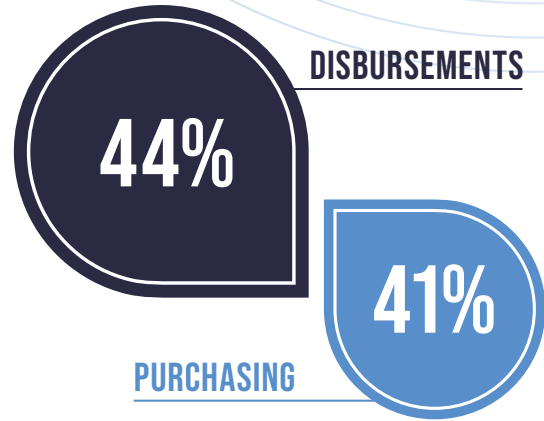




Nine in 10 organizations (91%) use **DATA ANALYSIS TECHNIQUES** as part of their anti-fraud programs.



The most common risk areas monitored by data analytics are

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

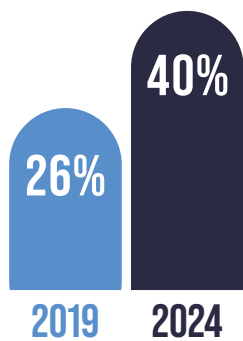


INTERNAL STRUCTURED DATA

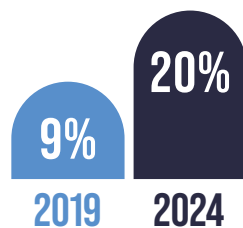
is the most common source of data for analysis, with 77% of organizations relying on this traditional approach.

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%

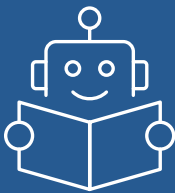
OF ORGANIZATIONS

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.