

Presentation of ACFE findings in view of Fraud Awareness Week 2021 (14-20 November 2021)



Edited by

Professor Dimitrios v. Skiadas, *LLB, Mjur, PhD, CFE*



**JEAN MONNET CHAIR
EU BUDGETARY GOVERNANCE
AND AUDIT**

Co-funded by the
Erasmus+ Programme
of the European Union
2017-2020

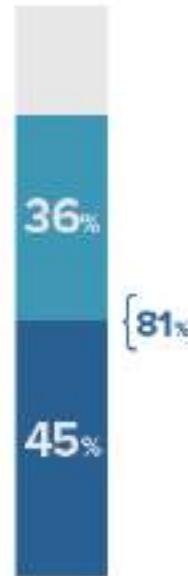


Cyberfraud and COVID-19

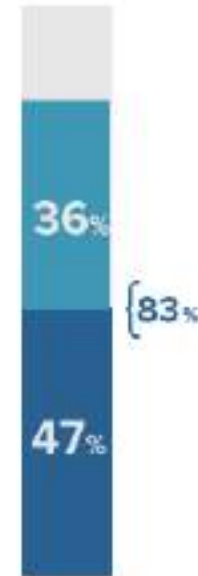
How anti-fraud professionals view cyberfraud risks

At the start of the COVID-19 pandemic, anti-fraud professionals reported seeing a rise in cyberfraud, which steadily increased as the pandemic continued.

