

# 2024 ANTI-FRAUD TECHNOLOGY BENCHMARKING REPORT

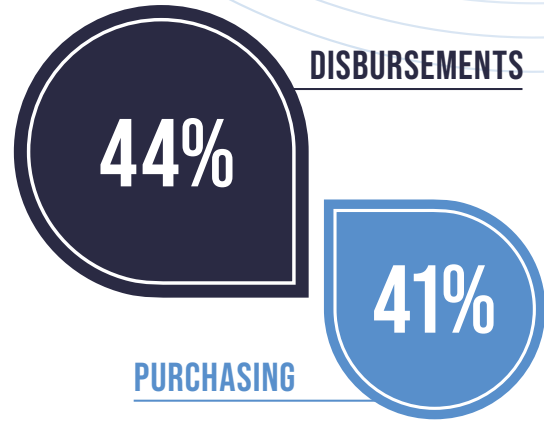


# TABLE OF CONTENTS

Key Findings.....	<b>3</b>
Introduction.....	<b>5</b>
Methodology.....	<b>5</b>
How Are Organizations Using Data Analytics in Their Anti-Fraud Initiatives? .....	<b>6</b>
What Other Technologies Are Organizations Using in Their Anti-Fraud Initiatives?.....	<b>14</b>
What Challenges Do Organizations Face in Implementing New Anti-Fraud Technology?.....	<b>21</b>
How Is Generative AI Affecting Organizations' Anti-Fraud Programs? .....	<b>24</b>
How Are Organizations' Anti-Fraud Technology Budgets Expected to Change in the Next Two Years?.....	<b>27</b>
Respondent Demographics.....	<b>29</b>

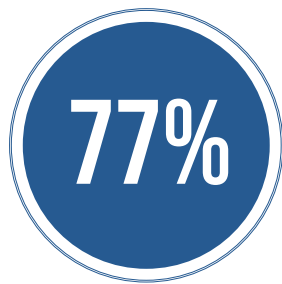


Nine in 10 organizations (91%) use **DATA ANALYSIS TECHNIQUES** as part of their anti-fraud programs.



The most common risk areas monitored by data analytics are

**DISBURSEMENTS (44%)** and **PURCHASING (41%)**.

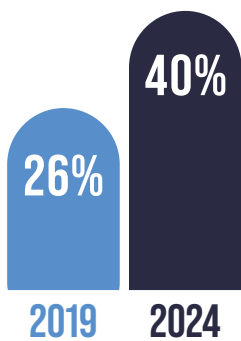


**INTERNAL STRUCTURED DATA**

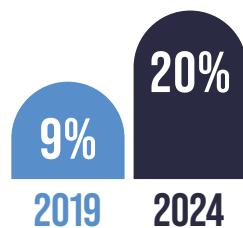
is the most common source of data for analysis, with 77% of organizations relying on this traditional approach.

The use of both **BIOMETRICS and ROBOTICS** in anti-fraud programs has steadily increased over the past few years.

**BIOMETRICS**



**ROBOTICS**



**Two in five organizations (40%)** currently use

**PHYSICAL BIOMETRICS**

as part of their anti-fraud program, and **another 17% expect to adopt this technology** in the next two years.



## THE USE OF ARTIFICIAL INTELLIGENCE (AI) and MACHINE LEARNING

in anti-fraud programs is expected to nearly

# TRIPLE

over the next two years.



# 83%

of organizations expect to implement **GENERATIVE AI** as part of their anti-fraud programs over the next two years.

A majority of organizations (**61%**) either currently contribute or are willing to **contribute to data consortiums** to aid their anti-fraud efforts.

# 61%

OF ORGANIZATIONS

Three in five organizations (**59%**) expect to **increase their budgets for anti-fraud technology** over the next two years.

# 59%

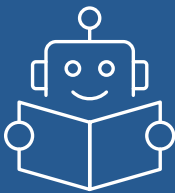
OF ORGANIZATIONS

# 82%

## BUDGET OR FINANCIAL RESTRICTIONS



are a top concern when implementing new anti-fraud technology, presenting a major or moderate challenge to **82%** of organizations.



## MORE THAN 50% OF ANTI-FRAUD PROGRAMS

currently use or expect to adopt computer vision analysis, robotics, and behavioral biometrics at some point in the future.

## INTRODUCTION


In 2024, using technology as part of an anti-fraud program is a necessity. Fraud perpetrators continually seek ways to exploit technological developments and human weaknesses to accomplish their schemes. Organizations must employ the most effective tools to guard against these threats, and that often means implementing new programs and training staff to effectively use them.

To understand how organizations are approaching this mission, the ACFE and SAS have partnered to conduct a series of studies on the use of anti-fraud technologies by organizations around the world. As a follow-up to our first two reports released in 2019 and 2022, our latest report explores trends in the current and expected adoption of traditional analytics, artificial intelligence (AI) and generative AI, case management tools, biometrics, and a host of other technologies that can be used to combat fraud. It is our hope that anti-fraud professionals, organizational management, and others find the information herein to be beneficial in benchmarking and assessing the effectiveness of their anti-fraud technology toolkits and planning for future technology-related budgets and resources.

## METHODOLOGY

In October 2023, we sent a 22-question survey to 80,426 ACFE members. Respondents were asked to provide information about their organizations' use of various technologies as part of their anti-fraud initiatives. Survey responses were collected anonymously. We received 1,187 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 29.)

The 2024 *Anti-Fraud Technology Benchmarking Report* was developed in partnership with SAS. As part of their support for this project, SAS offers complimentary access to a SAS Visual Analytics report where you can further explore the survey results with interactive charts based on various demographic categories, including industry and geographic region. View the SAS Visual Analytics report at [SAS.com/fraudsurvey](https://sas.com/fraudsurvey).



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

## WHAT DATA ANALYSIS TECHNIQUES DO ORGANIZATIONS USE TO FIGHT FRAUD?

The ability to effectively analyze data for warning signs of fraud is a crucial tool in an organization's fraud-fighting toolkit. More than 90% of organizations in our study use some form of data analysis as part of their anti-fraud program. As noted in Figure 1, the most common uses of fraud analytics are exception reporting and anomaly detection (57% of organizations) and automated red flags and business rules monitoring (54% of organizations).

In addition, every technique we asked about is expected to be adopted by more organizations in the next one to two years. Artificial intelligence (AI) and machine learning have the greatest anticipated adoption rate, with nearly one-third of organizations that do not currently use the technology expecting to add it to their anti-fraud program in the near future. This means that by 2026, half of all organizations expect to use AI

and machine learning as part of their fraud analytics initiatives. Furthermore, the expected adoption rate of AI and machine learning has increased since our prior study, which shows a growing momentum around these tools; in 2022, 26% of organizations expected to adopt this technology over the next two years, while 32% of organizations in our current study are planning to implement AI and machine learning in the near future. The use of predictive analytics and modeling is also expected to rise notably, with 22% of organizations planning to adopt this technology over the next two years.

However, despite the expected increase in the use of every data analysis technique in our study, reported adoption rates have shown little growth since 2019, highlighting the slow pace at which organizations are able to implement new technologies.

### THE USE OF ARTIFICIAL INTELLIGENCE and MACHINE LEARNING

in anti-fraud programs is expected to nearly **TRIPLE** over the next two years.



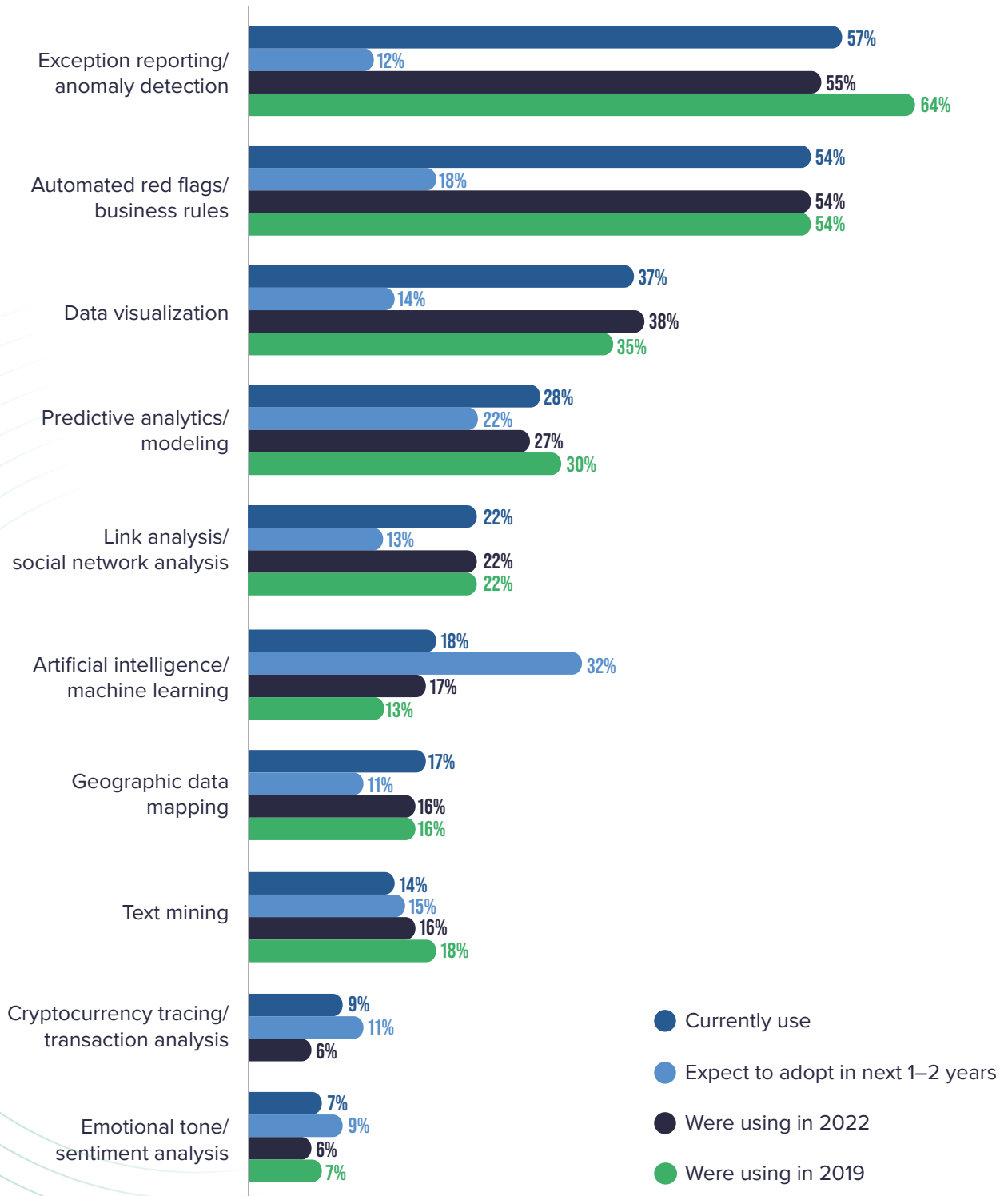
**3x**

“

**Automated red flags, machine learning, and predictive analytics can be useful these days due to the high volume of cyberattacks and the increased use of technology by criminals.”**

– Survey respondent

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





As organizations navigate implementing and improving their analytics programs, it can be helpful to see which tools others are using for various purposes. Figure 2 shows the most common programs for each of the analytics techniques in our study. In all categories, a significant portion of respondents noted that their organization uses a proprietary, in-house platform to perform the noted analytics technique.

