HOW IS **TECHNOLOGY** BEING USED TO FIGHT FRAUD?

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

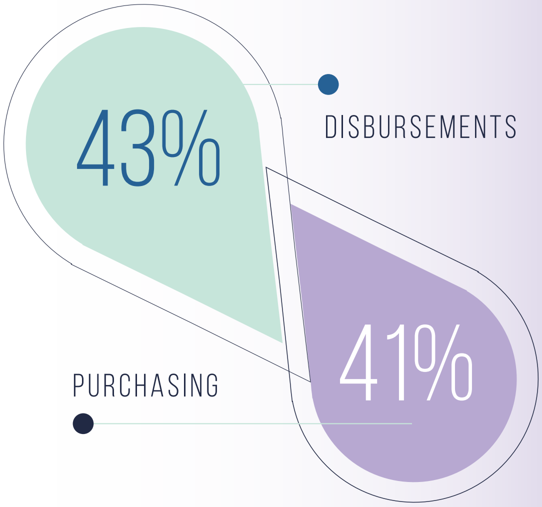
in anti-fraud programs is expected to more than

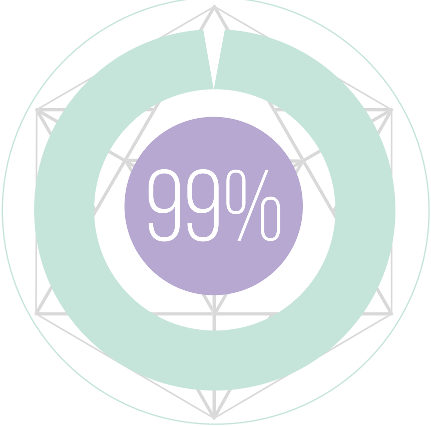
DOUBLE

over the next two years.

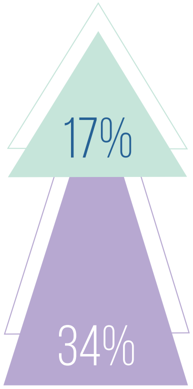
The risk areas where organizations most commonly use **data analytics to monitor for potential fraud** are

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.

HOW IS **TECHNOLOGY** BEING USED TO FIGHT FRAUD?

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.

ACFE®
Association of Certified Fraud Examiners

Source: ACFE Anti-Fraud Technology Benchmarking Report, 2022