ACFE
Association of Certified Fraud Examiners

sas

2022

ANTI-FRAUD TECHNOLOGY BENCHMARKING REPORT

TABLE OF CONTENTS

KEY FINDINGS

MORE THAN 1/2

of organizations currently use **exception reporting and anomaly detection, as well as automated monitoring of red flags and business analysis** as part of their anti-fraud programs.

Over the next two years, **use of each of these techniques is expected to grow** to more than

2/3 OF ORGANIZATIONS

THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

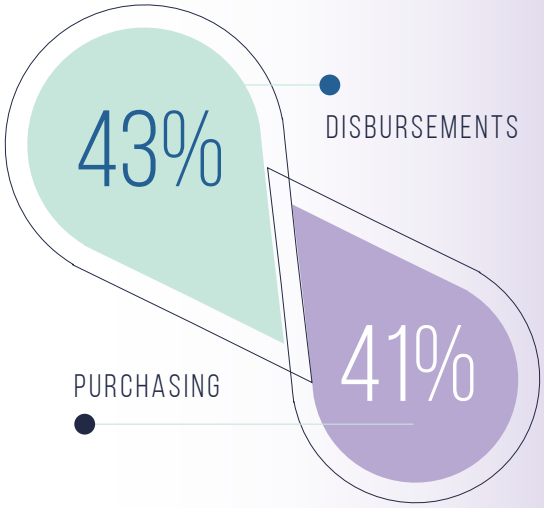
in anti-fraud programs is expected to more than

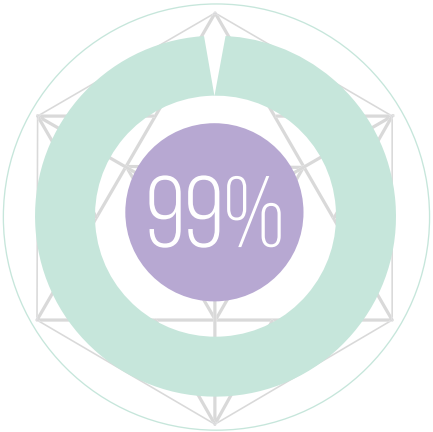
DOUBLE

over the next two years.

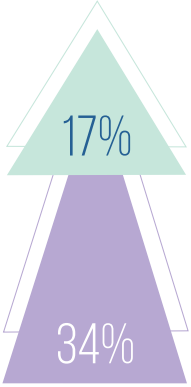
The risk areas where organizations most commonly use **data analytics to monitor for potential fraud** are

DISBURSEMENTS (43%) AND PURCHASING (41%).





99% of organizations say that the **increased volume of transactions reviewed and the improved timeliness of anomaly detection** are beneficial outcomes of their anti-fraud analytics programs.



34% of organizations currently use

PHYSICAL BIOMETRICS

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

KEY FINDINGS

MORE THAN

40% OF ORGANIZATIONS

expect to add computer vision analysis, robotics, or blockchain/distributed ledger technology to their anti-fraud technology toolkit in the future.

34% of organizations currently contribute to data-sharing consortiums to help combat fraud,

AND

24% would be willing to contribute in the future.

BUDGET AND FINANCIAL CONCERNS

are the biggest challenge for organizations in implementing new anti-fraud technologies.

60%

of organizations expect an increase in their

ANTI-FRAUD TECHNOLOGY BUDGETS

in the next two years.

43%

of organizations have increased their use of

DATA ANALYTICS

in response to the COVID-19 pandemic.

INTRODUCTION

The fight against fraud can feel like a battle to stay one step ahead of the fraud perpetrators, especially as the fraud risks that organizations face today are more dynamic and persistent than ever. Thankfully, anti-fraud professionals have a full suite of technologies they can deploy to combat these threats. From traditional data analytics to emerging options such as robotic process automation and computer vision analysis, anti-fraud technology plays a key role in many organizations' fraud programs.

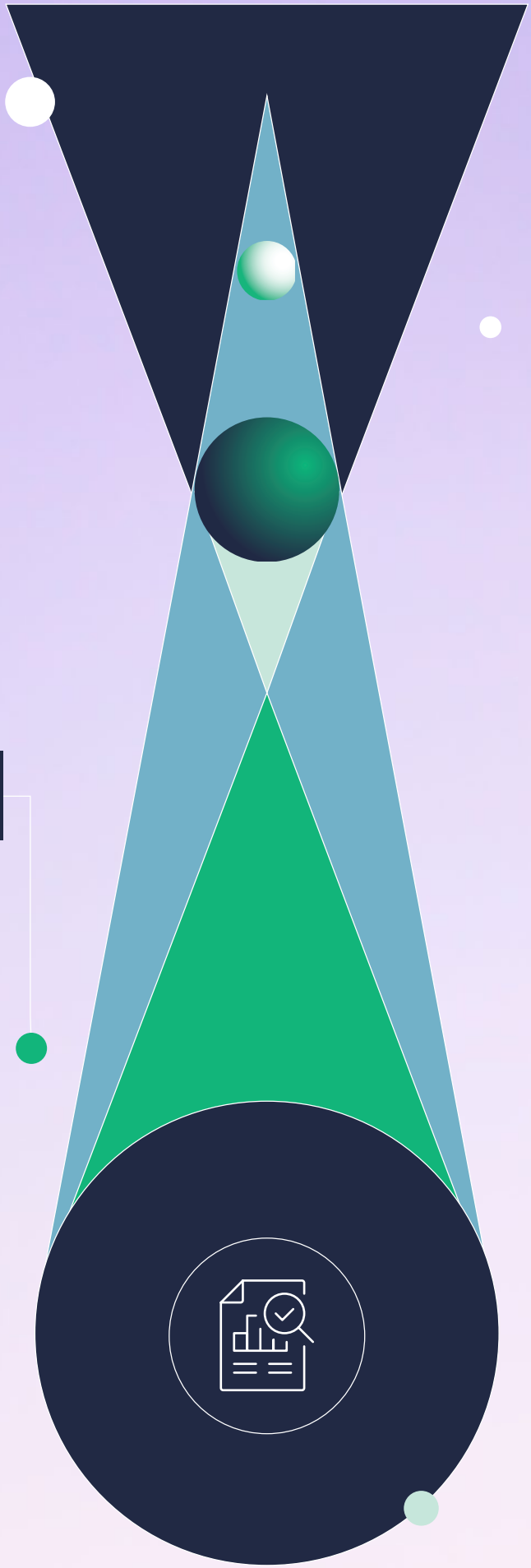
To understand how these technologies are being used by organizations, we surveyed ACFE members about the anti-fraud technologies their organizations currently use or plan to adopt. We hope that the insights from our study are helpful to organizations and professionals in benchmarking their own initiatives, gaining buy-in and context for future technology investments, and successfully implementing a comprehensive anti-fraud technology toolkit.

METHODOLOGY

In October 2021, we sent a 20-question survey to 80,011 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 884 survey responses that were usable for purposes of this report. This report provides a summary of respondents' answers to the survey questions.

The 2022 *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.**

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



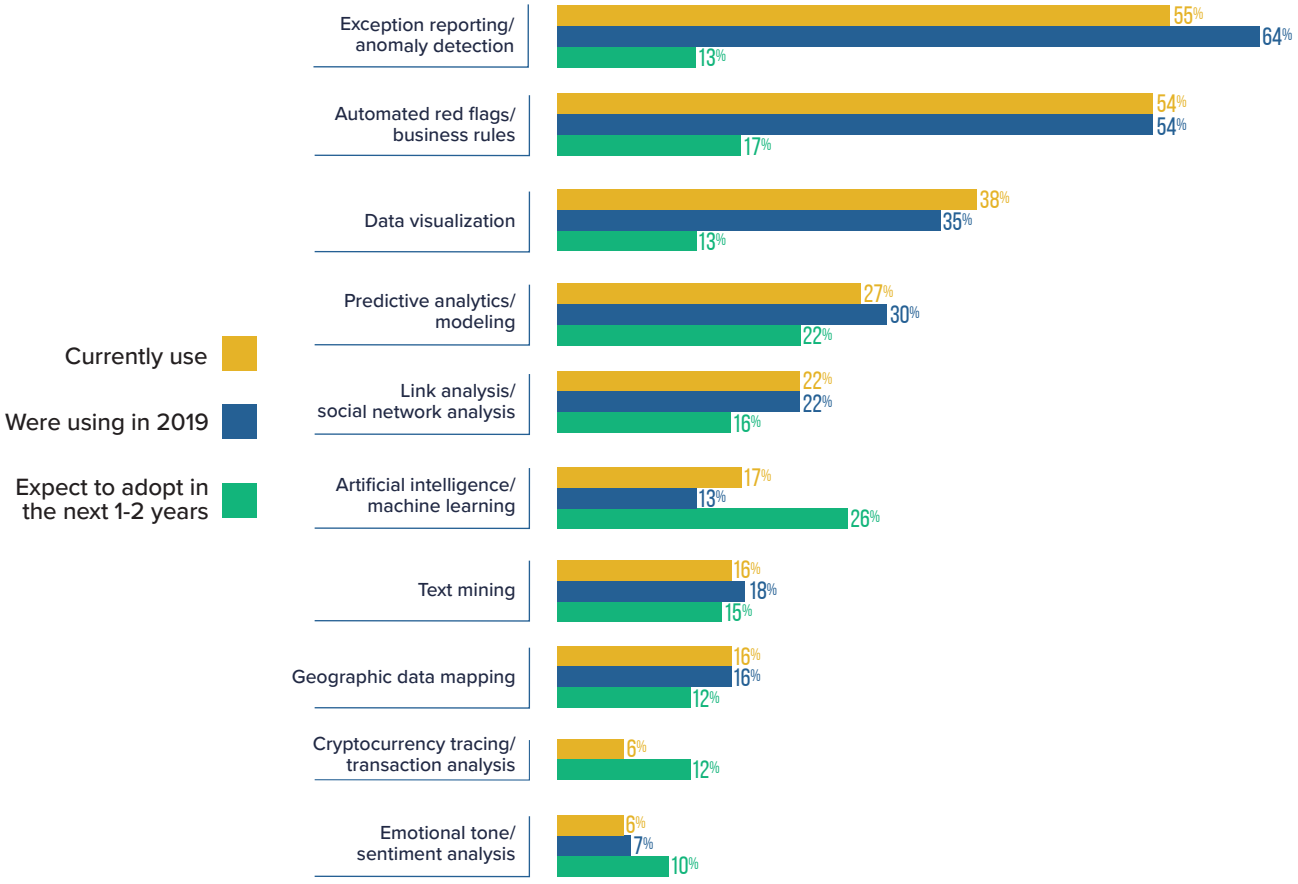
WHAT DATA ANALYSIS TECHNIQUES DO ORGANIZATIONS USE TO FIGHT FRAUD?