Observed as of May 2020



Observed as of August 2020



Observed as of November 2020



Significant increase

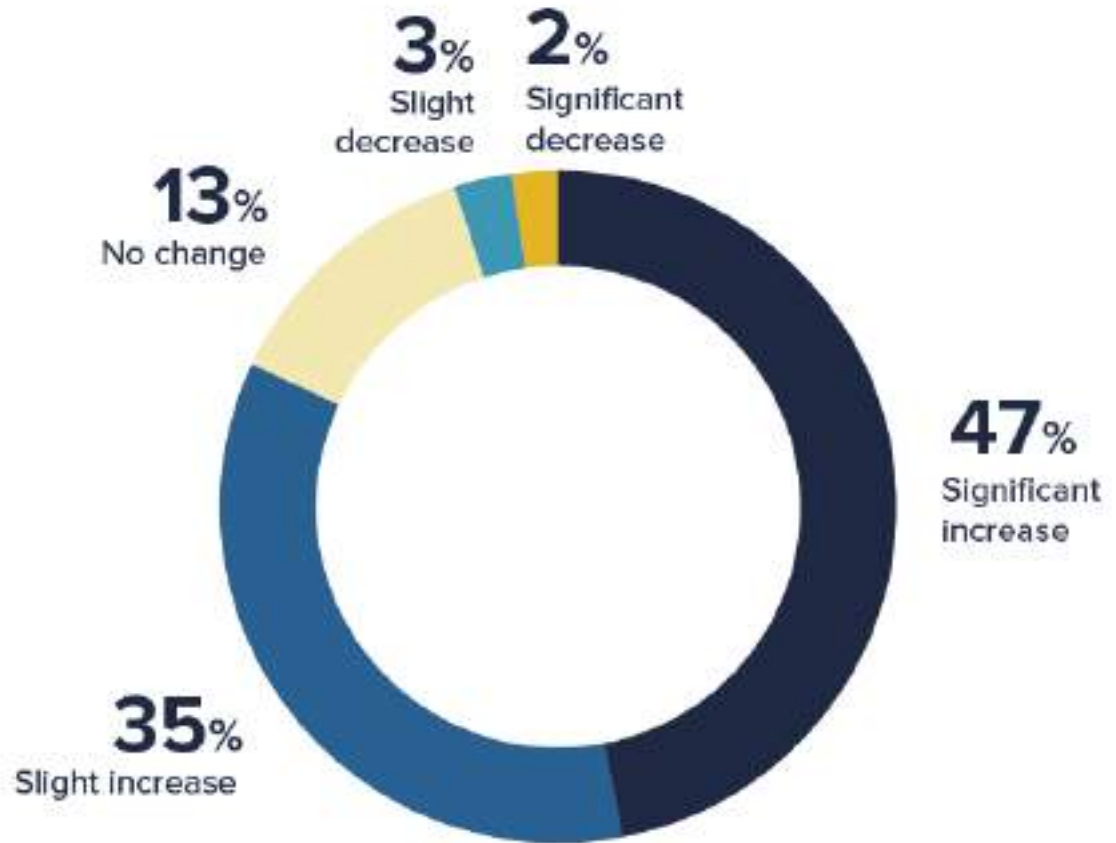
Slight increase

Cyberfraud and COVID-19

How anti-fraud professionals view cyberfraud risks

82%

expect to see **an increase** in cyberfraud in the coming year.¹



1. Through May 2022.

Cyberfraud and COVID-19

How anti-fraud professionals view cyberfraud risks

More than
a third

of anti-fraud professionals reported that cyberfraud-related issues pose a challenge for their organization's anti-fraud programs.


