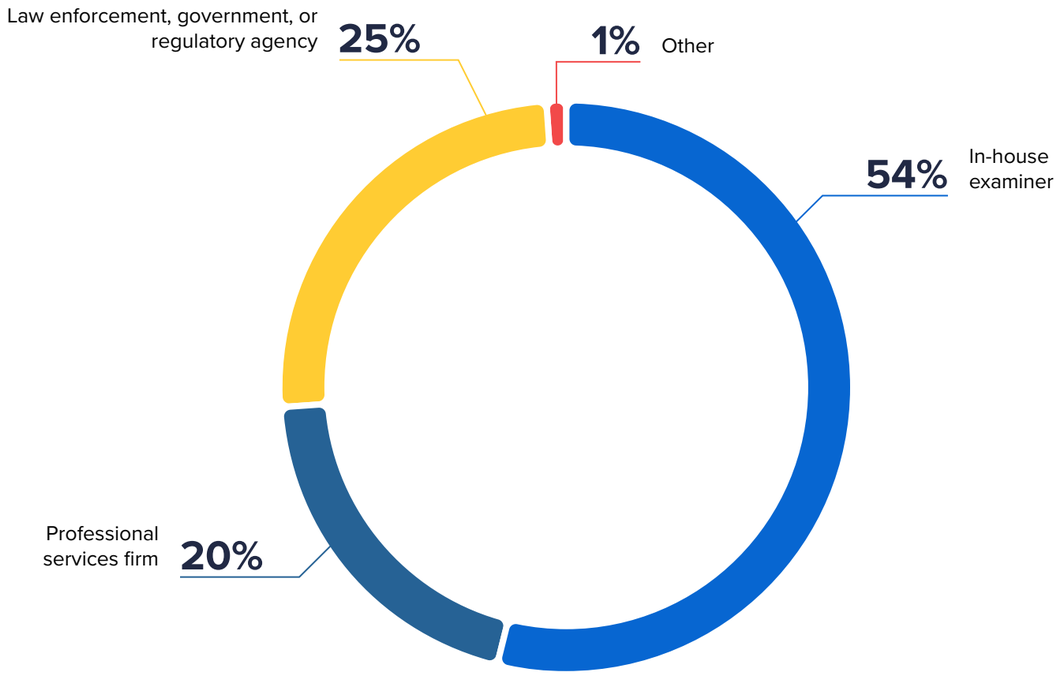


RESPONDENT DEMOGRAPHICS

RESPONDENTS' PROFESSIONAL ROLE

As shown in Figure 23, 54% of respondents in our study work in-house and conduct anti-fraud activities (e.g., investigations, prevention, detection, risk management, compliance) within a single organization. Another quarter (25%) work for a government, regulatory, or law enforcement agency, and conduct fraud-related engagements involving outside parties under the authority of that agency, and 20% work for a professional services firm that conducts anti-fraud engagements on behalf of other organizations.

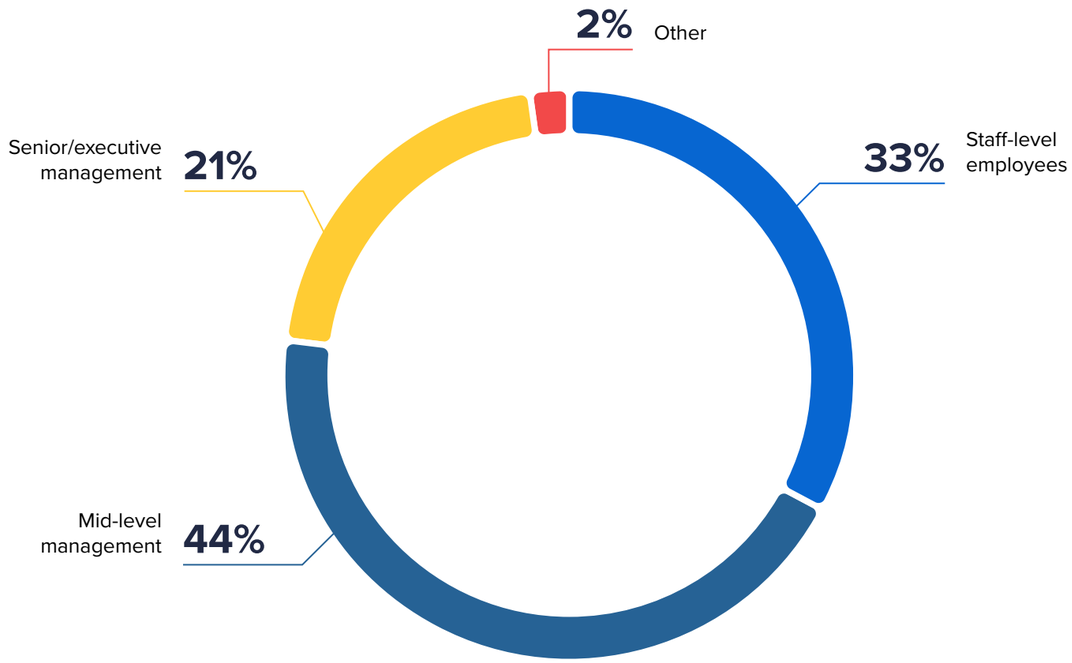
FIG. 23 Respondents' professional role



RESPONDENTS' POSITION LEVEL

More than 60% of respondents are in a management-level position, with 21% at the senior/executive level and 44% at the middle management level. Additionally, one-third are staff-level employees. (See Figure 24.)