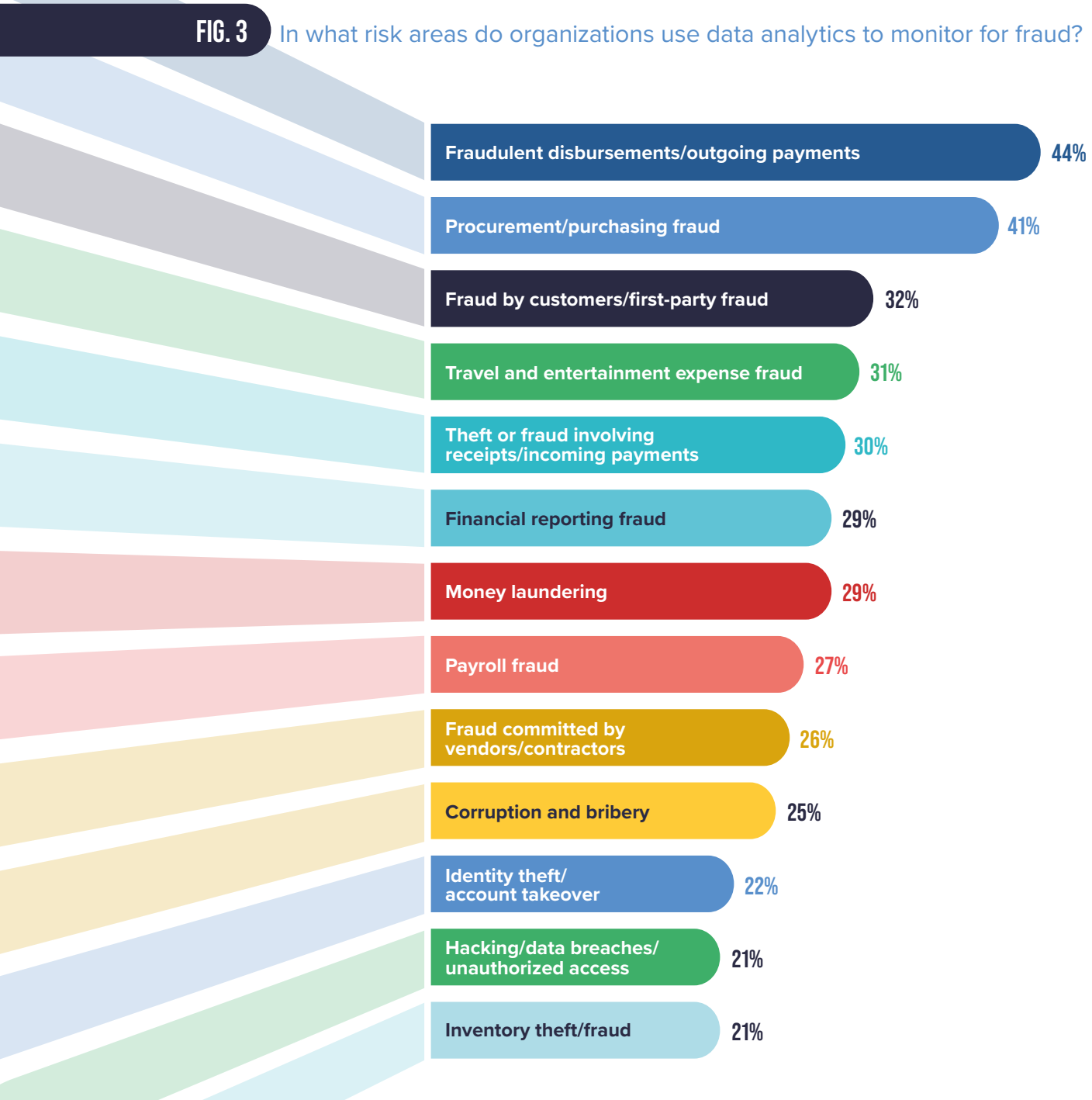
**FIG. 2** What are the most commonly used programs for each analytic technique?



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

To ensure data analytics are used as effectively and efficiently as possible, many organizations apply a risk-based approach, focusing their analytics initiatives on detecting potential fraud in specific risk areas within the company. Figure 3 shows that outgoing payments and disbursements is the area most commonly monitored using analytics (44% of organizations), followed closely by the procurement and purchasing function (41% of organizations).

**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?

Data containing red flags or evidence of fraud can exist in numerous places, both inside and outside the organization. We asked survey respondents which of several types of data they use as data sources for their anti-fraud analytics. As shown in Figure 4, the most common data source is internal structured data (77% of organizations), which is data that is formatted in recognizable and predictable structures, such as that found in databases and spreadsheets. In contrast, internal unstructured data—data that is found outside of structured formats, such as text documents, emails, and image files—is only used by 33% of organizations, and data from devices connected to the organization’s network is only used by 25%. Public records are the most common form of external data

used (40% of organizations), followed by government watch lists (31% of organizations).

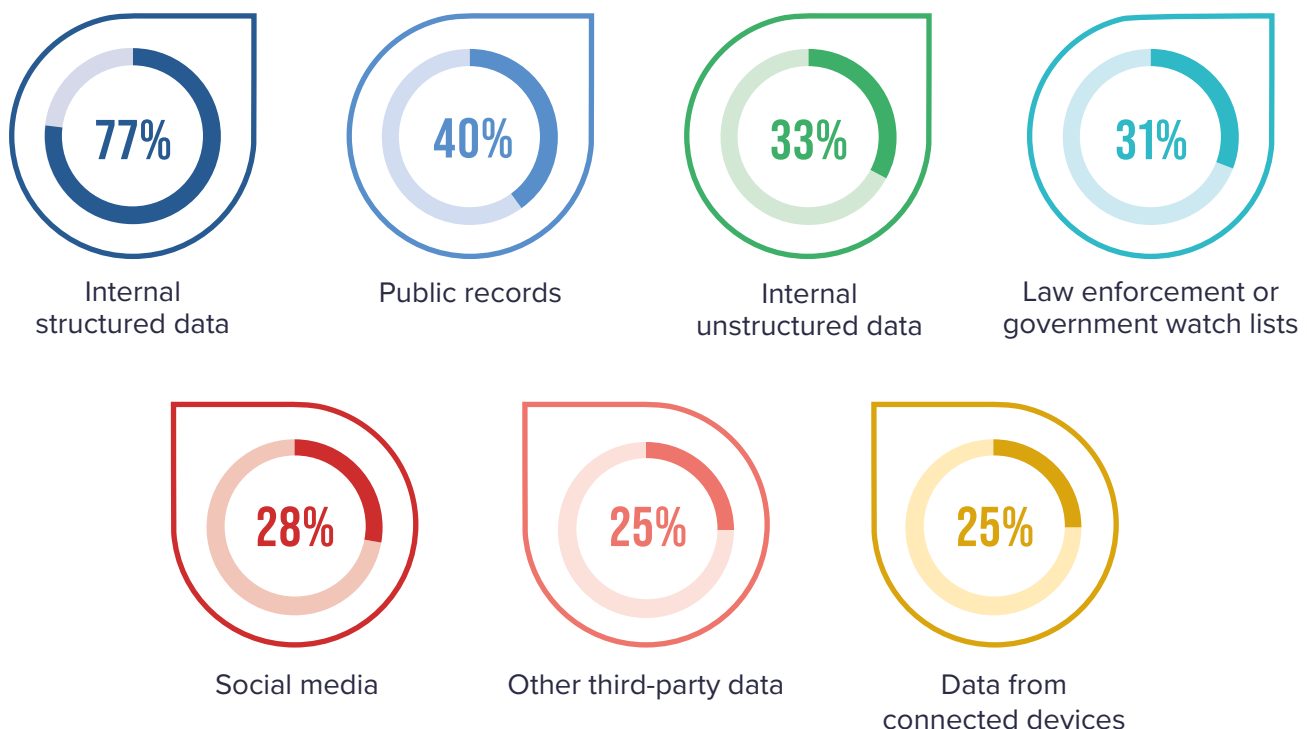
Additionally, analyzing data from multiple sources can provide valuable insight and evidence that might not be recognized by looking at only one data source. Of the organizations in our study, 62% currently use data from more than one source as part of their anti-fraud analytics, and 51% incorporate 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?

With more than 90% of organizations using some form of data analytics as part of their anti-fraud programs, it's clear the overall value of these initiatives is widely accepted. To provide further insight into the specific benefits provided by fraud analytics, we asked survey participants how their data analysis efforts affected four specific 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

Figure 5 shows that the increase in volume of transactions reviewed and potential frauds detected is the most realized benefit, with 93% of respondents indicating this to be either very or fairly beneficial. Similarly, 89% noted the increased efficiency as very or fairly beneficial, and 87% said the additional timeliness is very or fairly beneficial to their organization.