The variety of approaches for implementing anti-fraud analytics continues to grow; however, our study indicates that the most commonly used analytics are the tried-and-true techniques that organizations have found success with for decades. More than half of organizations currently use exception reporting and anomaly detection, as well as automated monitoring of red flags and business rules as part of their anti-fraud programs, making them the two most common approaches. With another 13% and 17% (respectively) of respondents expecting to adopt these types of analytics in the next two years, our study indicates that more than two-thirds of organizations will employ these anti-fraud analytics techniques by 2023.

Additionally, while only 17% of organizations' anti-fraud programs currently use artificial intelligence or machine learning analytics, these techniques are expected to experience the most growth, with 26% anticipating that their organizations will adopt this type of advanced analytics technology in the next two years.

Although many respondents project adoption of additional analytics approaches in coming years, the use of most of these initiatives has remained relatively flat since 2019. The one notable outlier is exception reporting and anomaly detection, which is used by 55% of the organizations in our current study, compared to 64% of organizations in our prior study. This might be due to organizations shifting their analytics initiatives or simply the different organizations being represented in each of the two studies.

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



We also asked about the software programs organizations are using to conduct each of these analytical techniques. The most common platforms are noted in Figure 2. While several off-the-shelf tools are mentioned for most categories, a notable number of organizations are still developing their own in-house, proprietary systems to employ in anti-fraud analytics initiatives.

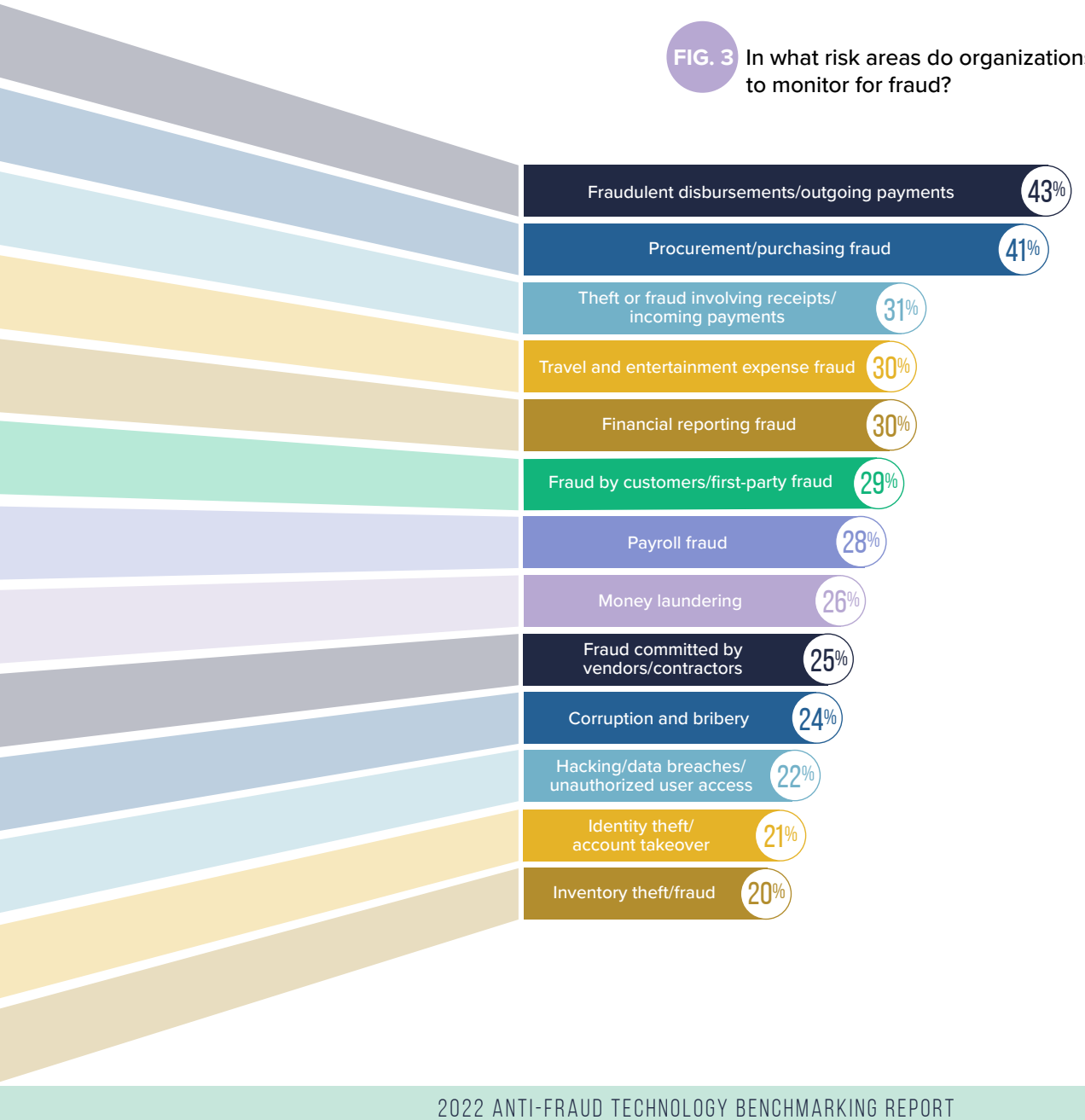
FIG. 2 What are the most commonly used programs for each analytic technique?

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

When deploying anti-fraud analytics, organizations often take a risk-based approach—that is, they tie their analytics initiatives to the areas of the organization where fraud risks are highest or where the evidence of potential fraud can be most effectively uncovered using data monitoring and analysis.

Because fraud risks vary by organization, the areas where analytics are used in this way will also vary. The two most common risk areas monitored with analytics in our study are fraudulent disbursements and outgoing payments (43% of respondents) and procurement and purchasing fraud (41% of respondents). Nearly every organization has functions for making and paying for purchases, and there is an inherent risk that funds might be stolen as part of these processes, so it would stand to reason that these are among the most common risk areas for organizations to monitor using data analytics. Other top fraud risk areas where analytics are used include theft or fraud involving incoming payments (31%), travel and entertainment expense fraud (30%), and financial reporting fraud (30%).

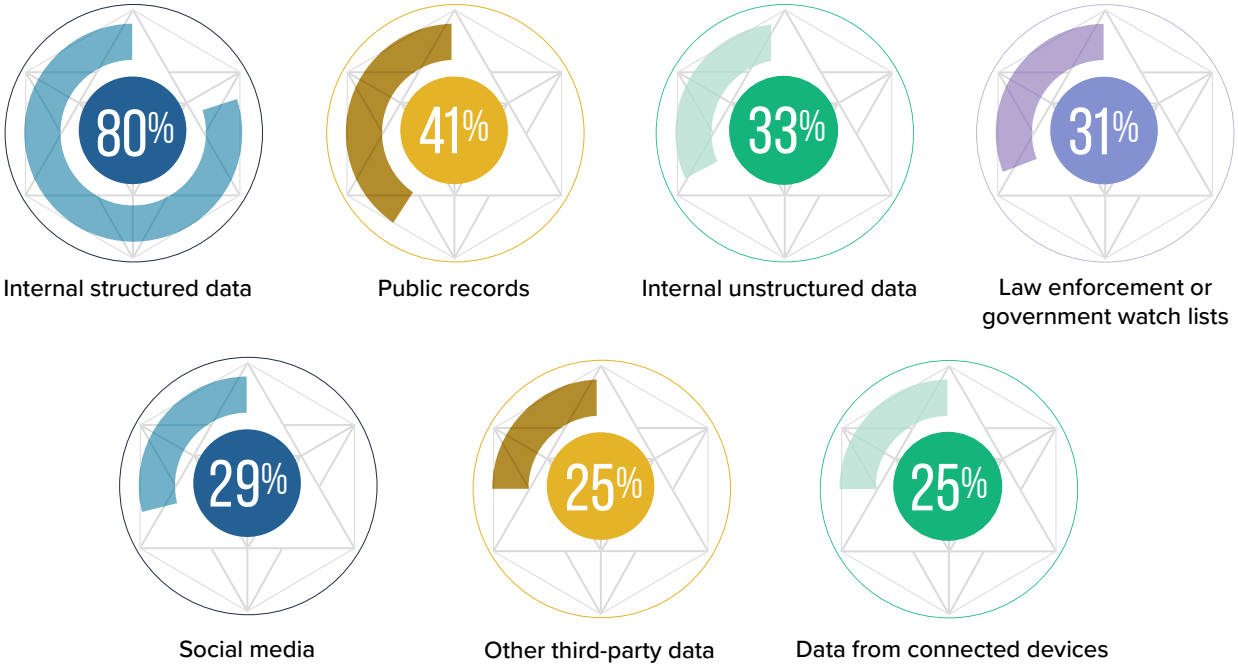
FIG. 3 In what risk areas do organizations use data analytics to monitor for fraud?