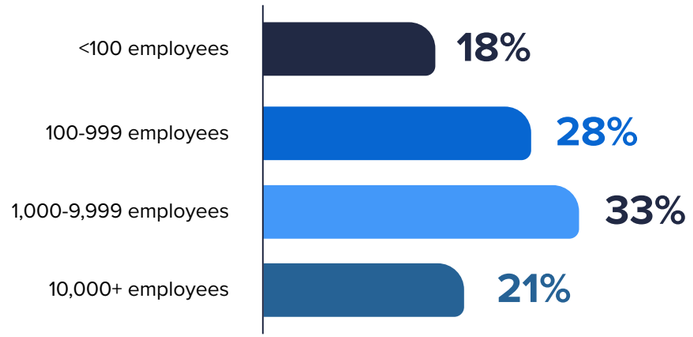
FIG. 24 Respondents' position level



SIZE OF RESPONDENTS' ORGANIZATIONS

Figure 25 reflects the size of the organizations that respondents work for; the greatest percentage (33%) work for companies with between 1,000 and 9,999 employees, followed by companies with 100 to 999 employees (28%).

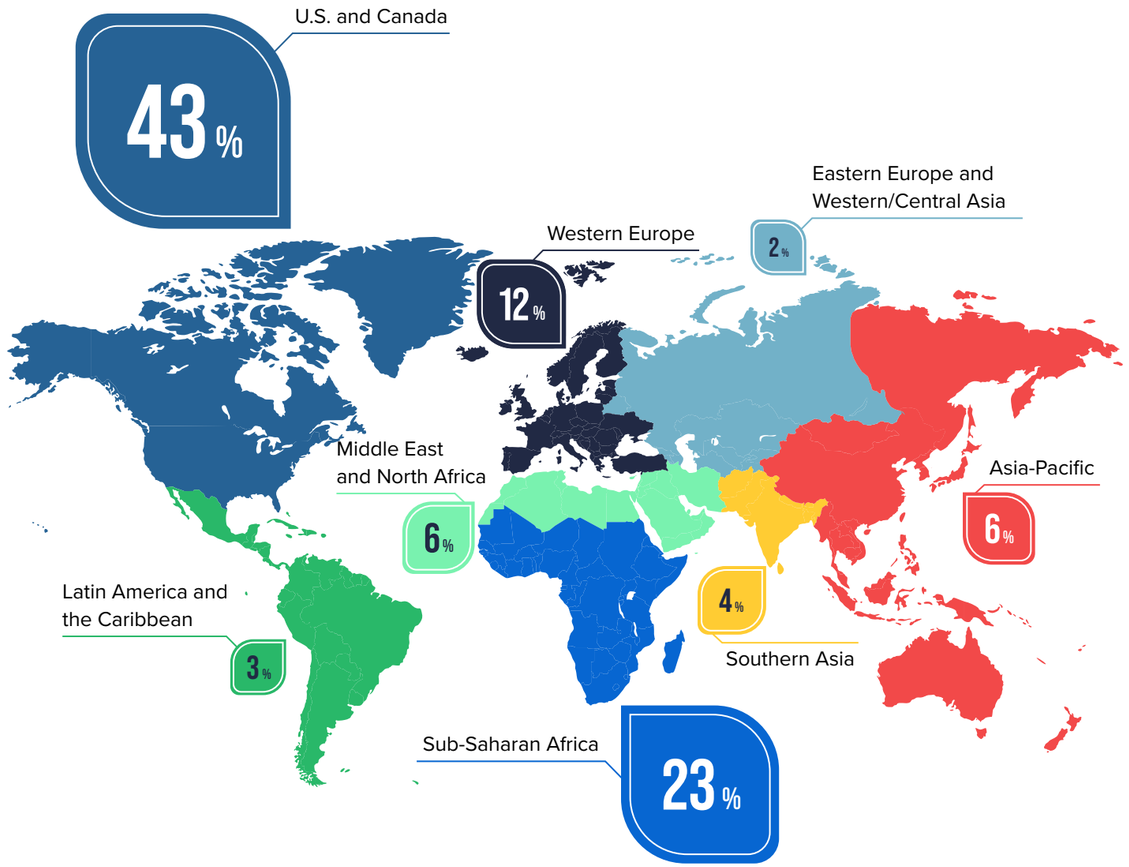
FIG. 25 Size of respondents' organizations



REGION OF RESPONDENTS' ORGANIZATIONS

As noted in Figure 26, the respondents in our study were distributed geographically, providing us with a global view into the current and anticipated future state of anti-fraud technology. The region with the largest percentage of respondents was the U.S. and Canada (43%), followed by Sub-Saharan Africa (23%), and Western Europe (12%).