Challenges maintaining
data privacy/security



Inability to proactively identify and
mitigate emerging threats



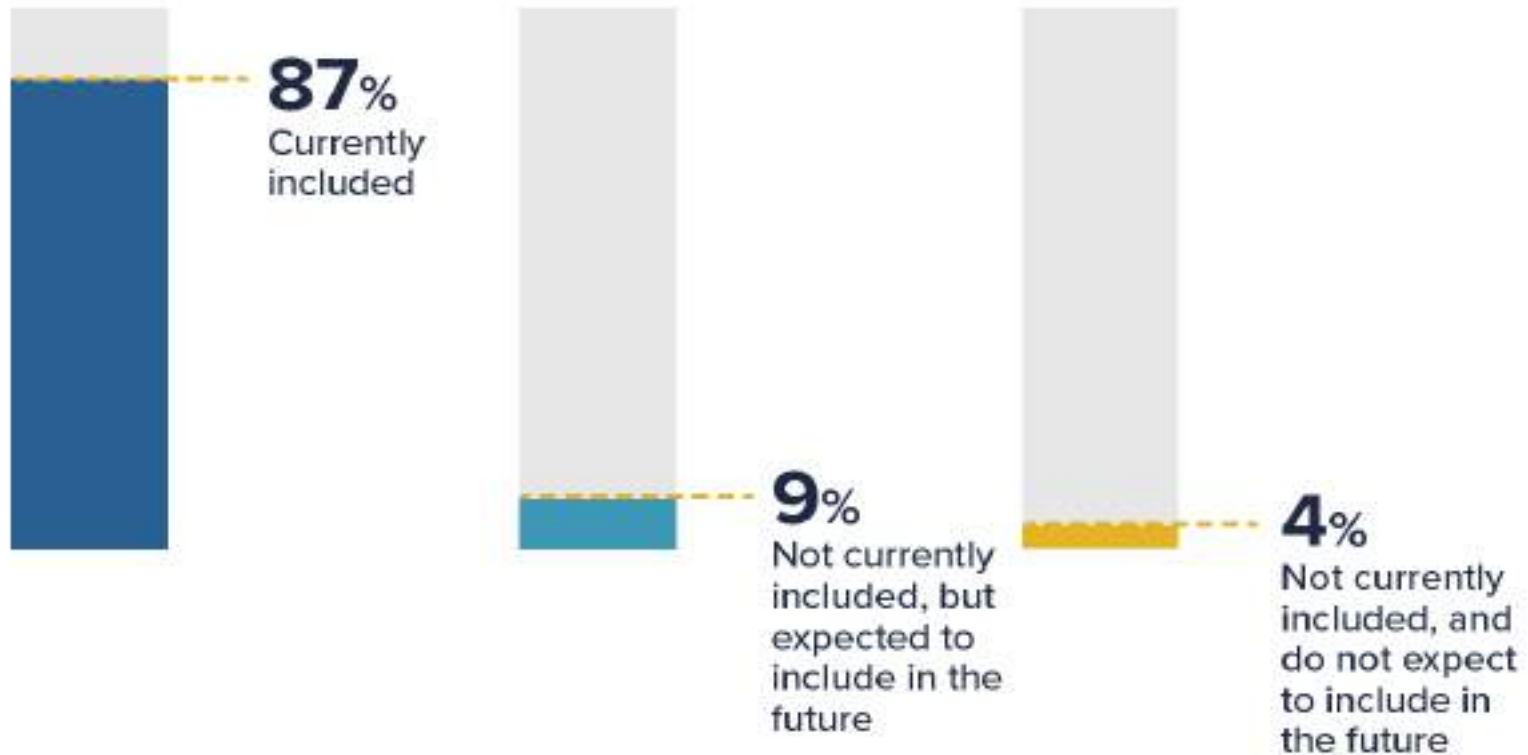
 Current challenge

 Expect to remain a challenge

Cyberfraud and COVID-19

How anti-fraud professionals view cyberfraud risks

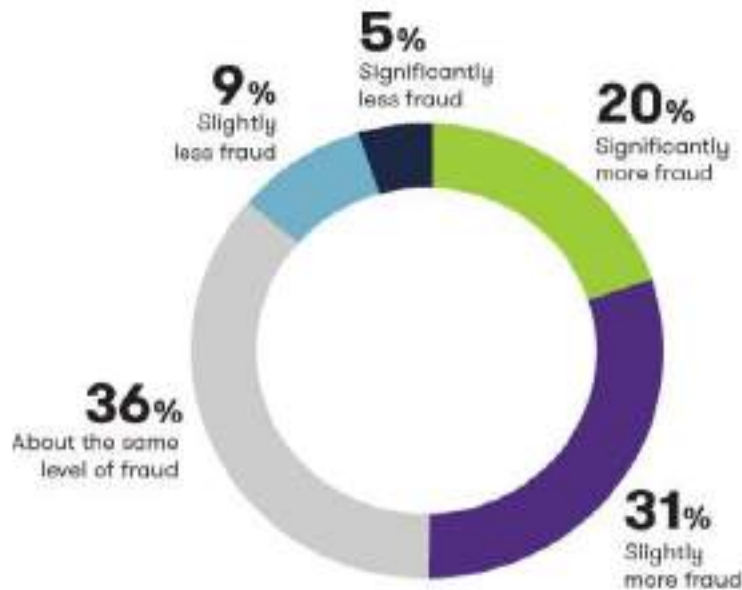
87% said they currently cover cyberfraud in their fraud awareness training, while **9%** said they plan to include it in the future.



The next normal: Preparing for a post-Pandemic fraud landscape

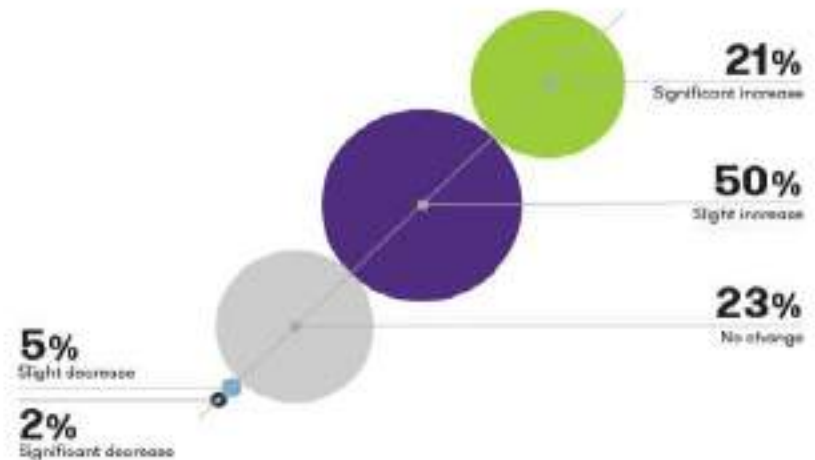
How the COVID-19 pandemic has affected the level of fraud and how organizations are tackling it