**Data analytics helps to enrich anti-fraud results/ reports. It not only reduces turnaround time, it [also] helps investigators to focus on very important aspects of the investigation.”**

– Survey respondent

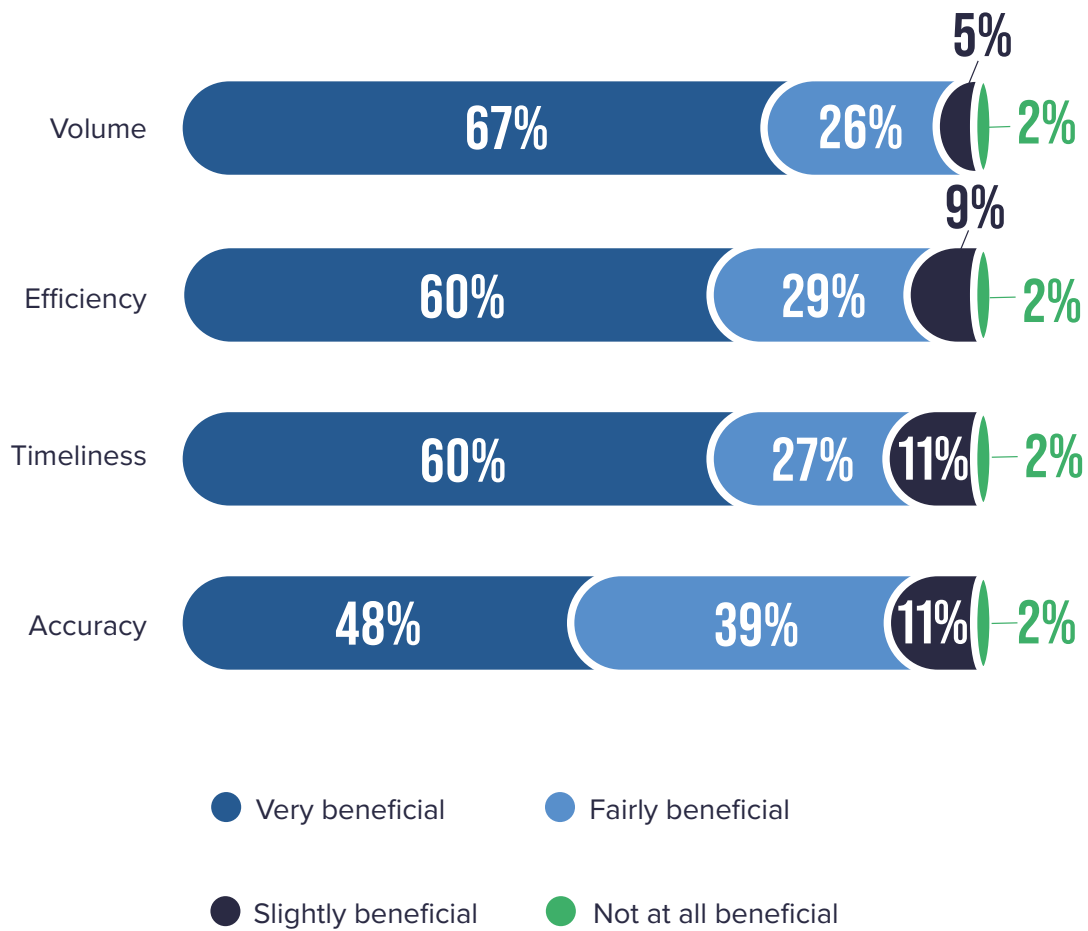


**Data is only as good as what is put in. Many times, fraud is related to what is not put into the system (missing data).”**

– Survey respondent

FIG. 5

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



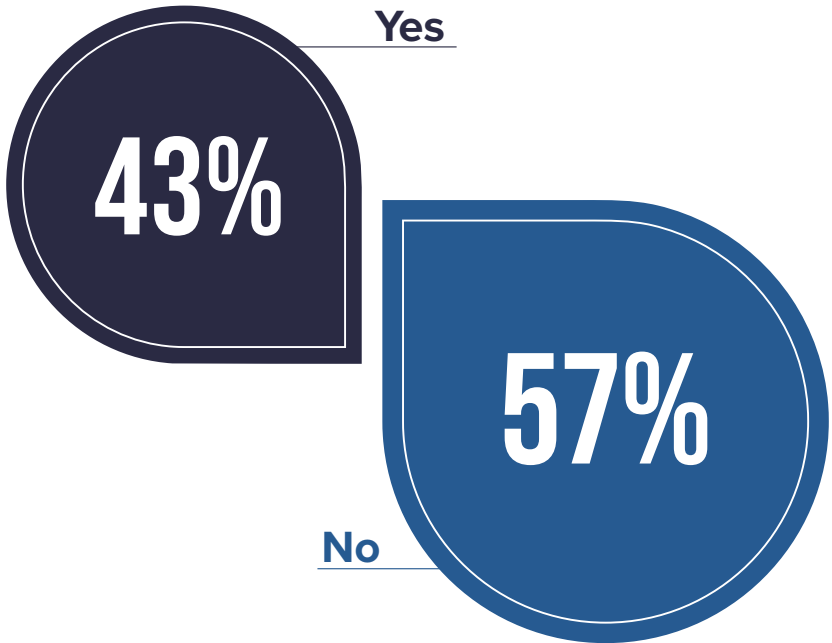


# WHAT OTHER TECHNOLOGIES ARE ORGANIZATIONS USING IN THEIR ANTI-FRAUD INITIATIVES?

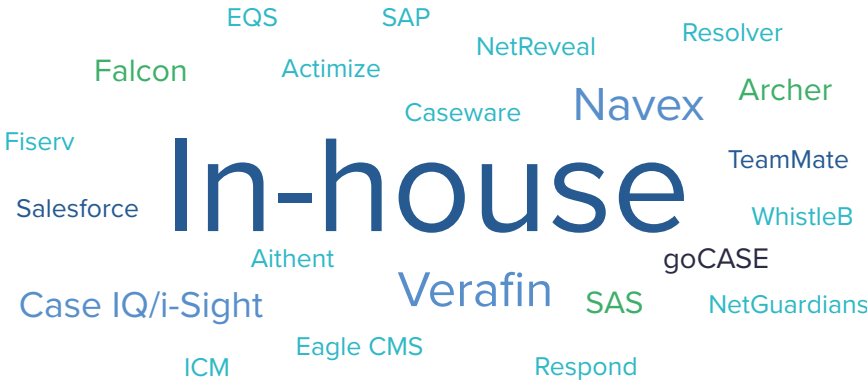
## ARE ORGANIZATIONS USING CASE MANAGEMENT SOFTWARE?

When assessing or investigating potential fraud, case management software can make documenting the response and organizing the related information more effective and efficient. However, 57% of respondents to our survey indicated that their organizations do not use this type of tool as part of their anti-fraud programs. Among the 43% of organizations that do utilize a case management system, in-house or proprietary platforms are the most common type of software used.

**FIG. 6** Are organizations using case management software?



**FIG. 7** What are the most common case management software programs?\*

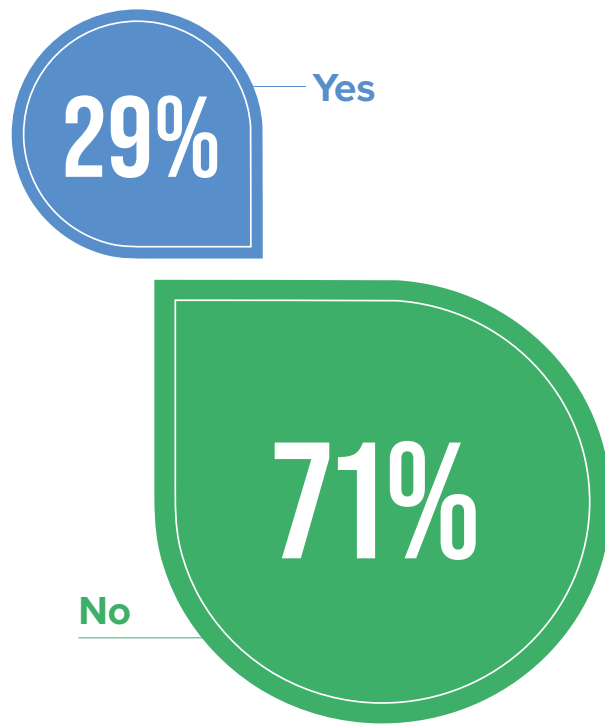


\* Text size is relative to frequency of responses (i.e., larger text indicates more responses, and smaller text indicates fewer responses).

## ARE ORGANIZATIONS USING DIGITAL FORENSICS/E-DISCOVERY SOFTWARE?

Electronic forms of evidence, including digital files and data, can play a significant role in fraud investigations. The use of digital forensics and e-discovery software programs can provide numerous benefits when obtaining and managing this type of evidence. However, more than 70% of respondents indicated that their organizations' anti-fraud programs do not include the use of any formal digital forensics or e-discovery software platform. For the 29% of respondents whose organizations do use this type of software, the most commonly used program is EnCase, followed by Cellebrite and Relativity.

**FIG. 8** Are organizations using digital forensics/e-discovery software?



**FIG. 9** What are the most common digital forensics/e-discovery software programs?\*



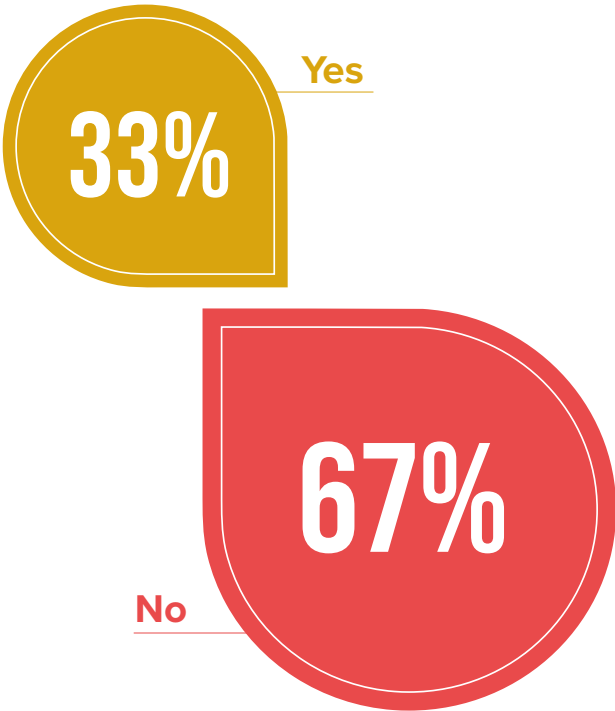
\* Text size is relative to frequency of responses (i.e., larger text indicates more responses, and smaller text indicates fewer responses).