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

Evidence of potential and actual fraud can exist in various forms and locations; consequently, effectively analyzing data for warning signs of fraud often involves pulling data from multiple sources. The vast majority of respondents in our study (80%) include internal structured data in their anti-fraud analytics initiatives, which is nearly double the percentage of respondents that use data from any other source. This highlights that most organizations still rely heavily on traditional analytics approaches and data sources to drive their anti-fraud programs. In contrast, only one-third of participants' organizations currently use internal data from unstructured sources. Additionally, some organizations also bring in data from external sources, such as public records (41%), law enforcement or government watch lists (31%), social media (29%), and other third-party data (25%).

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



DATA EXISTS IN TWO FORMATS: **STRUCTURED** AND **UNSTRUCTURED.**

Structured data is data that is formatted in recognizable and predictable structures, such as the data found in databases and spreadsheets. Examples of structured data include sales records, payment or expense details, and financial reports. *Unstructured data*, in contrast, is data found outside structured databases and spreadsheets. Examples of unstructured data include text documents, email and instant messages, and image files.

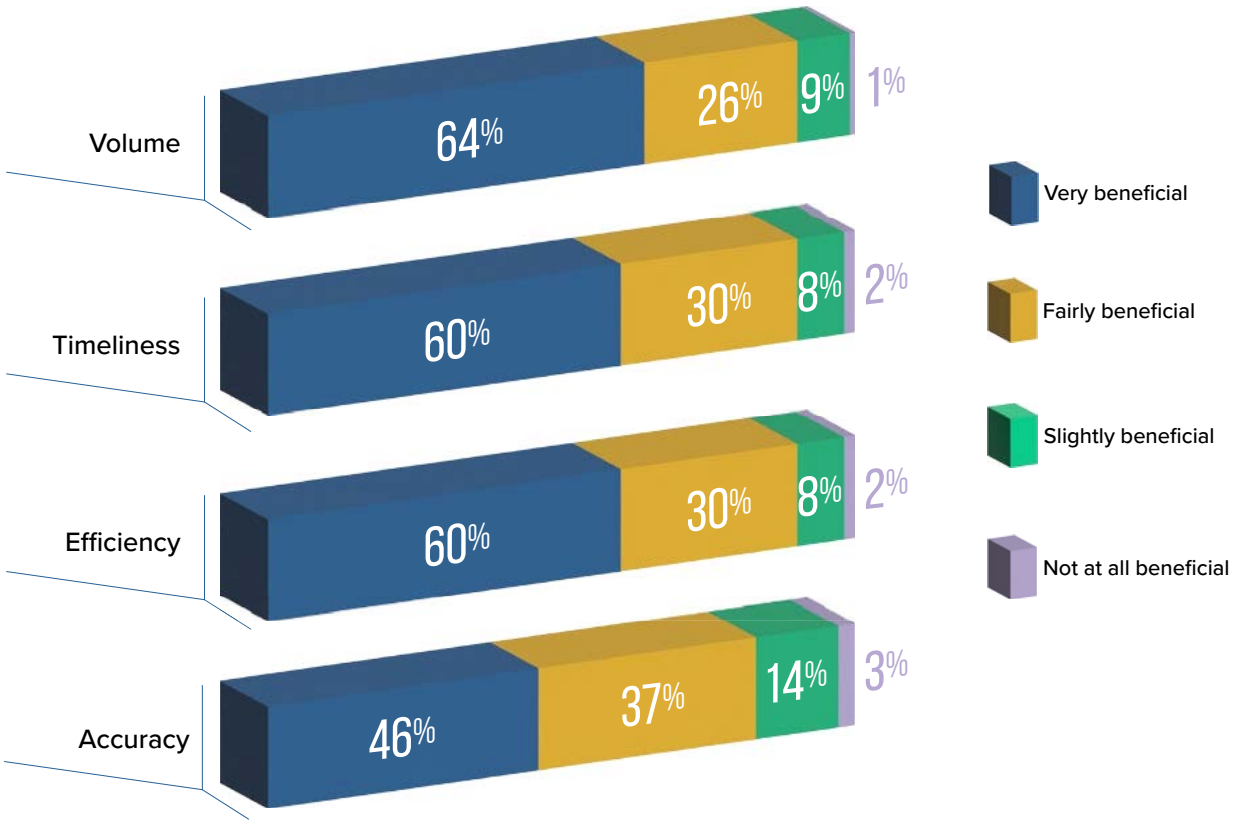
HOW BENEFICIAL IS DATA ANALYTICS TO DIFFERENT AREAS OF ORGANIZATIONS' ANTI-FRAUD INITIATIVES?

When obtaining buy-in and setting objectives for new anti-fraud technologies, it can be helpful to define the benefits the organization expects to realize from the technology's use. To provide insight into the value that data analytics can provide, we asked survey respondents about how beneficial their organizations' anti-fraud analytics programs have been with respect to four 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

As noted in Figure 5, nearly all respondents (97%–99%) have seen benefits in each of these areas, with volume, timeliness, and efficiency being cited as either very or fairly beneficial by 90% of survey participants.

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?

Case management software enables fraud teams to track, report on, and retain information about current and prior fraud allegations and investigations. Our study indicates that 42% of organizations have implemented a case management program, meaning more than half of the organizations in our study are not using a formal platform to manage their case processes and data. Of the organizations with a case management system in place, the most common is a proprietary program that was developed in-house; however, a wide variety of third-party platforms are used by the respondents in our study.

FIG. 6 Are organizations using case management software?

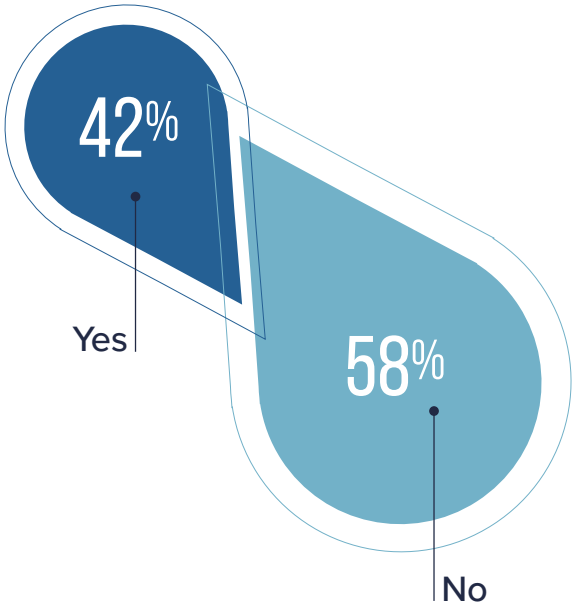
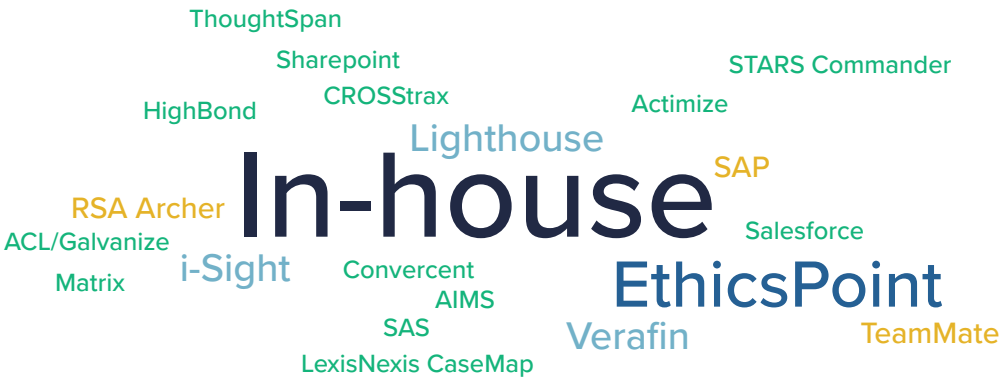


FIG. 7 What are the most common case management software programs?



ARE ORGANIZATIONS USING DIGITAL FORENSICS/E-DISCOVERY SOFTWARE?