Change in the amount of fraud uncovered



51% of organizations have **uncovered more fraud** since the onset of the pandemic

Expected change in the overall level of fraud impacting organizations

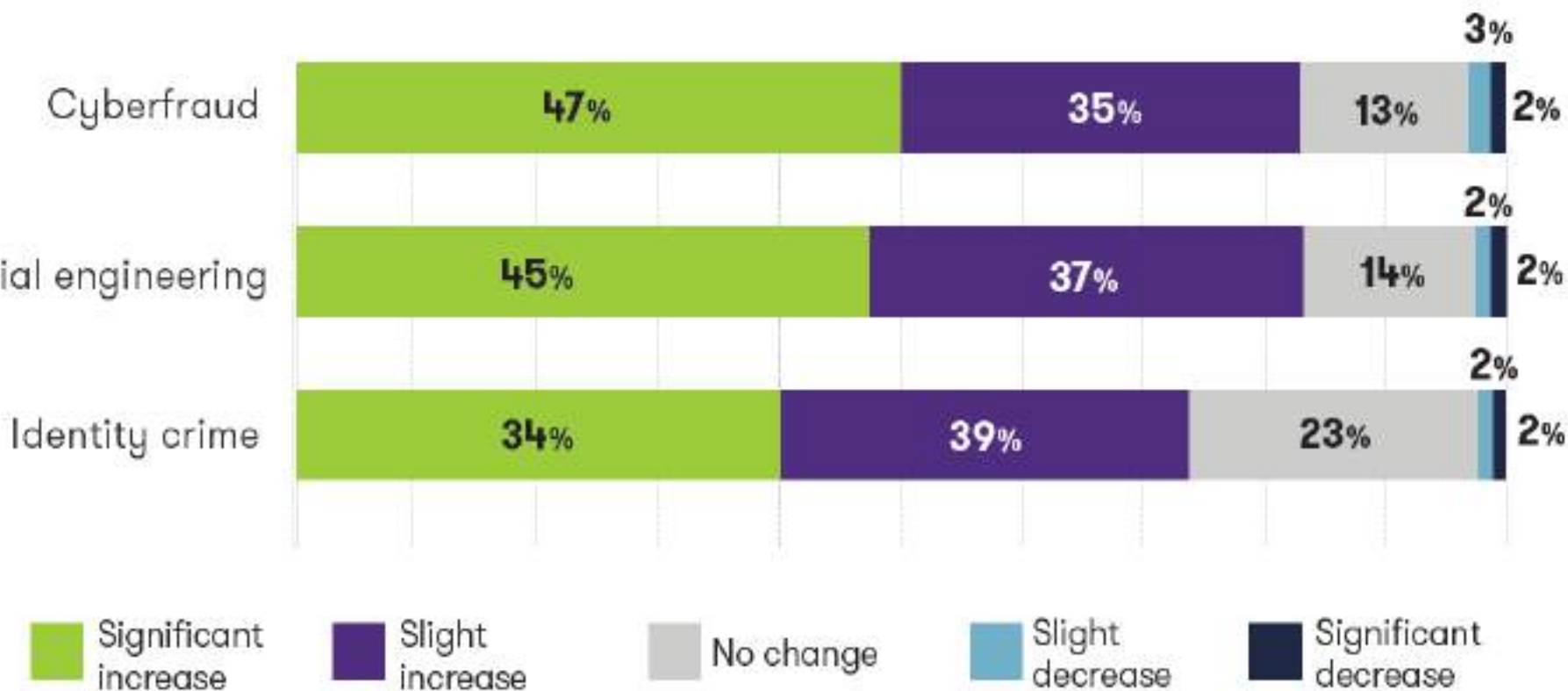


71% expect the **level of fraud** impacting their organizations to **increase** over the next year