## ARE ORGANIZATIONS USING ONLINE-EVIDENCE CAPTURING SOFTWARE?

Digital evidence relevant to fraud investigations is also regularly obtained from online sources, and organizations can employ online-evidence capturing software to collect and preserve this evidence. As shown in Figure 10, more than two-thirds of respondents' organizations do not currently incorporate online-evidence capturing software in their anti-fraud programs. Of the 33% of organizations that do have such software in place, in-house or proprietary programs are the most commonly used by a significant margin.

**FIG. 10** Are organizations using online-evidence capturing software?



**FIG. 11** What are the most common online-evidence capturing software programs?\*



\* Text size is relative to frequency of responses (i.e., larger text indicates more responses, and smaller text indicates fewer responses).

## WHAT EMERGING TECHNOLOGIES ARE ORGANIZATIONS USING TO FIGHT FRAUD?

As new classes of technology that support fraud investigation, detection, and prevention emerge, many organizations evaluate the potential benefits those technologies can provide for their anti-fraud programs. We asked survey respondents which categories of emerging technologies they either currently use in their anti-fraud program or expect to incorporate in the future.

As illustrated in Figure 12, 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; 40% of respondents noted that their organization currently employs physical biometrics, with another 17% expecting to adopt this technology in the near future. While the current use of physical biometrics is twice as common as computer vision analysis

(20%), robotics (20%), and behavioral biometrics (20%), all four of these technologies are either in use now or expected to be used by more than 50% of respondent organizations at some point in the future. Conversely, more than half of respondents indicated that they do not expect their organizations to ever use blockchain/distributed ledger technology or virtual/augmented reality as part of their anti-fraud programs.

Additionally, our studies have shown a steady increase in the use of both biometrics and robotics as part of anti-fraud programs over the past several years. In 2019, only 26% of organizations were using any form of biometrics in their programs, while 40% of organizations in our current study use physical biometrics alone. Likewise, the use of robotics to fight fraud has grown from 9% of organizations in 2019 to 20% in this year's study.

“

**Emerging technologies in anti-fraud initiatives will provide organizations with the necessary resources and tools to identify trends and indications of fraud with more efficiency and effectiveness.”**

– Survey respondent

“

**Not everything is relevant to every organization. It's important to know what the best and most relevant technology is for the organization.”**

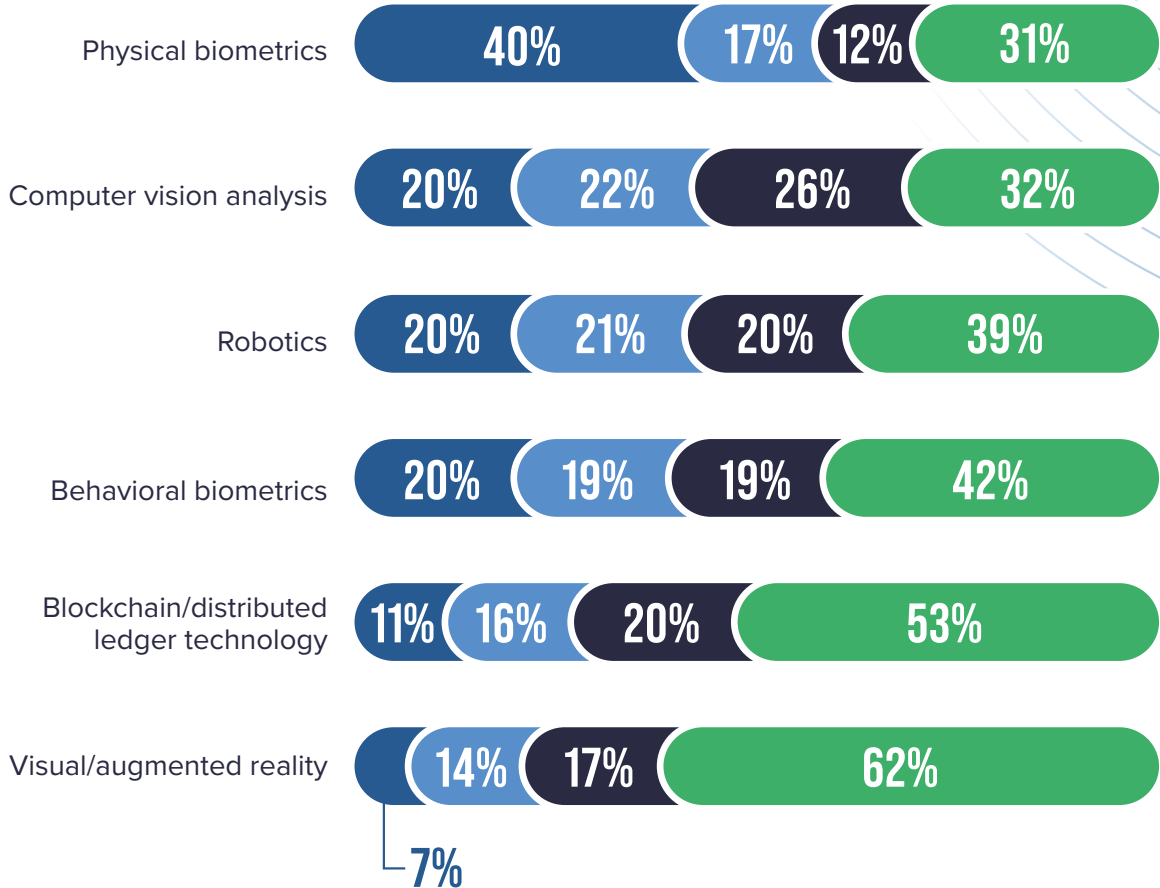
– Survey respondent

“

**While there is still some refinement to be done with respect to the applicability of emerging technologies in anti-fraud initiatives, investigators cannot afford to overlook their importance.”**

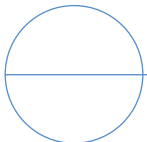
– Survey respondent

FIG. 12 What emerging technologies are organizations using to fight fraud?



● Currently use    ● Do not currently use, but expect to deploy in the next 1–2 years

● Do not currently use, but expect to deploy more than 2 years from now    ● Do not expect to use



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

While many organizations derive insights from their own data that can bolster their fraud prevention or detection efforts, these insights can be limited by the scope of the internal data available. Data-sharing consortiums pool data from multiple organizations, generally within the same industry, to be analyzed for trends and patterns related to potential fraudulent activity that can then be leveraged in the participating organizations' anti-fraud programs. The ability to access similar organizations' data can potentially improve analysis and monitoring results due to the larger sample size.

As shown in Figure 13, 61% of respondent organizations indicated that they either currently contribute to a data-sharing consortium (35%) or would be willing to in the future (26%). In addition, the percentage of organizations who are not planning to participate in a consortium has fallen steadily over the last several years, illustrating an increased recognition of the value of collaboration and data sharing as part of the fight against fraud.

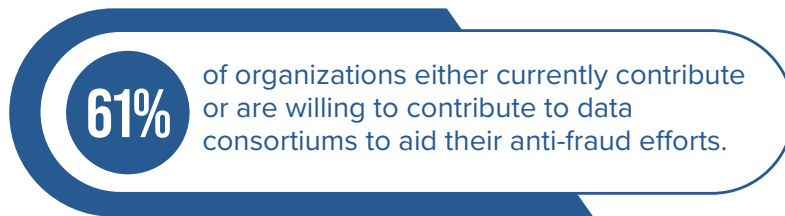
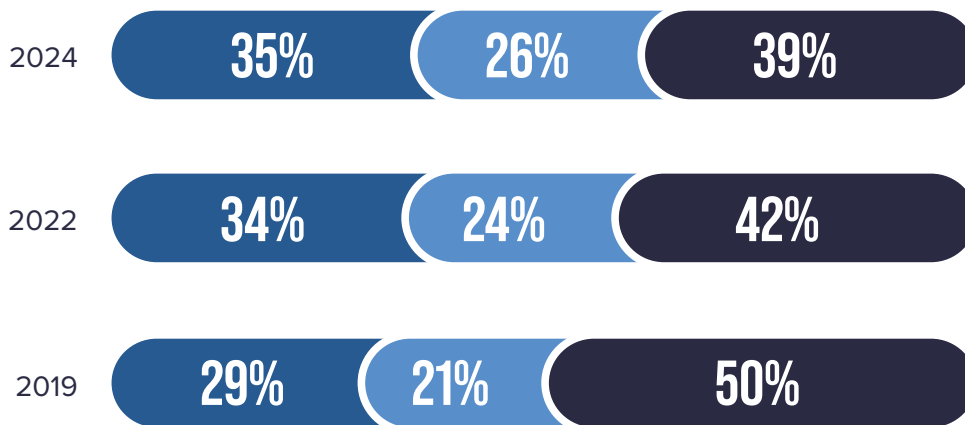


FIG. 13

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



● Currently contribute

● Do not currently contribute, but would be willing to contribute in the future

● Do not contribute and have no plans to do so



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

The implementation of new technology is not without challenges that can impact how effective the technology is for anti-fraud applications. We asked respondents about several factors that can complicate the onboarding of new technological solutions to determine how much of a challenge each represents. Each of the eight factors presents at least

a minor challenge to 80% or more of respondent organizations. Budget/financial restrictions are the most significant barrier, presenting a major or moderate challenge to 82% of respondents. Other top-cited challenges include poor data quality or integration and limitations in staffing and in-house skills relevant to the technology.