While evidence in fraud-related cases might be found on employee or organizational devices, the majority of organizations in our study are not currently using any formal digital forensics or e-discovery software to collect and capture this information. Just under 30% have adopted a program for this purpose; of those, EnCase is the most commonly used platform, followed by Relativity.

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

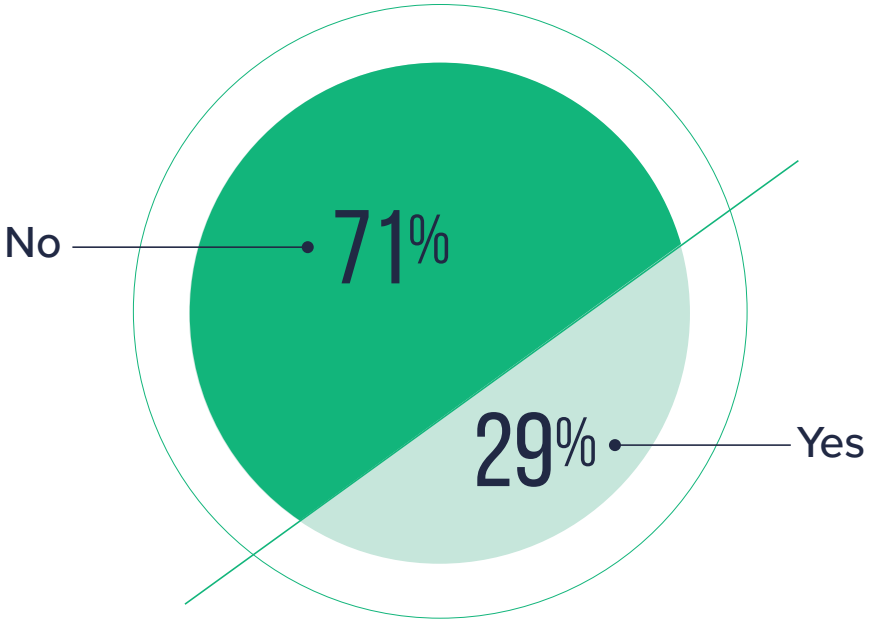


FIG. 9 What are the most common digital forensics/e-discovery software programs?

ARE ORGANIZATIONS USING ONLINE-EVIDENCE CAPTURING SOFTWARE?

Evidence from online sources, such as websites and social media, can be a critical component of building a fraud case; capturing and storing this type of evidence, however, involves a different set of considerations than working with internal sources of evidence. Consequently, specialized software can be used to help investigators with the privacy, compliance, retention, and logistical factors inherent in working with online evidence. One-third of our survey respondents currently use this type of software, showing that the use of such programs is not widespread. Additionally, for those organizations that have adopted online-evidence capturing software, the most commonly used tools are proprietary programs developed in-house for this purpose.

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

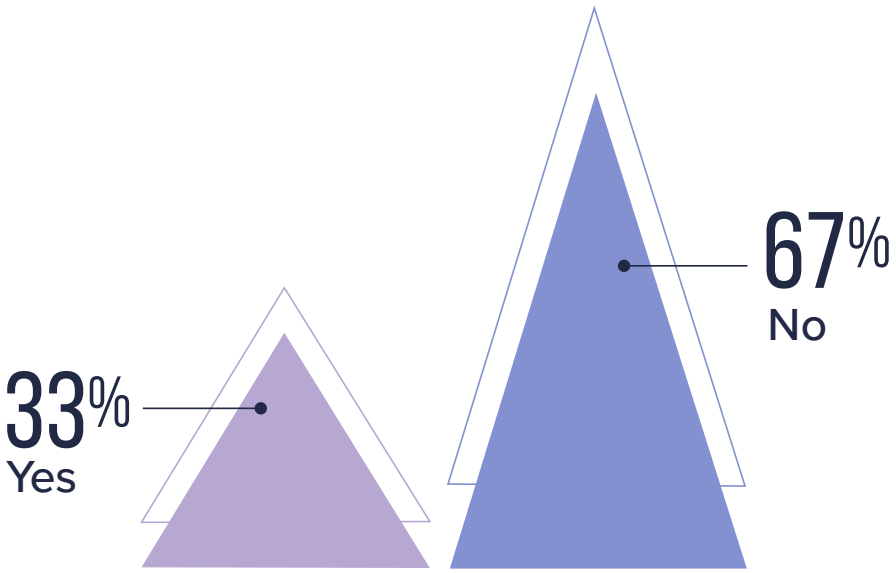
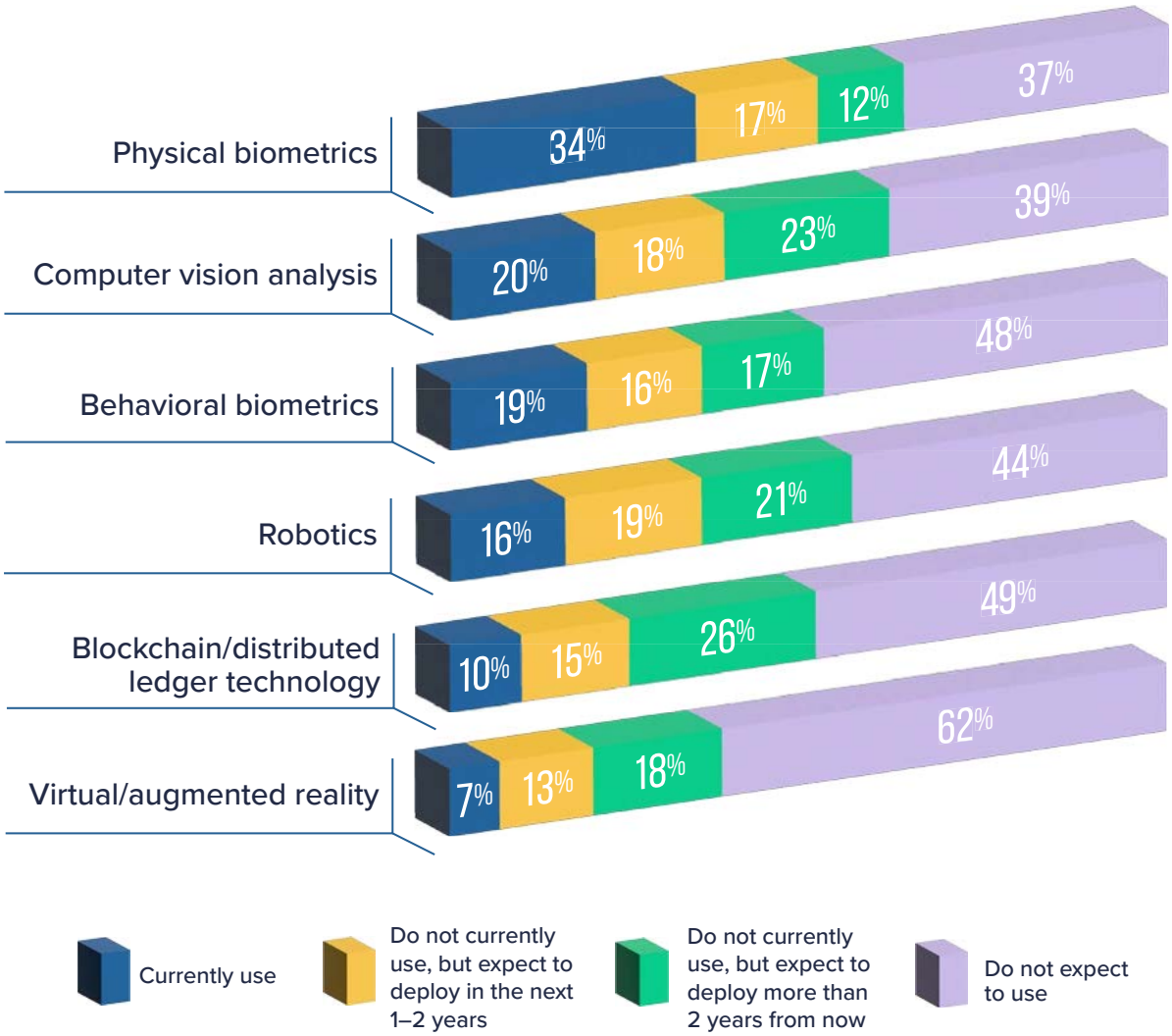


FIG. 11 What are the most common online-evidence capturing software programs?

WHAT EMERGING TECHNOLOGIES ARE ORGANIZATIONS USING TO FIGHT FRAUD?

As new technologies emerge, some organizations tend to adopt them quickly, while others delay or decline adoption for various reasons. We asked survey respondents about their organizations' current and expected use of several recently emerging technologies as part of their anti-fraud programs. As Figure 12 shows, physical biometrics (e.g., fingerprint, facial, or vocal recognition tools) are the most commonly employed emerging technology, with 34% of organizations currently using them and 17% anticipating adopting them in the next 1–2 years. Computer vision analysis—or the use of computer- or artificial intelligence–based analysis of video or photographic data—is also becoming more common; one-fifth of organizations already employ this technology, and 18% expect to add it within the next two years. Virtual and augmented reality tools are currently the least widespread of the emerging technologies we analyzed; 62% of organizations in our study do not expect to use virtual or augmented reality as part of their anti-fraud technology suite.

