2026 ANTI-FRAUD TECHNOLOGY BENCHMARKING REPORT

The use 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.

To aid in this endeavor, the Association of Certified Fraud Examiners (ACFE), in partnership with SAS, created the 2026 *Anti-Fraud Technology Benchmarking Report*. Now in its fourth edition, this report examines how organizations use technology to detect and prevent fraud, the challenges they face when implementing new tools and how emerging technologies like artificial intelligence (AI) are shaping the future of anti-fraud programs.

The report provides insights into opportunities and vulnerabilities presented by technologies, benchmarking of anti-fraud programs' technology, and how to prepare for future technological developments with fraud resilience at the forefront.

KEY FINDINGS

7%

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

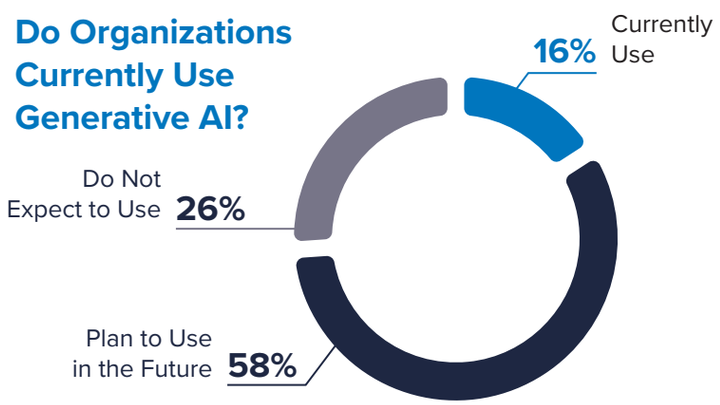
These schemes have increased the most over the past two years:

- **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%)**

ACFE Association of Certified Fraud Examiners | SAS

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.

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.



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

10%



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

29%

DOWNLOAD THE FULL REPORT

to explore how organizations are adapting their fraud prevention strategies and where anti-fraud technology is headed next.

ACFE Association of Certified Fraud Examiners | sas