ANTI-FRAUD TECHNOLOGY
BENCHMARKING REPORT

DEVELOPED IN PARTNERSHIP WITH

ACFE
Association of Certified Fraud Examiners
of organizations currently use exception reporting or anomaly detection techniques in their fraud-related initiatives.

AND

use automated monitoring of red flags or violations of business rules.

Over the next two years, the use of each of these types of analytics is expected to grow to 72% of organizations.

of organizations say the increased volume of transactions they can review with data analytics is very beneficial to their anti-fraud programs.

The risk areas where organizations most commonly use data analytics to monitor for potential fraud are PURCHASING (41%) AND DISBURSEMENTS (38%).

of organizations use a formal case management software program.

26% of organizations currently use biometrics as part of their anti-fraud programs, and another 16% expect to deploy biometrics as part of their programs over the next two years.
Key Findings

Only 9% of organizations currently use blockchain/distributed ledger technology or robotics as part of their anti-fraud programs.

29% of organizations currently contribute to a data-sharing consortium to help prevent and detect fraud.

And another 21% would be willing to contribute to one in the future.

55% of organizations expect to increase their budgets for anti-fraud technology over the next two years.

80% of organizations noted this factor to be a major or moderate challenge.
# Table of Contents

- Key Findings .................................................................................................................. 2
- Introduction .................................................................................................................... 5
- Methodology ................................................................................................................ 5
- How Are Organizations Using Data Analytics in Their Anti-Fraud Initiatives? ........... 6
- What Other Technologies Are Organizations Using in Their Anti-Fraud Initiatives? .... 12
- What Challenges Do Organizations Face in Implementing New Anti-Fraud Technology? .... 18
- How Are Organizations’ Anti-Fraud Technology Budgets Expected to Change in the Next Two Years? .......................................................... 20
- Respondent Demographics ......................................................................................... 22
INTRODUCTION

Technological advancements present opportunities for both fraud perpetrators and those trying to stop them. As criminals find new ways to exploit technology to commit their schemes and target new potential victims, anti-fraud professionals must ensure they are likewise adopting new technologies that are the most effective in navigating the evolving threat landscape.

But which technologies are most effective in helping organizations manage their fraud risk? Which tools provide benefits that outweigh the costs? How are organizations successfully harnessing the power of data and technology as part of their anti-fraud programs?

We know the answers to these and other questions can be crucial in gaining management buy-in and successfully implementing new anti-fraud technologies. Consequently, we conducted this benchmarking study to help organizations understand what anti-fraud technologies their peers are using and to assist in guiding future adoption of anti-fraud technologies. We hope the information contained in this benchmarking report helps organizations effectively evaluate anti-fraud technologies so that they can remain one step ahead of potential fraud perpetrators.

METHODOLOGY

In February 2019, we sent a 19-question survey to 41,181 randomly selected 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 a total of 2,255 survey responses, 1,055 of which were usable for purposes of this report. This report provides a summary of respondents’ answers to the survey questions.

The 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 readers 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 www.sas.com/fraudsurvey.
Data analytics typically refers to the use of analytics software to identify trends, patterns, anomalies, and exceptions in data. In recent years, organizations have increasingly adopted data analytics techniques and approaches to assist with marketing, customer service, brand protection, financial management, and numerous other areas, including fraud prevention and detection.
With regard to fighting fraud, a variety of techniques and technologies can be used to analyze data in order to find red flags and control gaps that might indicate the potential for misconduct. We asked survey respondents about the types of data analytics their organizations currently use as part of their anti-fraud initiatives, as well as the types of analytics they expect their organizations to adopt or deploy in the next one to two years.

As shown in Figure 1, nearly two-thirds of organizations currently use exception reporting or anomaly detection techniques in their fraud-related initiatives, and more than half have implemented automated monitoring of red flags or violations of business rules. These types of techniques are often considered among the more traditional analytic approaches and have been used in the anti-fraud field the longest of the techniques in our survey, so it stands to reason that they have been adopted by the largest percentage of organizations. Our survey data also indicates that these analytic approaches will continue to be the most common, with a total of 72% of organizations expecting to use each of these techniques over the next two years.

Data visualization and predictive analytics/predictive modeling are comparatively newer types of analytics techniques that have been or are expected to be adopted by a significant portion of organizations. In the next two years, these types of analytics are likely to be used by a cumulative 47% and 52% of organizations, respectively, as part of their anti-fraud initiatives.