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

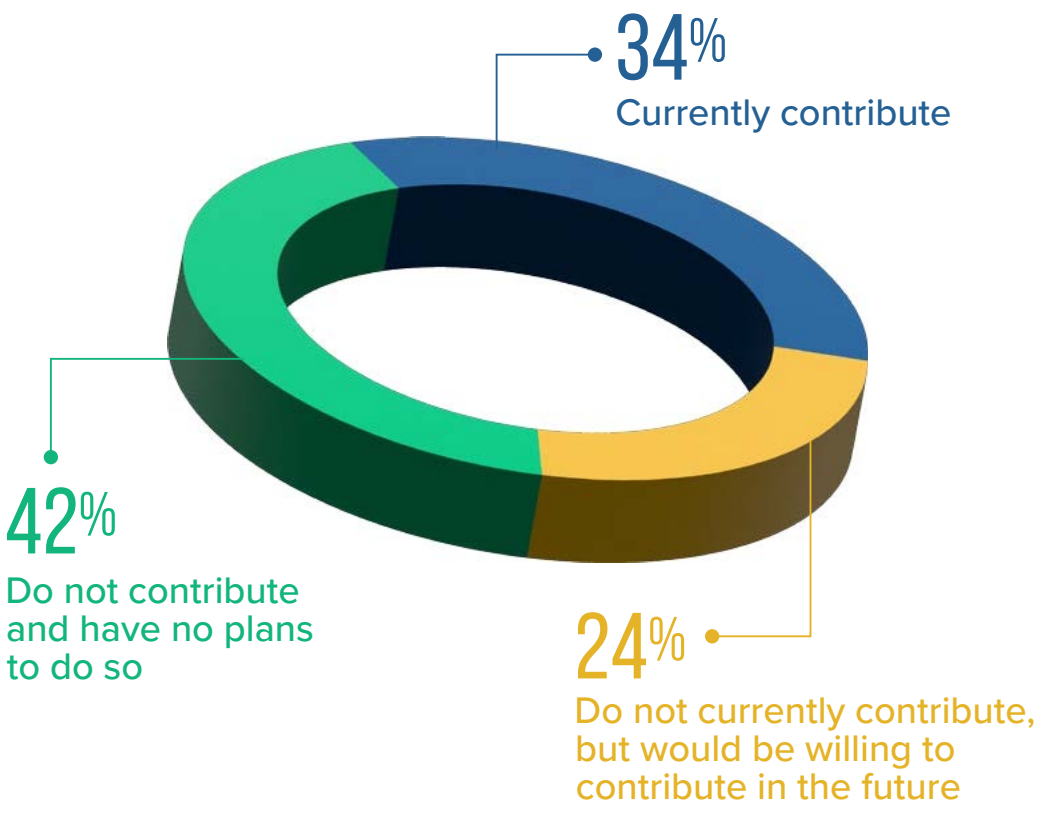


ARE ORGANIZATIONS CONTRIBUTING TO DATA-SHARING CONSORTIUMS TO HELP PREVENT OR DETECT FRAUD?

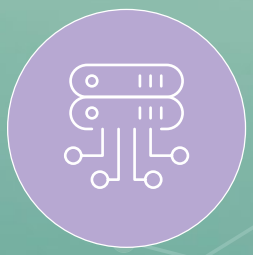
Data-sharing consortiums can be a valuable tool in the fight against fraud. These initiatives, which often are set up within specific industry groups, involve organizations agreeing to contribute their respective data into an aggregated database that all member organizations can access. Pooling data across organizations like this facilitates broader analysis and monitoring for trends, and thus potentially enables organizations to take earlier protective measures against growing threats. However, concerns around data privacy and logistics might limit participation.

Approximately one-third (34%) of the organizations in our study are currently contributing to data-sharing consortiums. Almost one-quarter (24%) indicated they do not currently contribute but would consider doing so in the future.

FIG. 13 Are organizations contributing to data-sharing consortiums to help prevent or detect fraud?

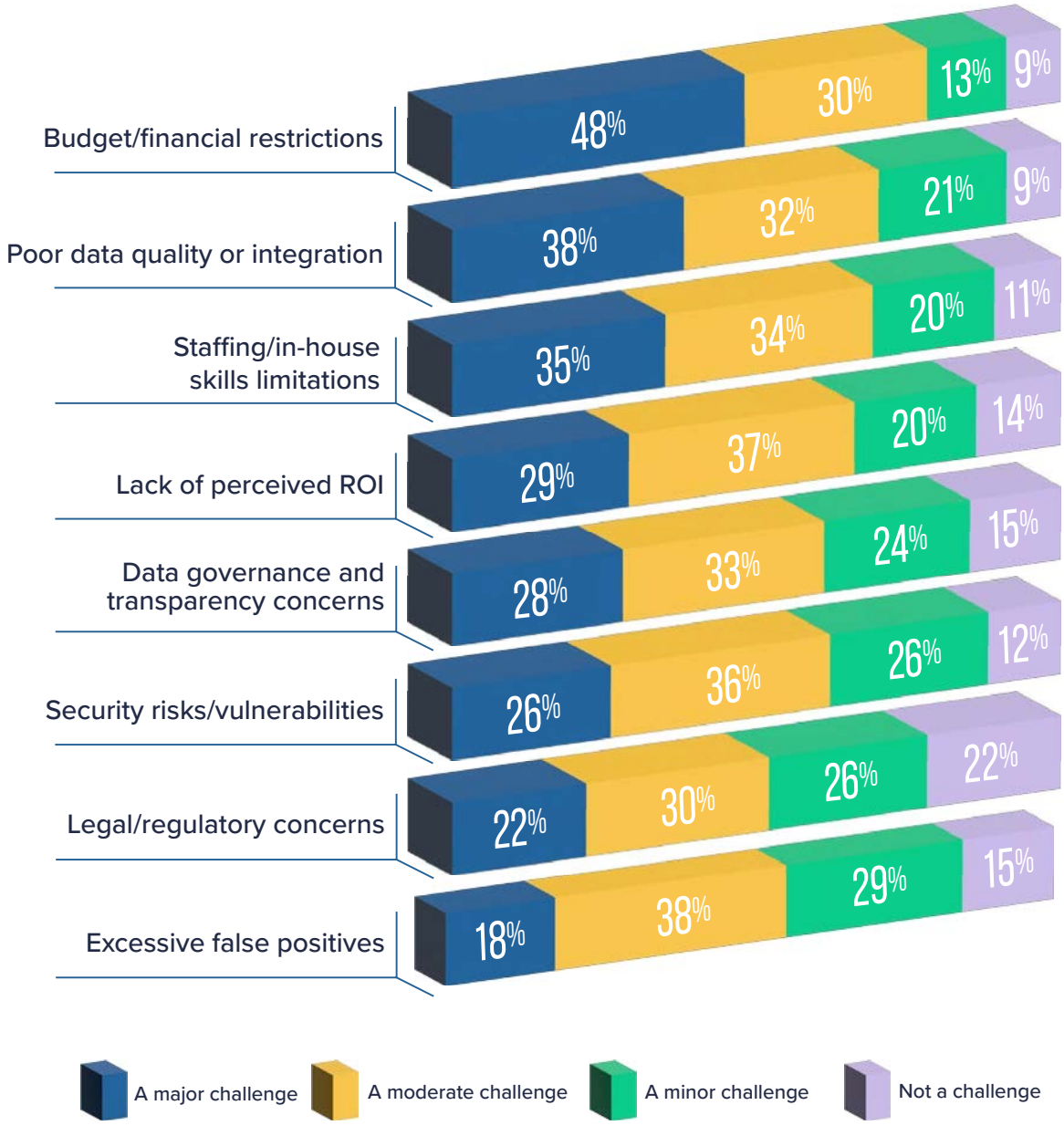


WHAT CHALLENGES DO ORGANIZATIONS FACE IN IMPLEMENTING NEW ANTI-FRAUD TECHNOLOGY?



Adopting new technology in an organization can come with challenges, both in the planning and implementation stages. We asked respondents about the types of hurdles they face as part of enacting new anti-fraud technologies; the top obstacle noted is budget and financial restrictions, with 78% of participants saying this is a major or moderate challenge at their organizations. This is followed by challenges with poor data quality or integration (70%) and limitations with staffing and in-house skills (69%).