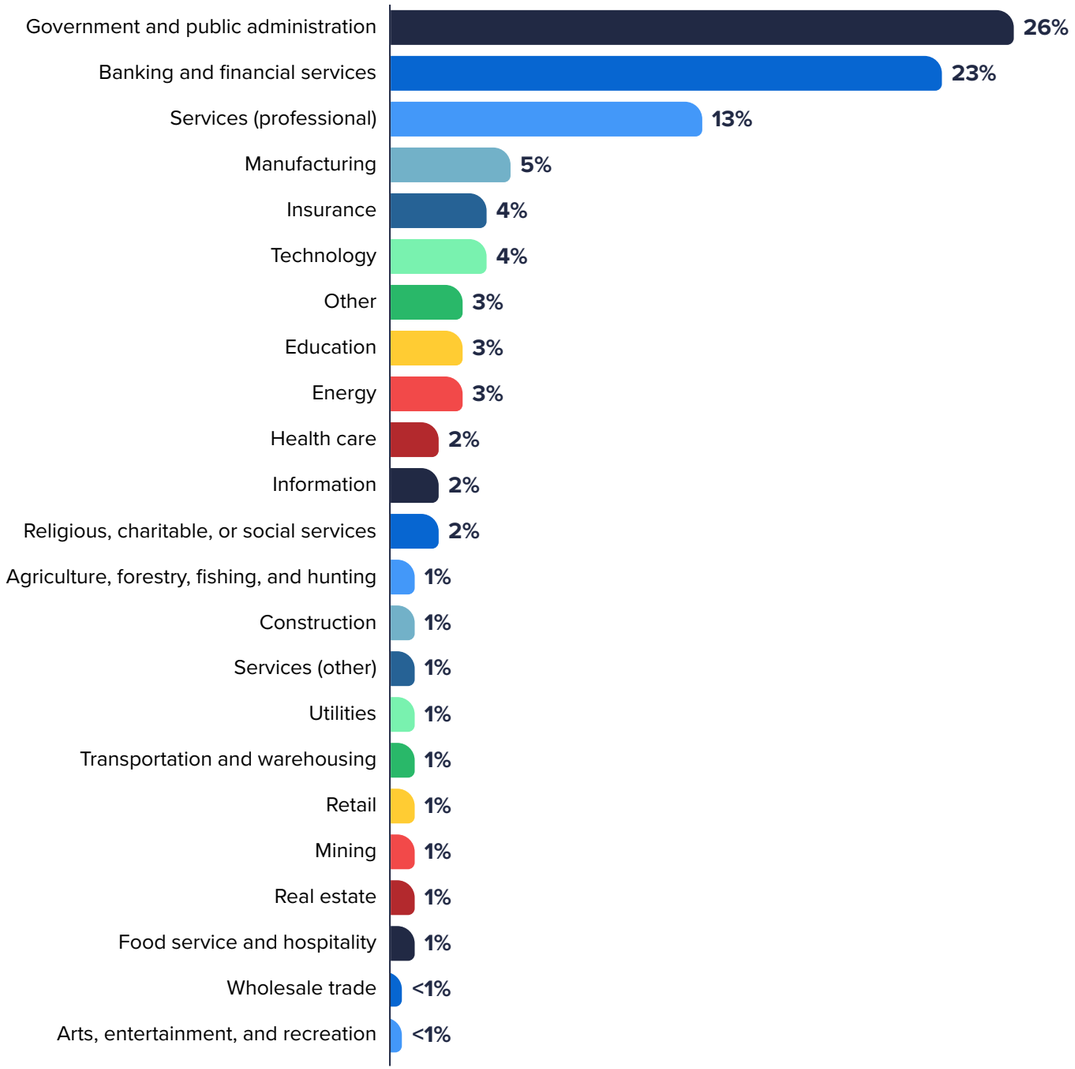
FIG. 26 Region of respondents' organizations



INDUSTRY OF RESPONDENTS' ORGANIZATIONS

The two industries most commonly represented by respondents in our study were government and public administration (26%) and banking and financial services (23%). The remaining 51% of responses were spread out across all other industries, as shown in Figure 27.

FIG. 27 Industry of respondents' organizations



ABOUT THE ACFE

Founded in 1988 by Dr. Joseph T. Wells, CFE, CPA, the Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 95,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession.

The ACFE unites and supports the global anti-fraud community by providing educational tools and practical solutions for professionals through events, publications, networking, and educational materials for colleges and universities. The ACFE offers its members the opportunity for professional certification. The Certified Fraud Examiner (CFE) credential is preferred by businesses and government entities around the world and indicates expertise in fraud prevention and detection.

Learn more at ACFE.com.

ABOUT SAS

SAS is a global leader in data and AI. SAS helps organizations transform data into trusted decisions faster by providing knowledge in the moments that matter. And in a digital world where fighting fraud and financial crimes grows more complex by the day, SAS delivers the most powerful fraud, anti-money laundering and security intelligence solutions to keep you ahead. That's why 90% of Fortune 100 companies trust SAS to solve their toughest challenges with greater speed, scale and efficiency. SAS gives you THE POWER TO KNOW®.

Learn more about SAS.

ACFE
Association of Certified Fraud Examiners

sas