**Organizational silos with multiple fraud teams trying to find solutions—this is improving, and centralization of fraud strategy is underway, but it is very challenging. Onboarding new technologies in a timely manner to stay ahead of fraud is a challenge.”**

– Survey respondent



**Another challenge of implementing new anti-fraud technology within an organization is ensuring there is a collaborative effort that maximizes resources and ROI.”**

– Survey respondent

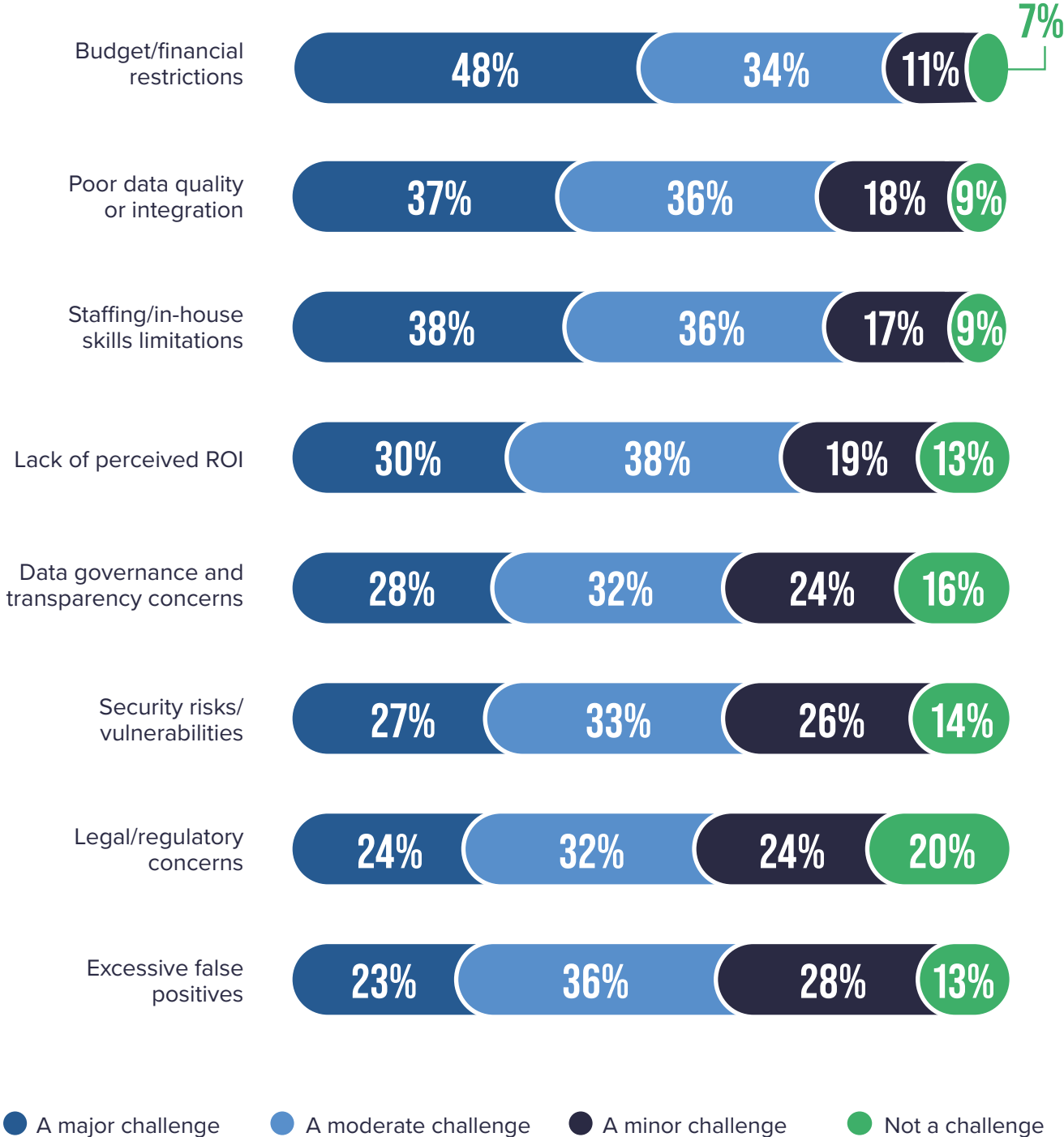


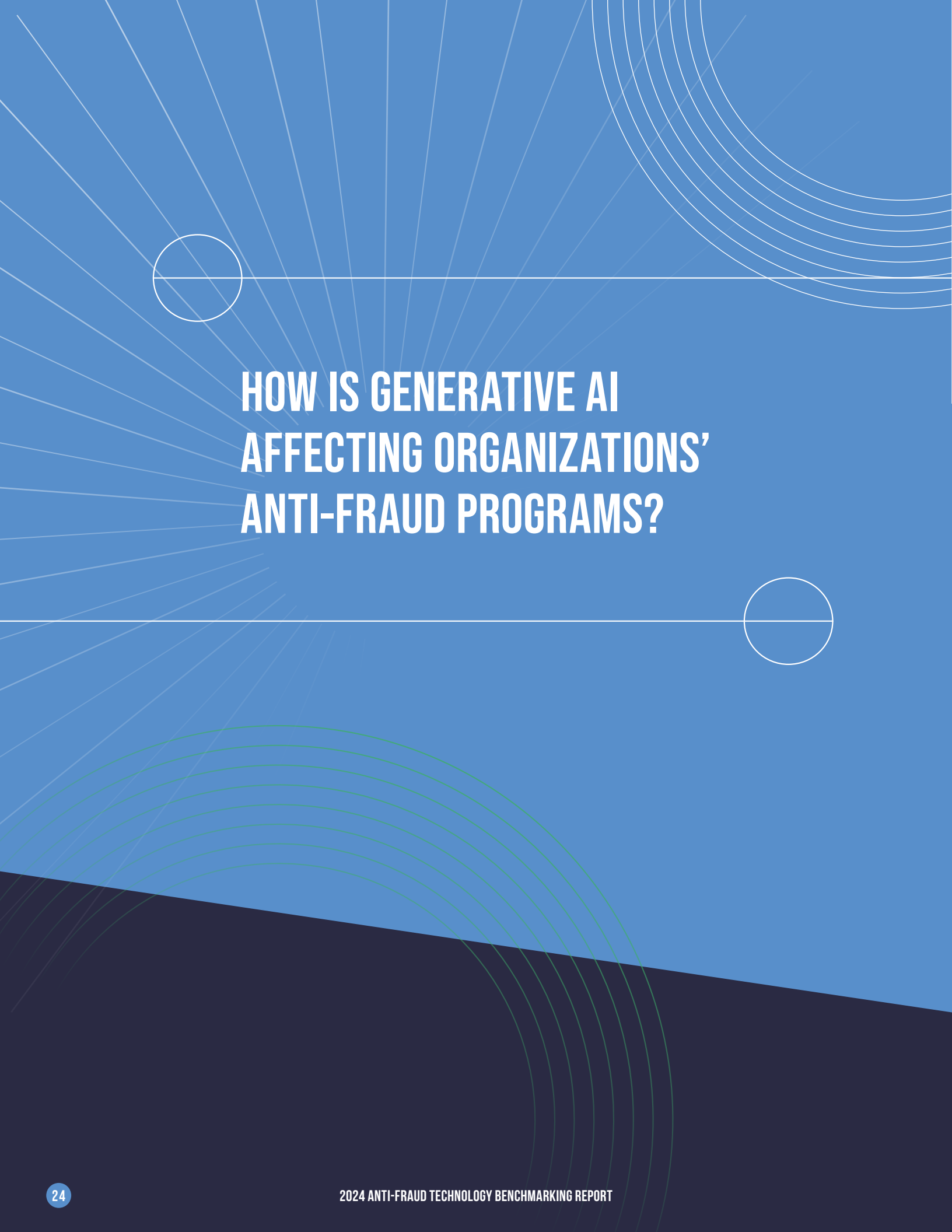
82%

## BUDGET OR FINANCIAL RESTRICTIONS

are a top concern when implementing new anti-fraud technology, as they present a major or moderate challenge to **82%** of organizations.

FIG. 14 What challenges do organizations face in implementing new anti-fraud technology?





# HOW IS GENERATIVE AI AFFECTING ORGANIZATIONS' ANTI-FRAUD PROGRAMS?



*Generative AI* is the term used to describe deep learning artificial intelligence models used for high-quality image, video, audio, or text generation. This technology has risen in prominence quickly, and many organizations are experimenting with and formally implementing it to assist their operations across numerous functions.

As part of our study, we explored the implementation of generative AI as part of organizations' anti-fraud programs. Most respondents (83%) indicated that their organizations expect to adopt generative AI tools as part of their anti-fraud toolkit over the next two years.

When assessing whether and how to employ this technology, organizations must consider several factors. As noted in Figure 15, 85% of organizations consider the accuracy of the results achieved by generative AI as a very important or important factor in this decision, while security risks and vulnerabilities receive the same level of consideration by 83%. Additionally, although ease of use is often noted as one of the main benefits of generative AI, 77% of organizations still consider staffing and in-house skills related to the technology an important or very important factor in determining whether to implement it.