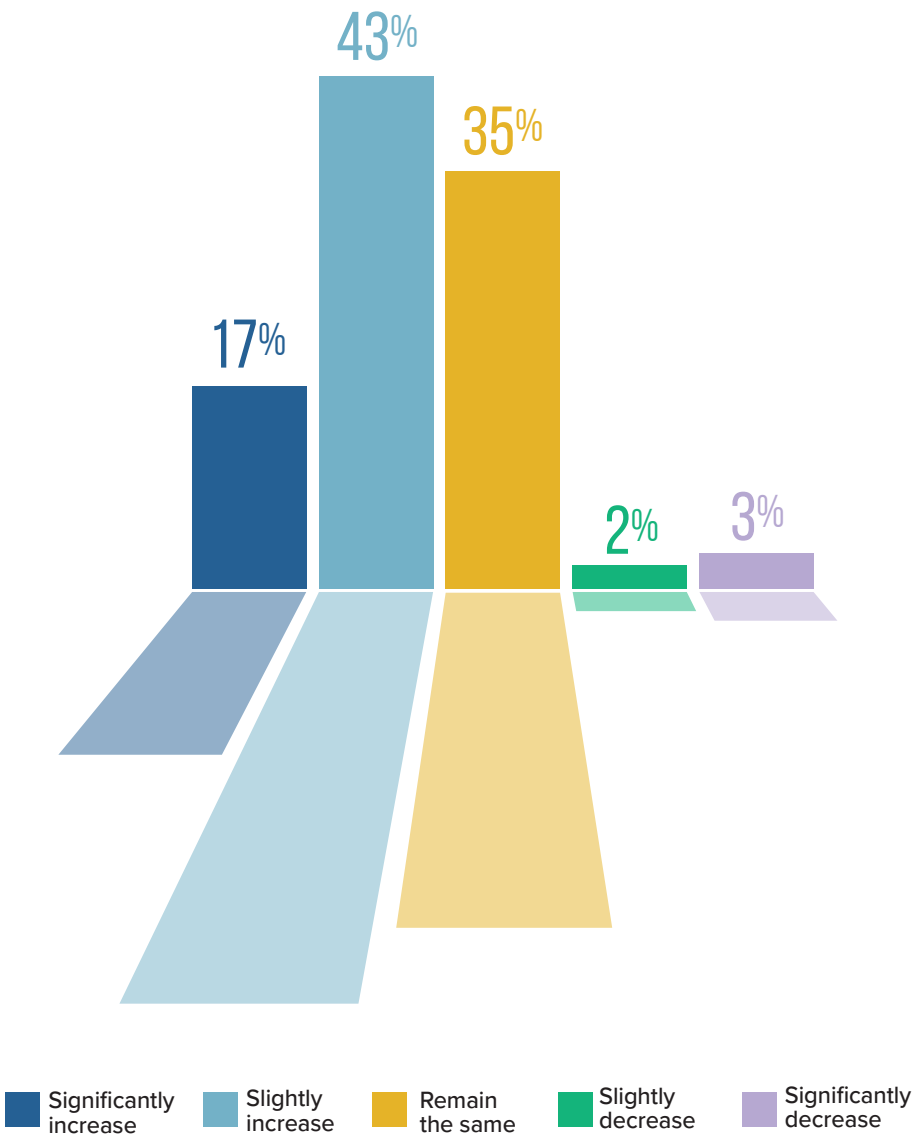
FIG.14 What challenges do organizations face in implementing new anti-fraud technology?



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

As new technologies are adopted and the use of existing technology is expanded, organizations typically must invest additional resources to fund these initiatives. Even with budget concerns being the top challenge noted by survey respondents (see Figure 14), our survey shows that the majority of organizations are already budgeting for expanded technology use, with 60% expecting a significant (17%) or slight (43%) budget increase for anti-fraud technology in the next two years. Approximately one-third of organizations anticipate their budgets to remain about the same, and only 5% expect a decrease in their anti-fraud program's technology budget.

FIG. 15 How are organizations' anti-fraud technology budgets expected to change in the next two years?

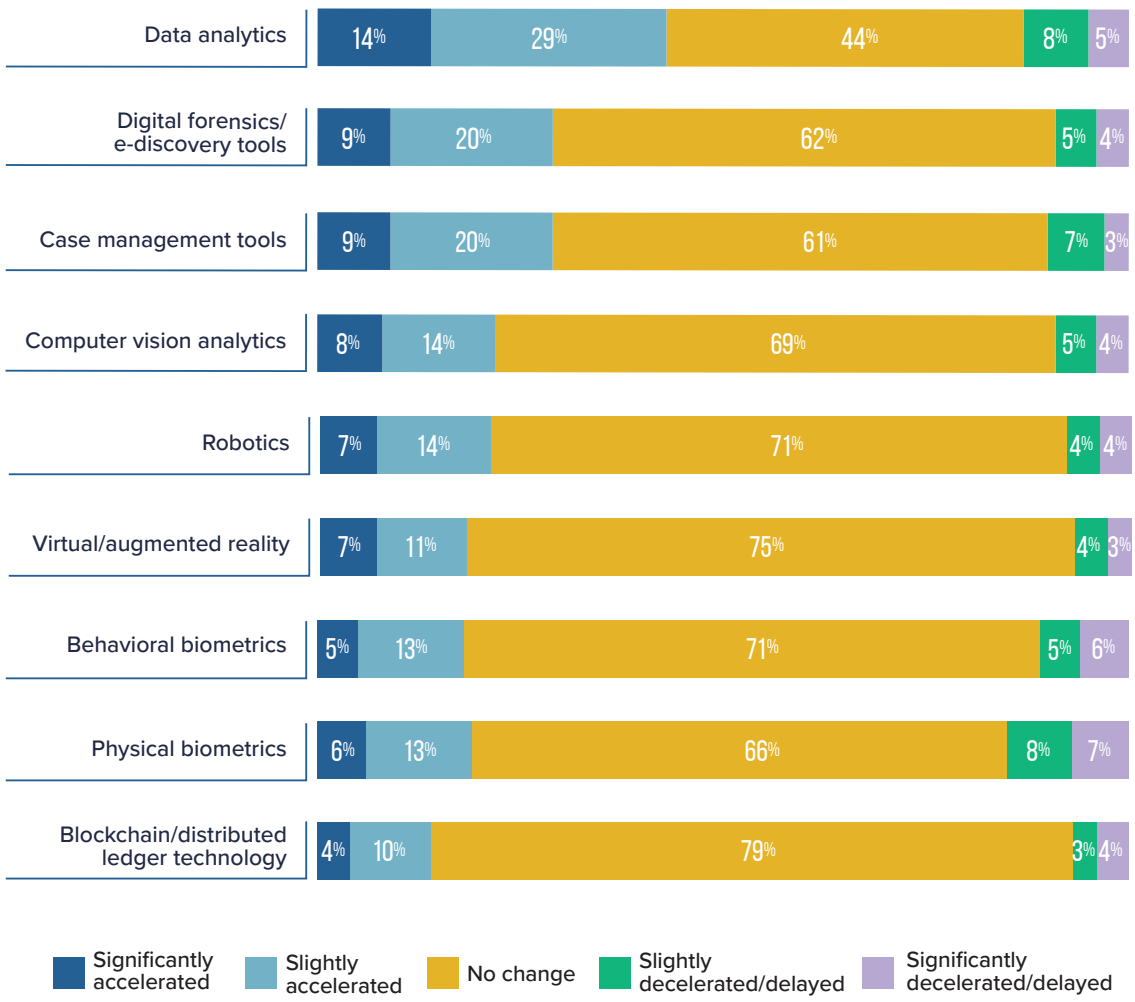


HOW HAS THE COVID-19 PANDEMIC AFFECTED ORGANIZATIONS' USE OF ANTI-FRAUD TECHNOLOGY?

The disruptions caused by the COVID-19 pandemic resulted in increased dependence on technology in many areas of individuals' lives, from remote work environments and virtual meetings to online grocery ordering and telemedicine. Both the expanded use of various technologies and the related changes in consumer and employee behavior had notable effects on organizations' fraud risks and anti-fraud programs.

We asked respondents how the pandemic affected their organizations' use of various anti-fraud technologies. More than 40% noted that their use of data analytics has accelerated either slightly (29%) or significantly (14%) throughout this time, and nearly 30% have seen an accelerated use of digital forensics/e-discovery tools and case management tools. On the opposite end of the spectrum, physical biometrics initiatives were the most negatively affected by the pandemic, with 15% of respondents seeing a decrease or delay in the use of those tools. The technology least affected by the pandemic was blockchain and distributed ledger platforms, as 79% of respondents did not see any change in their organizations' use of these technologies.

FIG. 16 How has the COVID-19 pandemic affected organizations' use of anti-fraud technology?