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

<table>
<thead>
<tr>
<th>Technique</th>
<th>Currently use</th>
<th>Expect to adopt in next 1–2 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception reporting/anomaly detection</td>
<td>64%</td>
<td>8%</td>
</tr>
<tr>
<td>Automated red flags/business rules</td>
<td>54%</td>
<td>18%</td>
</tr>
<tr>
<td>Data visualization</td>
<td>35%</td>
<td>12%</td>
</tr>
<tr>
<td>Predictive analytics/modeling</td>
<td>30%</td>
<td>22%</td>
</tr>
<tr>
<td>Link analysis/social network analysis</td>
<td>22%</td>
<td>13%</td>
</tr>
<tr>
<td>Text mining</td>
<td>18%</td>
<td>12%</td>
</tr>
<tr>
<td>Geographic data mapping</td>
<td>16%</td>
<td>10%</td>
</tr>
<tr>
<td>Artificial intelligence/machine learning</td>
<td>13%</td>
<td>7%</td>
</tr>
<tr>
<td>Emotional tone/sentiment analysis</td>
<td>9%</td>
<td>3%</td>
</tr>
</tbody>
</table>
Our study also reveals that the use of artificial intelligence and machine learning is expected to grow considerably over the next two years. While only 13% of organizations are currently applying these technologies to prevent and detect fraud, the implementation rate is likely to almost triple in the near future as more organizations adopt this technology.

For organizations currently employing each of these techniques, we inquired about what specific software programs they use to support that initiative. Figure 2 shows the most common programs for each analytic technique. Interestingly, across all categories, a significant number of organizations are still developing their own in-house, proprietary technologies to support their anti-fraud analytics initiatives, rather than purchasing third-party tools.

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

<table>
<thead>
<tr>
<th>Exception reporting/anomaly detection</th>
<th>Automated red flags/business rules</th>
<th>Data visualization</th>
<th>Predictive analytics/modeling</th>
<th>Link analysis/social network analysis</th>
<th>Text mining</th>
<th>Geographic data mapping</th>
<th>Artificial intelligence/machine learning</th>
<th>Emotional tone/sentiment analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excel</td>
<td>In-house</td>
<td>Tableau</td>
<td>In-house</td>
<td>i2 Analysts Notebook</td>
<td>ACL</td>
<td>In-house</td>
<td>In-house</td>
<td>In-house</td>
</tr>
<tr>
<td>ACL</td>
<td>ACL</td>
<td>Excel</td>
<td>Excel</td>
<td>In-house</td>
<td>Excel</td>
<td>Tableau</td>
<td>Python</td>
<td>SAS</td>
</tr>
<tr>
<td>In-house</td>
<td>Excel</td>
<td>Power BI</td>
<td>ACL</td>
<td>SAS</td>
<td>In-house</td>
<td>Google</td>
<td>SAS</td>
<td>Excel</td>
</tr>
<tr>
<td>IDEA</td>
<td>IDEA</td>
<td>In-house</td>
<td>SAS</td>
<td>LexisNexis</td>
<td>Python</td>
<td>Excel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP</td>
<td>SAP</td>
<td>ACL</td>
<td>IDEA</td>
<td>Facebook</td>
<td>SAS</td>
<td>Power BI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In what **risk areas** do organizations use data analytics to monitor for fraud?

The decision to use data analytics to monitor for fraud within specific business functions and operations often varies based on numerous factors, including access to data, technological or process limitations, and assessed level of risk. We asked respondents to note the risk areas for which their organizations currently use data analytics or automated monitoring tools to identify red flags of potential fraud. In general, organizations are proactively monitoring their data across numerous fraud risk areas, with the most prominent being purchasing (41%), disbursements (38%), fraud by customers/first-party fraud (35%), and travel and entertainment (34%).

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

![Bar chart showing the percentage of organizations using data analytics in various risk areas:
- Purchasing: 41%
- Disbursements: 38%
- Fraud by customers/first-party fraud: 35%
- Travel and entertainment: 34%
- Financial reporting fraud: 31%
- Receipts/incoming payments: 31%
- Money laundering: 31%
- Payroll: 30%
- Fraud committed by vendors/contractors: 30%
- Hacking/unauthorized user access/third-party fraud: 23%
- Corruption and bribery: 22%
- Inventory: 20%]
WHAT SOURCES OF DATA DO ORGANIZATIONS USE IN THEIR ANTI-FRAUD DATA ANALYTICS INITIATIVES?

Obtaining a full picture of potentially fraudulent activity often involves gathering and analyzing data from multiple sources. Nearly three-quarters of the organizations in our study use internal structured data to conduct their anti-fraud analytics tests, making this by far the most common data source. In contrast, only 30% of organizations use internal unstructured data, and 26% gather data from employee devices that are connected to the organization’s network. Some organizations are also bringing in data from outside sources, such as public records (43%), government watch lists (32%), social media (29%), and other third-party data sources (27%).