“**The use of generative AI in other anti-fraud initiatives could play a significant part in identifying anomalies, trends, and indications in larger volumes of data with minimal resource concerns. However, the organization will need to ensure that proper guidelines are in place to minimize errors and bias.**” – Survey respondent

“**Accuracy, in my opinion, is the biggest challenge for generative AI, as investigators will find it difficult to trust or deploy an inaccurate technology. This is because investigation should be an exact science.**”  
– Survey respondent

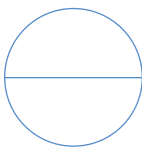
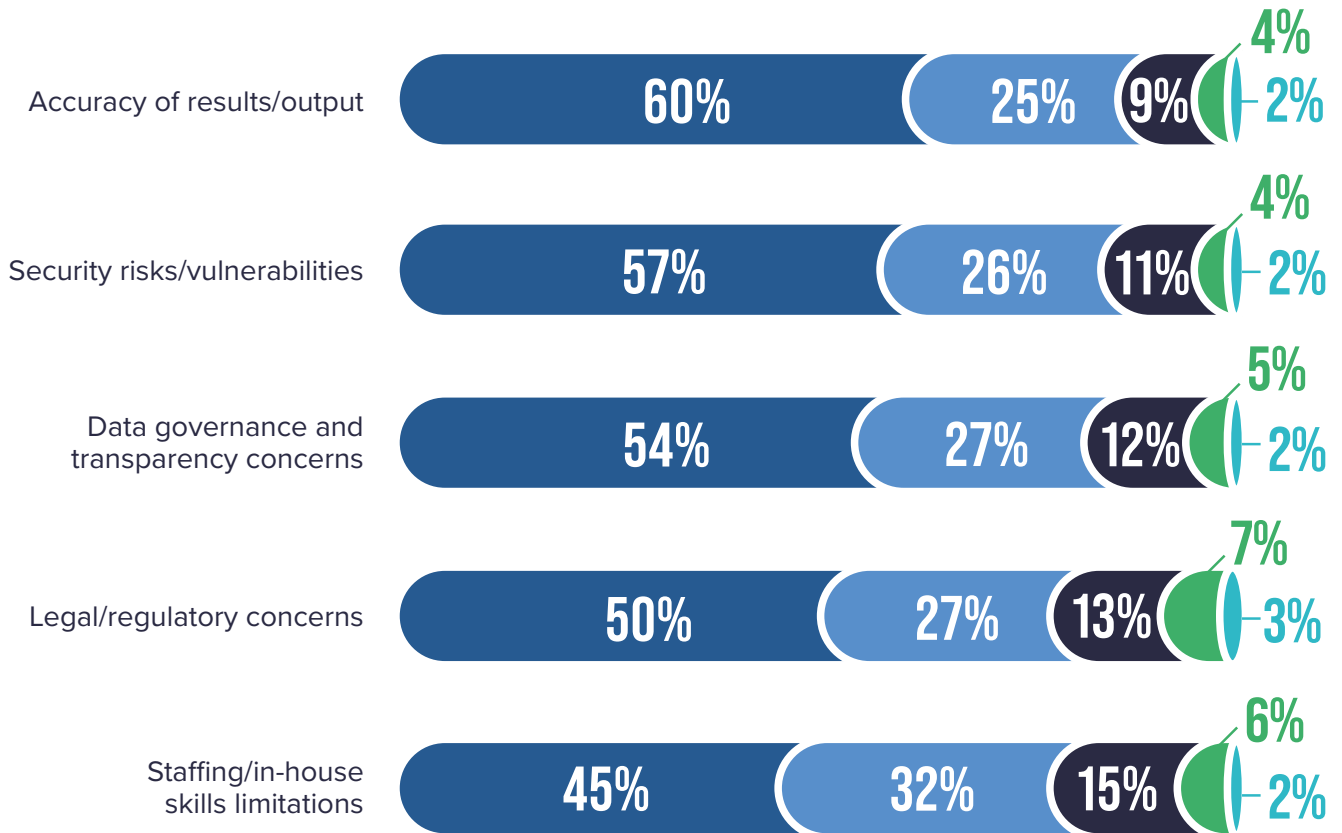
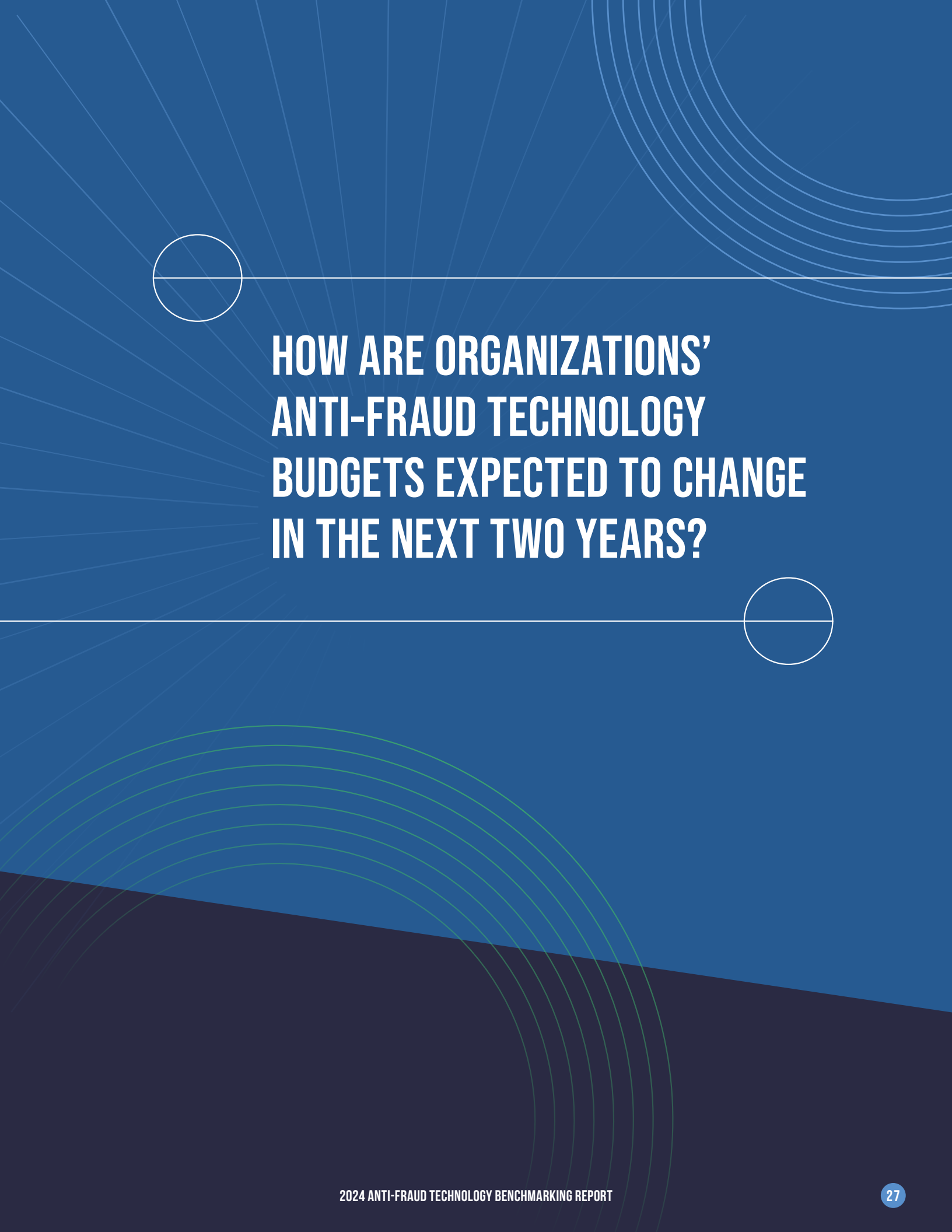


FIG. 15

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



● Very important   
 ● Important   
 ● Moderately important  
● Slightly important   
 ● Not important



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

Keeping ahead of fraudsters often means dedicating resources to purchase and implement additional tools to prevent and detect their schemes. As noted in Figure 14, budget and financial restrictions present a major or moderate challenge to most organizations' implementation of new anti-fraud technology. Even

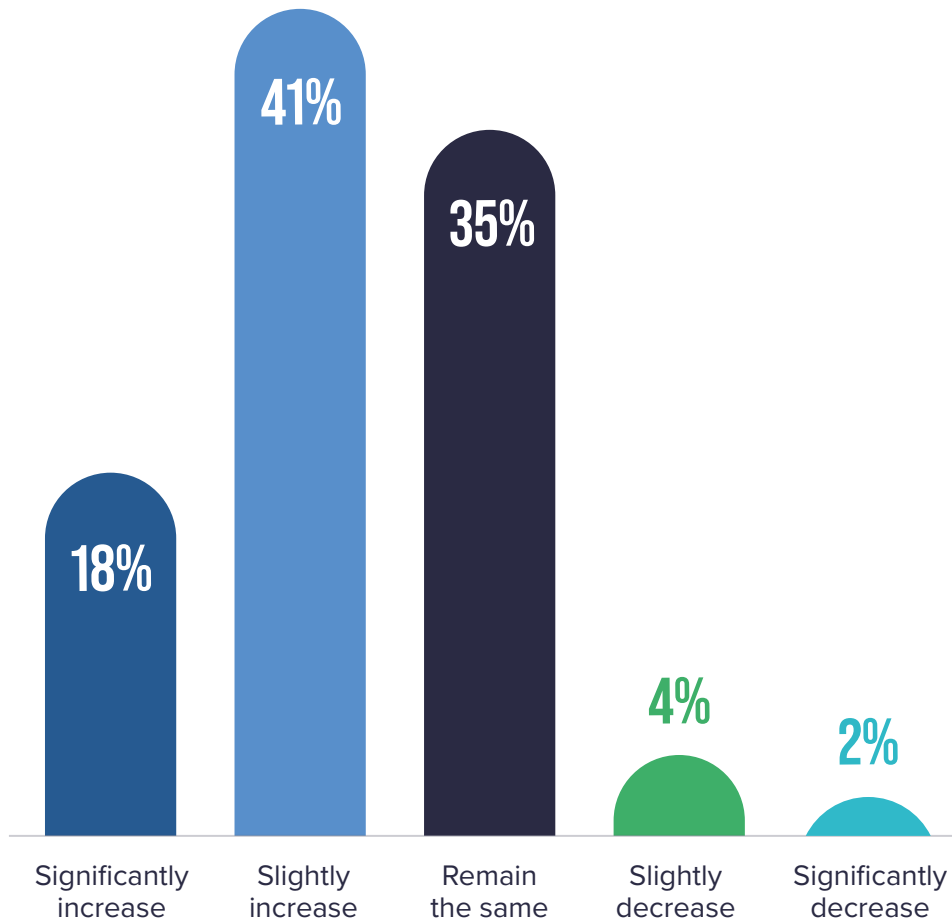
still, our study shows that 59% of organizations expect to increase their budgets for anti-fraud technology over the next two years (see Figure 16). Only 6% of organizations anticipate budget cuts in this area, demonstrating the accepted value that deploying new technology can bring to the fight against fraud.