RESPONDENT DEMOGRAPHICS

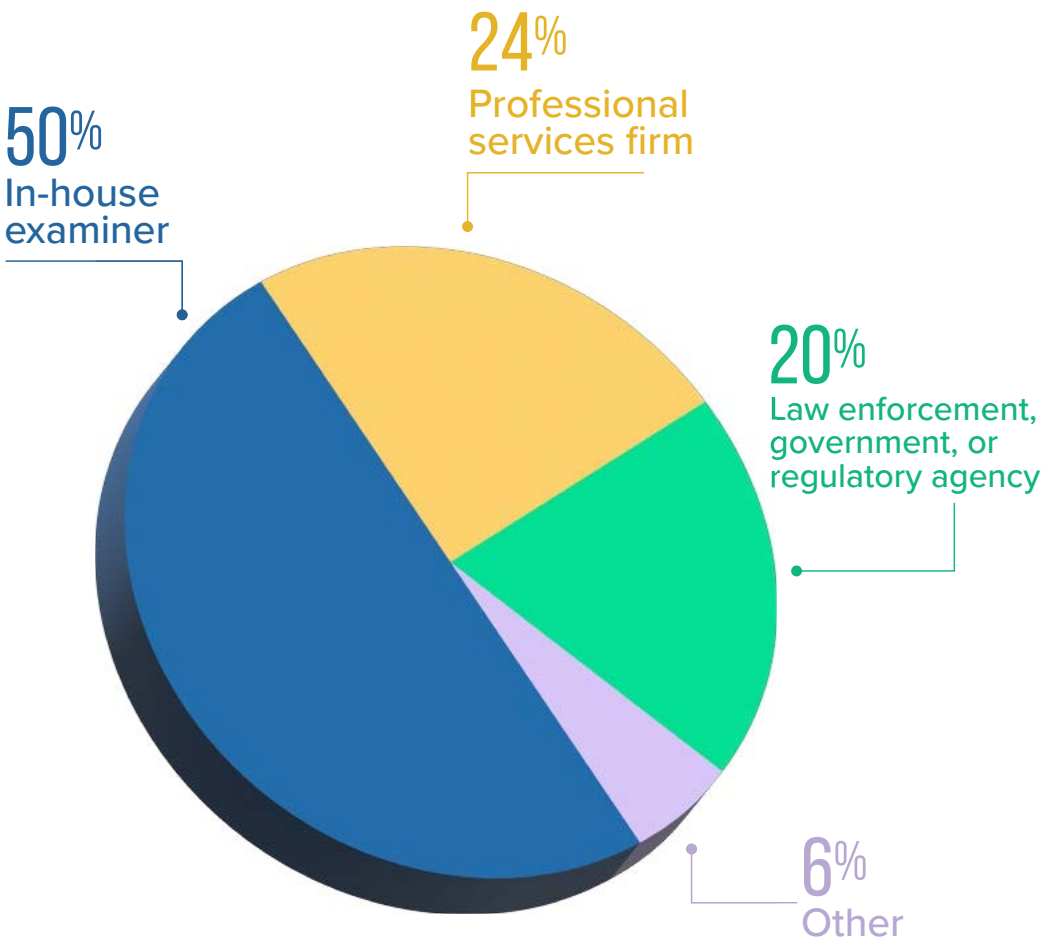
To understand the nature of how our respondents use anti-fraud technology, we asked several demographic questions as part of our survey. This information helps provide context for the findings throughout this report.

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.**

RESPONDENTS' PROFESSIONAL ROLE

Half of the respondents to our survey work in-house and conduct anti-fraud activities (e.g., internal audit, investigations, compliance, risk management) within a single organization. Another 24% work at professional services firms and conduct anti-fraud activities or engagements on behalf of clients, while 20% work for a government, regulatory, or law enforcement agency and conduct investigations or other anti-fraud engagements involving outside parties under their agency's authority. Because the respondents in these latter two categories perform engagements that affect numerous parties, their use of anti-fraud technology likely extends to other organizations, not just their employers.

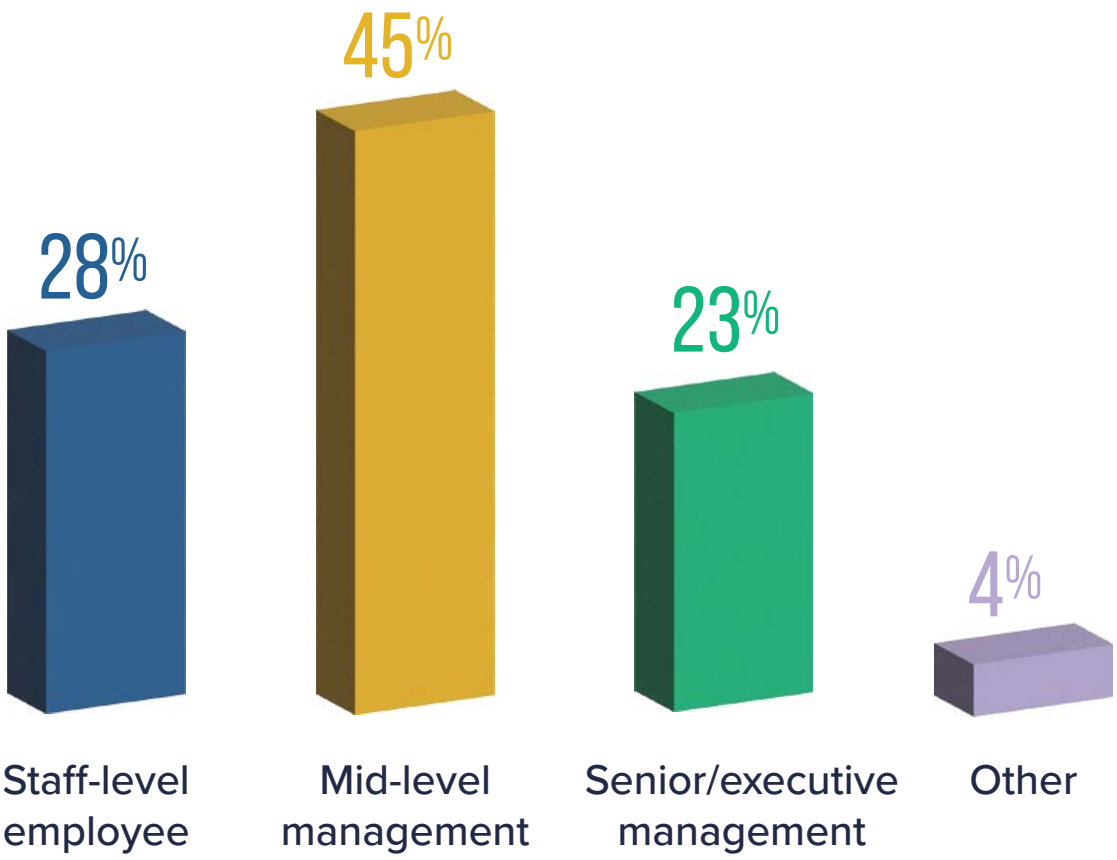
FIG. 17 Respondents' professional roles



RESPONDENTS' POSITION LEVEL

More than two-thirds of survey respondents (68%) are in managerial positions, with 45% at the mid-management level (e.g., managers and directors), and 23% at the senior or executive management level (e.g., C-suite). Respondents in these roles are likely to have additional decision-making power regarding the use of anti-fraud technology, especially as compared to the 28% of respondents who are in staff-level roles with no managerial responsibilities.

FIG. 18 Respondents' professional levels

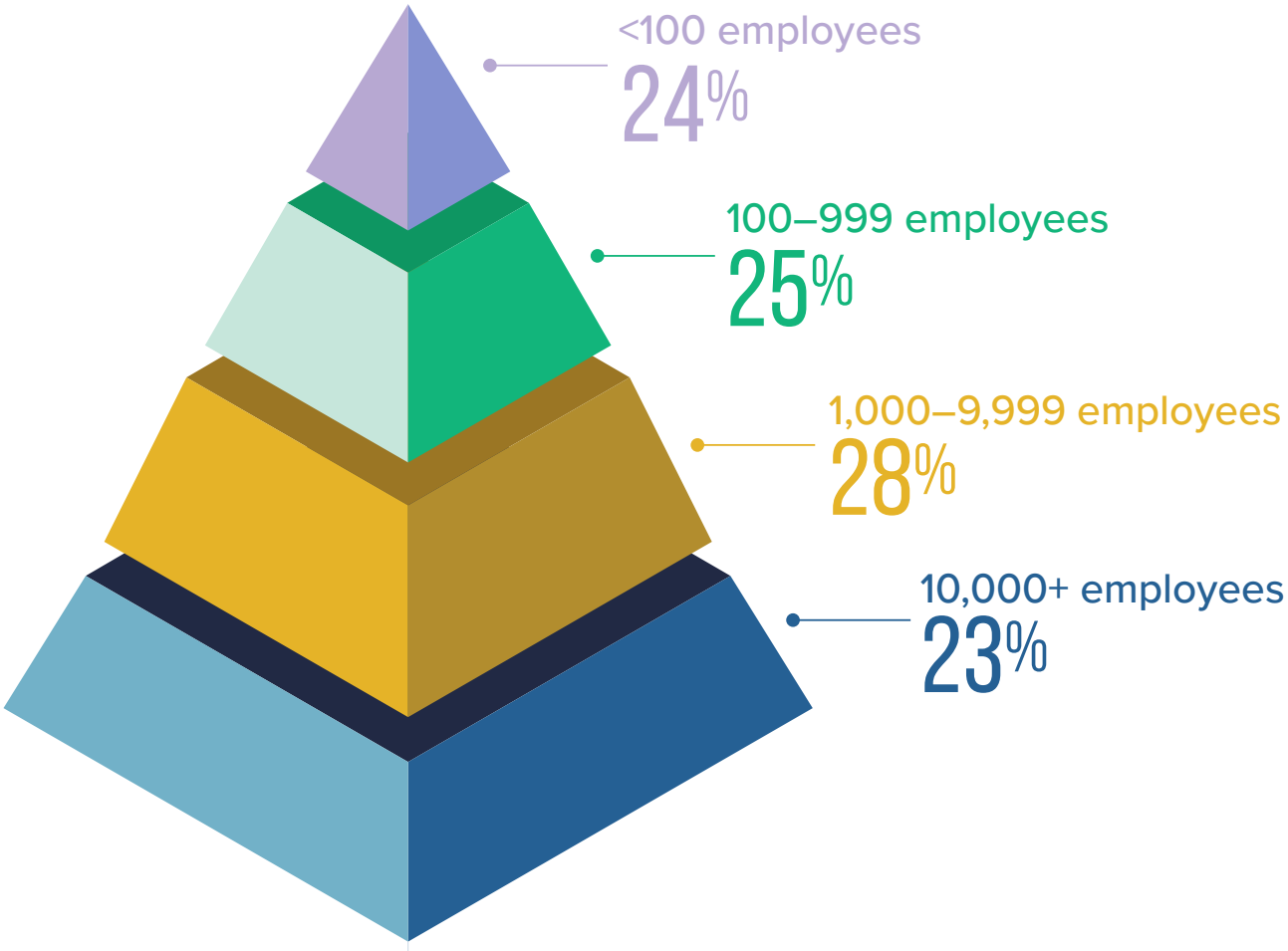


SIZE OF RESPONDENTS' ORGANIZATIONS

The strategies, needs, and resources available for anti-fraud technology can vary widely depending on the size of the organization; consequently, we asked survey participants how many employees work at their organizations to help provide additional context for our findings.