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 attempting to implement new anti-fraud technologies, obtaining management buy-in can be a challenge for many organizations. Part of overcoming this challenge involves being able to articulate and prove the benefits that such technology can provide. For survey respondents who are currently employing data analytics in their anti-fraud programs, we asked how beneficial the use of this technology has been with regard to the following considerations:

- Volume, enabling them to review more transactions and identify more cases of suspected fraud
- Accuracy, resulting in a reduced false-positive rate
- Efficiency, by automating time-consuming tasks
- Timeliness, allowing them to detect anomalies more quickly

Figure 5 shows that the vast majority of organizations experience substantial benefits from their use of anti-fraud analytics, with 83% to 90% of organizations rating their analytics programs as being either very beneficial or fairly beneficial in each of these four areas. The top benefit realized pertains to volume: 64% of survey respondents said the increased volume of transactions they can review using data analytics is very beneficial to their anti-fraud programs.

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?

In addition to data analytics, numerous other types of technologies can be used to improve an organization’s ability to effectively and efficiently combat fraud. To help organizations assess their full anti-fraud technology toolkit and to provide insight into other organizations’ use of various anti-fraud software programs, we collected data about the types of case management, digital forensics, online-evidence capturing, and other emerging technologies used by the organizations in our study.
Part of effectively managing fraud cases involves being able to track and report on the results of all the organization’s fraud investigations. Our data indicates that only 39% of organizations currently use a formal case management software program. Within those organizations, it is most common to use an in-house developed, proprietary program. Others use a variety of third-party programs.

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

- Yes: 39%
- No: 61%

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

- ThoughtSpan
- Polonious
- LexisNexis CaseMap
- RSA Archer
- In-House
- Actimize
- Encase
- Convercent
- VERAFIN
- EthicsPoint
- AccessData
- BAE Systems
- Business Objects
- NERA
- Lotus Notes
- LightHouse System
The use of digital forensics and e-discovery software is not common among the organizations in our study. Only approximately one-quarter of survey respondents indicated that their organizations have adopted such a program. Of those that have, EnCase is the most common, followed by AccessData’s Forensic Toolkit.

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

- Yes: 26%
- No: 74%

**FIG. 9** What are the most common digital forensics/e-discovery software programs?
As shown in Figure 10, many organizations collect data from online sources as part of their anti-fraud initiatives. The collection of online evidence often implicates privacy, verification, and retention considerations that are not present when an organization captures or analyzes its own internal data. Because of the specialized nature of this type of data collection, various software programs have been developed to assist with collecting, documenting, and preserving online evidence. However, our study shows that the use of this type of software is still relatively uncommon, with just 30% of organizations employing online-evidence capturing programs. Of those that do, many have developed their own in-house, proprietary programs.

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

FIG. 11 What are the most common online-evidence capturing software programs?
We asked survey respondents about their organizations’ current and expected use of several emerging technologies as part of their anti-fraud initiatives; their responses are reflected in Figure 12. The most common of these technologies currently being used to fight fraud is biometrics (e.g., fingerprint, facial, or keystroke recognition), with more than one-quarter already using such techniques and another 16% expecting to employ biometrics within the next two years. Both blockchain/distributed ledger technology and robotics, including robotic process automation, are currently used less frequently than biometrics (9% of organizations for both categories), but a similar proportion of organizations expect to implement these technologies in the next two years. The technology least likely to be adopted as part of anti-fraud programs is virtual or augmented reality; only 6% of organizations currently use this technology, and nearly two-thirds of the organizations in our study do not expect to employ virtual or augmented reality as part of their anti-fraud initiatives.

**FIG. 12 What emerging technologies are organizations using to fight fraud?**
Some industries and groups have established data-sharing consortiums, in which they feed certain data into an aggregated database that all member organizations can access. These initiatives are designed to help member organizations benefit from the collective data of the consortium in order to identify trends and protect themselves from known threats.

Of the organizations in our study, 29% currently contribute to such a consortium, and another 21% would be willing to contribute in the future. However, half of the respondents indicated that they do not have any plans to participate in a data-sharing consortium to help prevent and detect fraud. Sharing data in this way can provide large benefits, but there are numerous reasons organizations might opt out of such initiatives, such as privacy concerns and logistical challenges in disclosing their data to other organizations.
What Challenges Do Organizations Face in Implementing New Anti-Fraud Technology?