59% of organizations expect to **INCREASE THEIR BUDGETS** for anti-fraud technology over the next two years.



FIG. 16

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



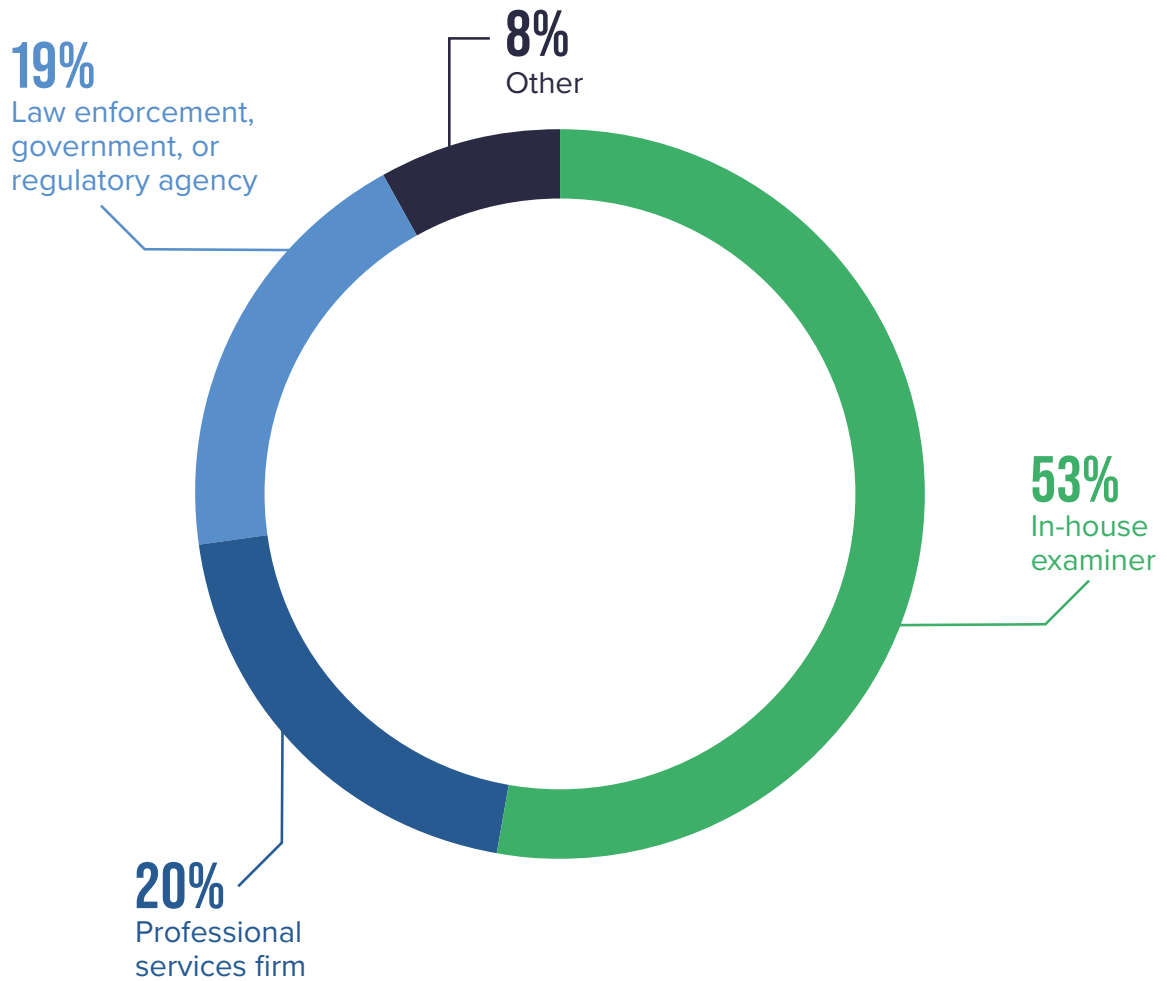
# RESPONDENT DEMOGRAPHICS

This report contains analyses of our survey findings based on all responses received in all demographic categories. For sub-analyses based on specific industries, regions, and organization sizes, please visit [SAS.com/fraudsurvey](https://sas.com/fraudsurvey).

## RESPONDENTS' PROFESSIONAL ROLE

More than half (53%) of the individuals who participated in our study work in-house and conduct anti-fraud activities within a single organization. Another 20% work for professional services firms that conduct anti-fraud activities or engagements on behalf of other organizations, and 19% work for a law enforcement, government, or regulatory agency that conducts fraud investigations or other engagements involving outside parties under the authority of their agency.

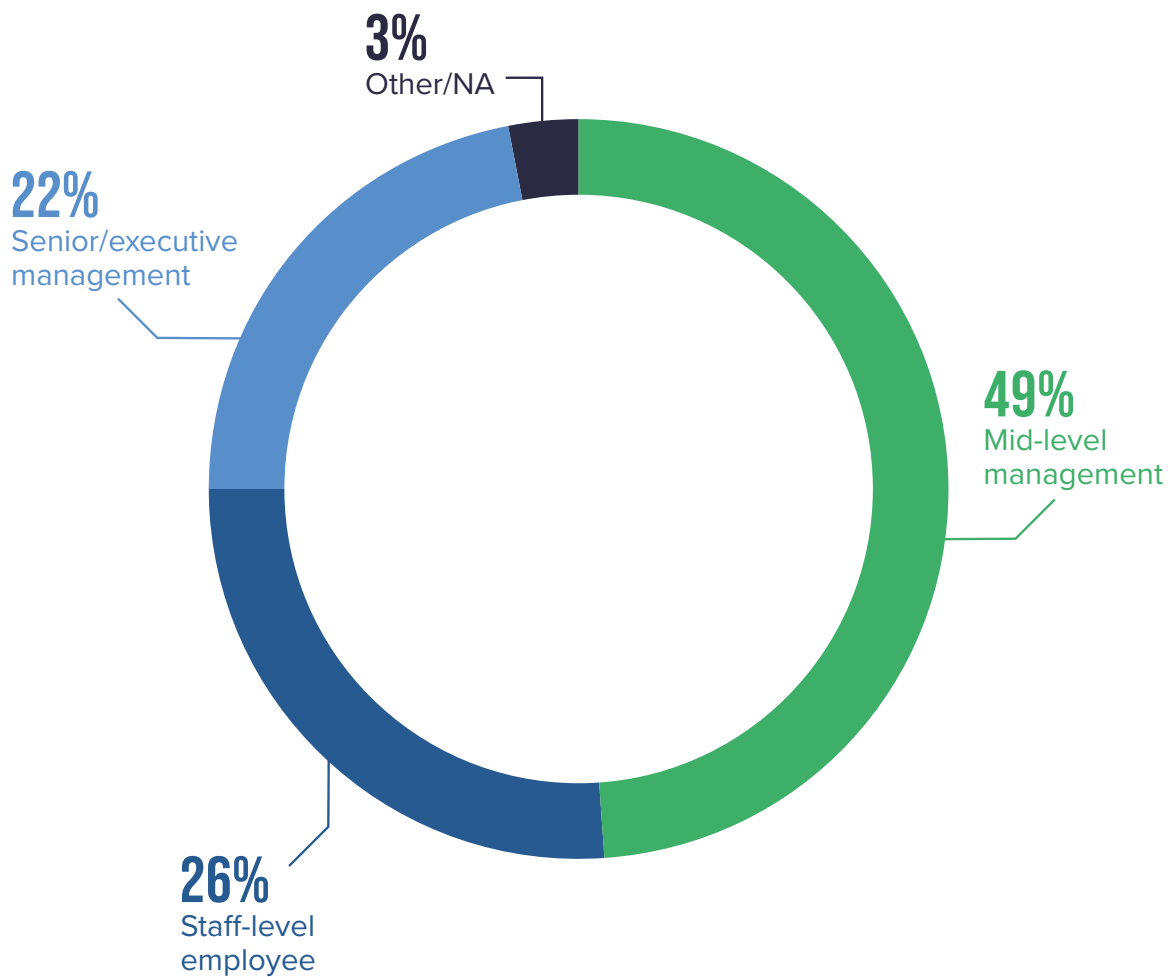
FIG. 17 Respondents' professional role



## RESPONDENTS' POSITION LEVEL

Nearly half of our survey respondents hold mid-level management positions within their organizations, while 26% are in staff-level (non-supervisory) roles, and 22% are at the senior or executive management level.