Respondents to our survey were distributed fairly evenly among organizations of differing sizes, with the largest percentage working at entities with 1,000 to 9,999 employees.

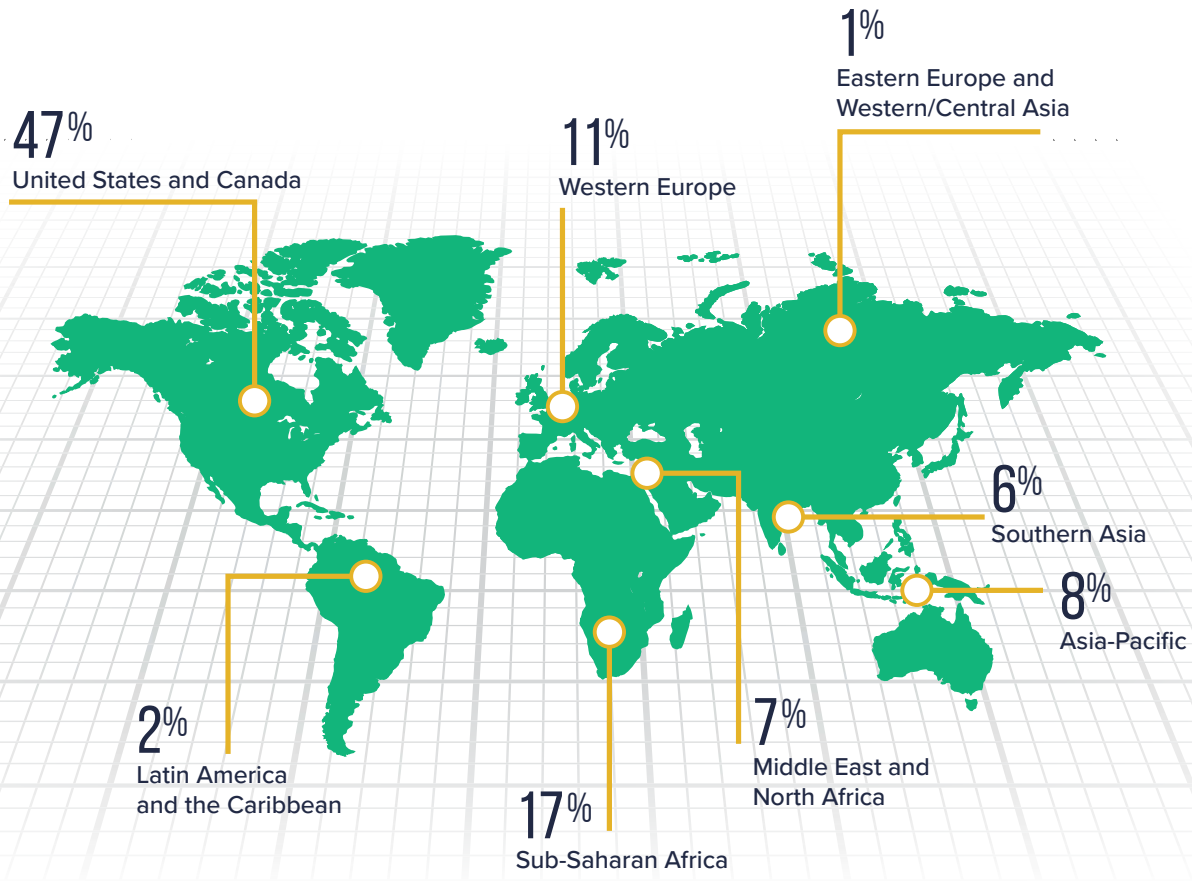
FIG. 19 Size of respondents' organizations



REGION OF RESPONDENTS' ORGANIZATIONS

Survey respondents represented organizations located throughout the world, with nearly half headquartered in the United States or Canada, 17% located in Sub-Saharan Africa, and 11% in Western Europe. The remaining quarter of participants are distributed throughout the Asia-Pacific region (8%), the Middle East and North Africa (7%), Southern Asia (6%), Latin America and the Caribbean (2%), and Eastern Europe and Western/Central Asia (1%).

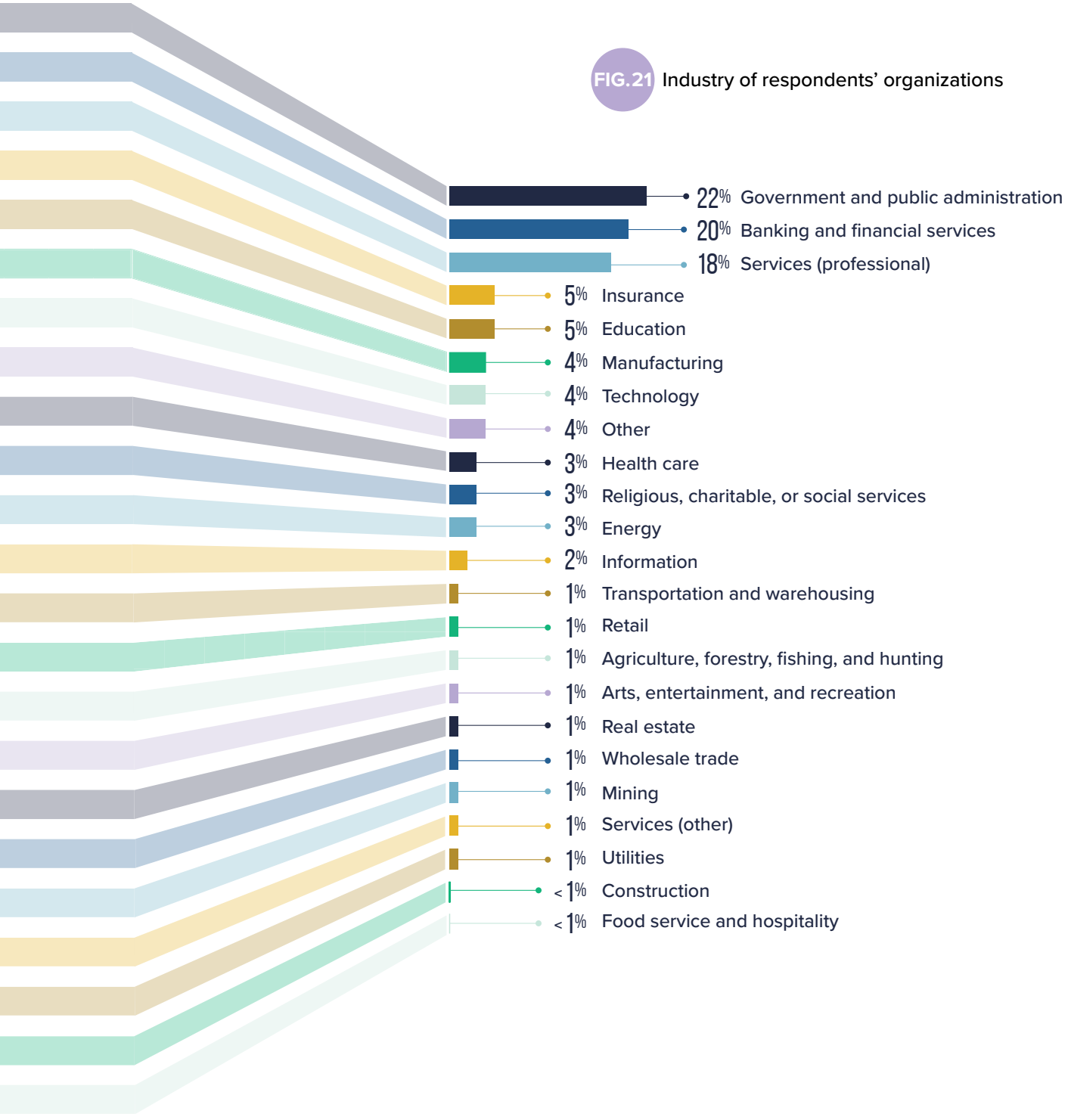
FIG.20 Region of respondents' organizations



INDUSTRY OF RESPONDENTS' ORGANIZATIONS

The industry representation of survey respondents largely reflects the overall demographics of the ACFE membership, with the largest proportions in government and public administration (22%), banking and financial services (20%), and professional services firms (18%).

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.

ABOUT SAS

SAS is the leader in analytics. Through innovative software and services, SAS empowers and inspires customers around the world to transform data into intelligence. SAS gives you THE POWER TO KNOW®. Learn more about SAS.

ACFE
Association of Certified Fraud Examiners

sas