While technological advancements can bring many benefits, adopting new technology often comes with challenges and potential barriers to success. Anti-fraud technology is no different.
We asked survey respondents how significant several common issues are when attempting to adopt new anti-fraud technology at their organizations. Figure 14 shows that budget and financial concerns are the biggest obstacle for many organizations, with 80% noting this factor to be a major or moderate challenge. Other common challenges include limitations in staffing and in-house skill sets (73%), concerns about poor data quality or integration issues (70%), and a lack of perceived return on investment (69%).

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

---

**BUDGET AND FINANCIAL CONCERNS ARE THE BIGGEST OBSTACLE FOR MANY ORGANIZATIONS.**
How Are Organizations’ Anti-Fraud Technology Budgets Expected to Change in the Next Two Years?
While financial restrictions are a significant challenge for a large percentage of organizations when it comes to implementing new anti-fraud technology (see Figure 14), there is some good news. Of the organizations in our study, 55% expect to increase their budgets for anti-fraud technology over the next two years—17% significantly and 38% slightly. Another 40% expect to have their budgets for such technology remain level. Only 6% of the organizations anticipate having their financial resources for anti-fraud technology reduced over the next two years.

**FIG. 15 How are organizations’ anti-fraud technology budgets expected to change in the next two years?**
Respondent Demographics
To understand the nature of how our respondents use anti-fraud technology, we asked about their specific anti-fraud roles. This information helps provide context for the findings in this report.

More than half (55%) of the respondents to our survey stated that they work in-house and conduct fraud prevention, detection, or investigation activities within a single company or agency, meaning that their use of anti-fraud technology likely affects only their employing organization. In contrast, 23% of respondents work for a professional services firm that performs anti-fraud engagements on behalf of other entities, and one-fifth work for a government, regulatory, or law enforcement agency that conducts fraud investigations involving outside parties. Respondents in the latter two categories likely use anti-fraud technology in ways that pertain to their clients or investigation targets, meaning their use affects numerous organizations, not just their employers.

FIG. 16 Respondents’ professional roles
Resources and budgets can vary widely by organization size, so understanding how many employees the respondents’ organizations have can be helpful for context in analyzing the use of anti-fraud technology. Figure 17 shows that respondents’ organizations were fairly evenly distributed among size categories, with a slightly larger proportion (29%) working at organizations with 1,000 to 9,999 employees.

FIG. 17 Size of respondents' organizations
We asked survey respondents about the geographical location of their organizations’ headquarters. As noted in Figure 18, nearly half of the organizations in our study are located in the U.S., while 13% are in Western Europe, and 12% are in Sub-Saharan Africa.

FIG. 18 Region of respondents’ organizations
INDUSTRY OF RESPONDENTS’ ORGANIZATIONS

The pervasiveness and types of technology used can vary across industries, and organizational leaders often wish to benchmark their own programs against other entities in the same sector. Consequently, we asked survey respondents to identify the primary industry of their employing organization. The top three industries covered by our survey responses were banking and financial services (21%), government and public administration (17%), and professional services (16%).

FIG. 19 Industry of respondents’ organizations

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 www.sas.com/fraudsurvey.
SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 83,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®.

The ACFE and SAS would like to thank Capgemini and Intel for their supporting sponsorship of this report.
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 85,000 members in more than 180 countries, the ACFE is reducing business fraud worldwide and providing the training and resources needed to fight fraud more effectively.

The ACFE provides educational tools and practical solutions for anti-fraud professionals through events, education, publications, networking, and educational tools for colleges and universities.

Certified Fraud Examiners
The ACFE offers its members the opportunity for professional certification with the Certified Fraud Examiner (CFE) credential. The CFE is preferred by businesses and government entities around the world, and indicates expertise in fraud prevention and detection. CFEs are anti-fraud experts who have demonstrated knowledge in four critical areas: Financial Transactions and Fraud Schemes, Law, Investigation, and Fraud Prevention and Deterrence.

Membership
Members of the ACFE include accountants, internal auditors, fraud investigators, law enforcement officers, lawyers, business leaders, risk/compliance professionals, and educators, all of whom have access to expert training, educational tools, and resources. Whether their career is focused exclusively on preventing and detecting fraudulent activities or they just want to learn more about fraud, the ACFE provides the essential tools and resources necessary for anti-fraud professionals to accomplish their objectives.

To learn more, visit ACFE.com or call (800) 245-3321 / +1 (512) 478-9000.

Contact
Association of Certified Fraud Examiners Global Headquarters
716 West Ave | Austin, TX 78701-2727 | USA
Phone: (800) 245-3321 / +1 (512) 478-9000
ACFE.com | info@ACFE.com

© 2019 Association of Certified Fraud Examiners, Inc. All rights reserved.