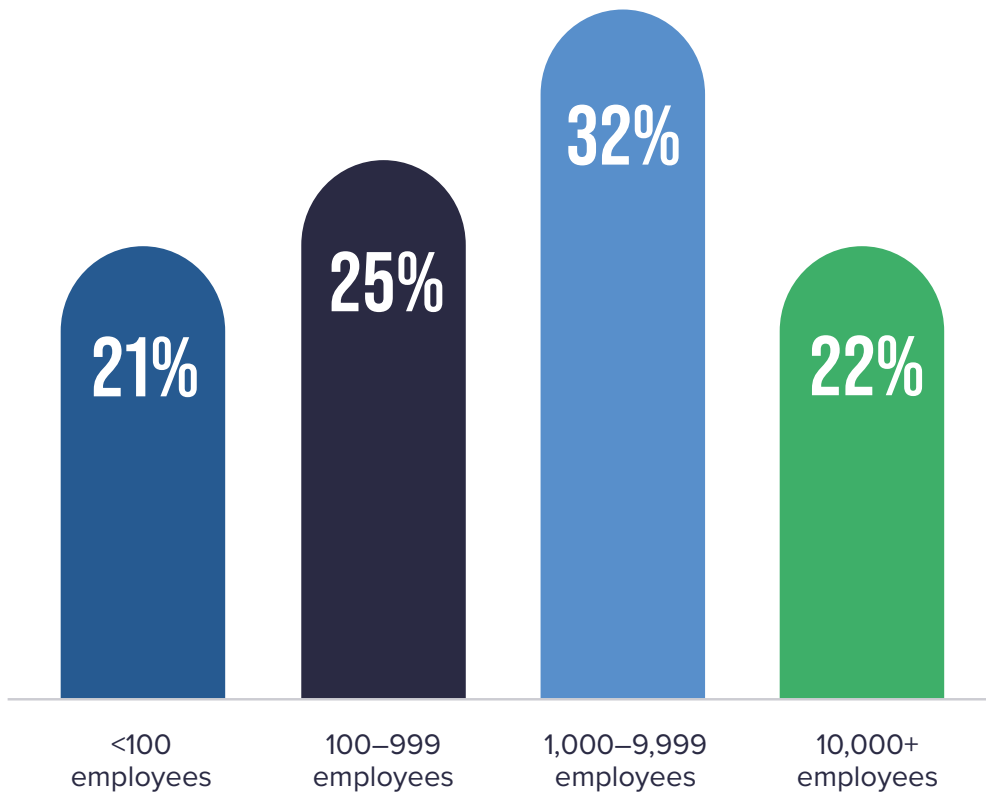
**FIG. 18** Respondents' position level



## SIZE OF RESPONDENTS' ORGANIZATIONS

Survey respondents represented a variety of organizational sizes. As noted in Figure 19, nearly one-third (32%) work for organizations with 1,000–9,999 employees, and one-quarter work for organizations with 100–999 employees.

**FIG. 19** Size of respondents' organizations

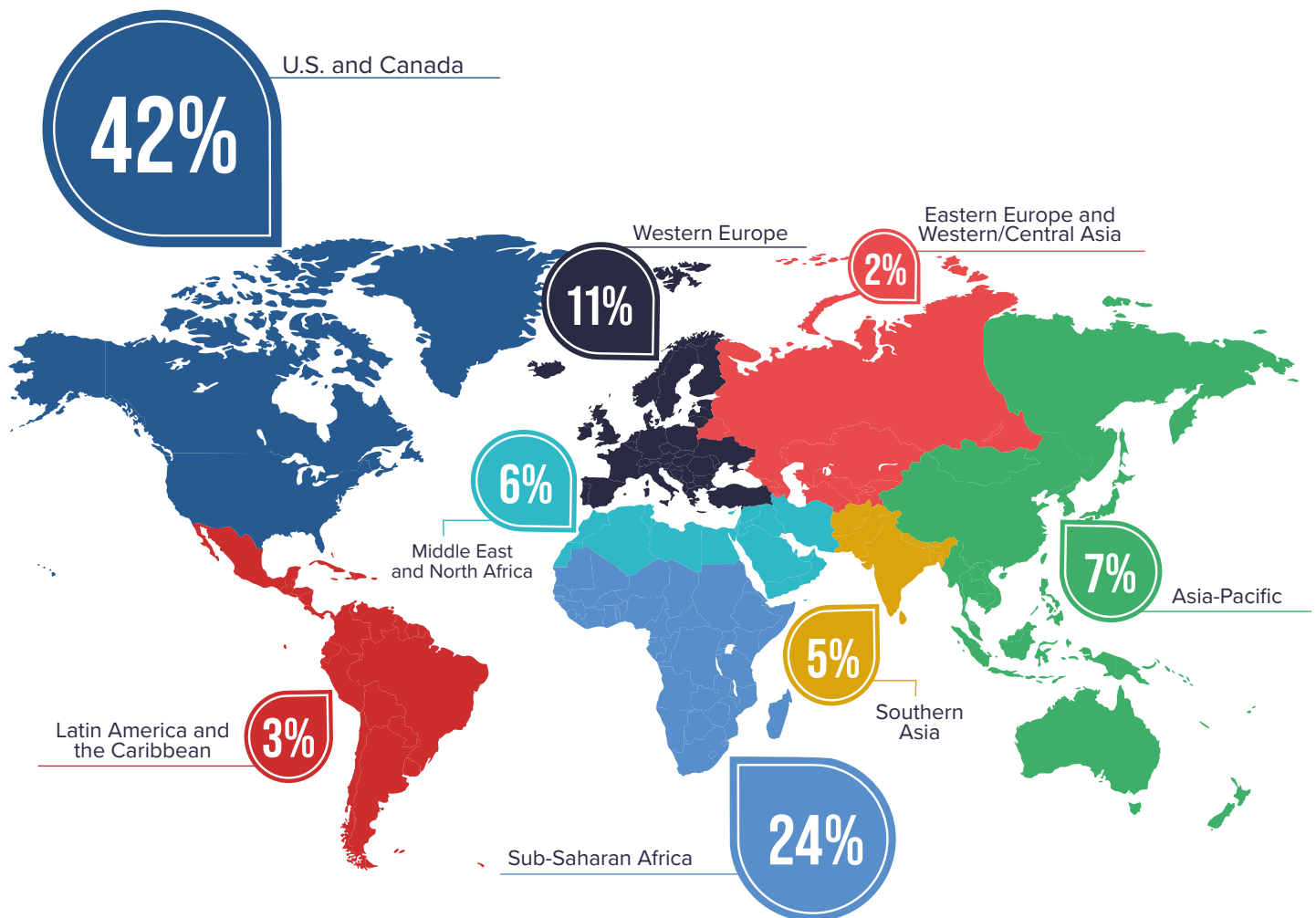




## REGION OF RESPONDENTS' ORGANIZATIONS

Survey respondents represented organizations in 111 countries around the world, providing a global view into trends in anti-fraud technology. The greatest proportion of respondents (42%) are from the United States and Canada, followed by Sub-Saharan Africa (24%) and Western Europe (11%).

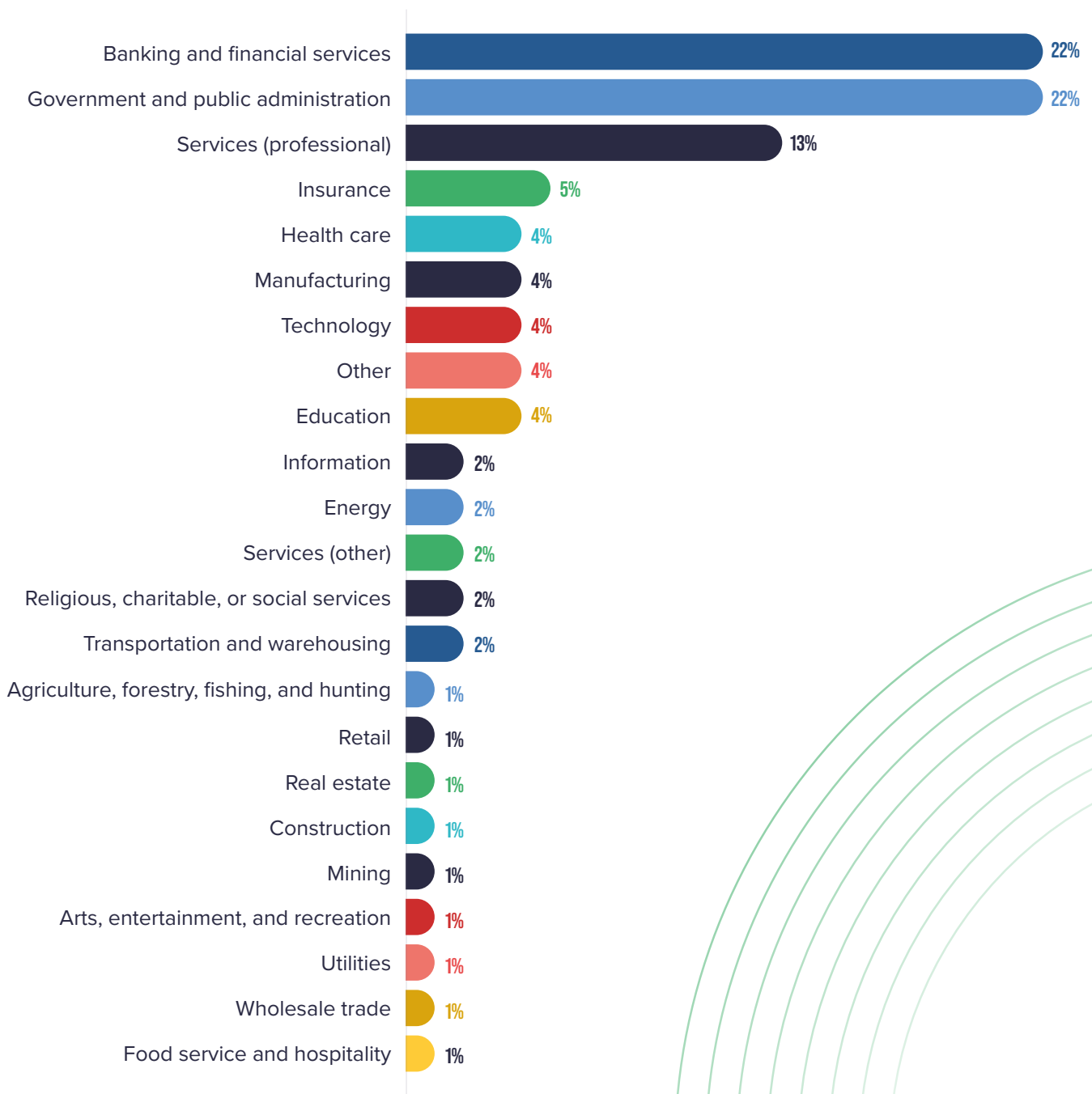
**FIG. 20** Region of respondents' organizations



## INDUSTRY OF RESPONDENTS' ORGANIZATIONS

The two most common industries represented in our study are banking and financial services, and government and public administration, each comprising 22% of survey participants. Other industries with notable representation are professional services (13%) and insurance (5%), with the remainder of participants spread among many other sectors.

**FIG. 21** 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 90,000 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](https://www.acfe.com).

## ABOUT SAS

SAS is the global leader in AI and analytics. 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. Since 1976, SAS has given customers world-wide THE POWER TO KNOW®. [Learn more about SAS.](#)