The next normal: Preparing for a post-Pandemic fraud landscape

How the COVID-19 pandemic has affected the level of fraud and how organizations are tackling it

Expected change in specific fraud risks over the next 12 months*



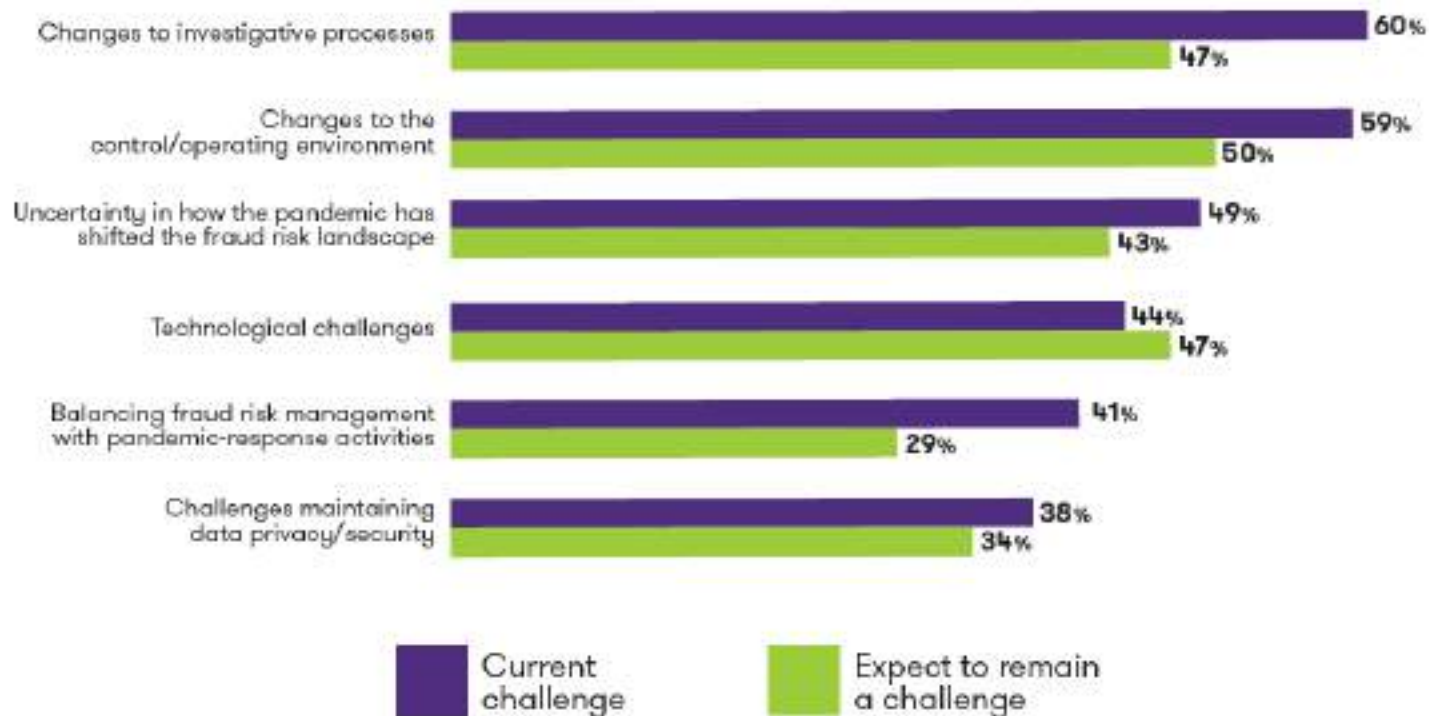
*12 months from June 2021

The next normal: Preparing for a post-Pandemic fraud landscape

How the COVID-19 pandemic has affected the level of fraud and how organizations are tackling it

Top challenges facing anti-fraud programs include changes to investigative processes and changes to the control/operating environment.

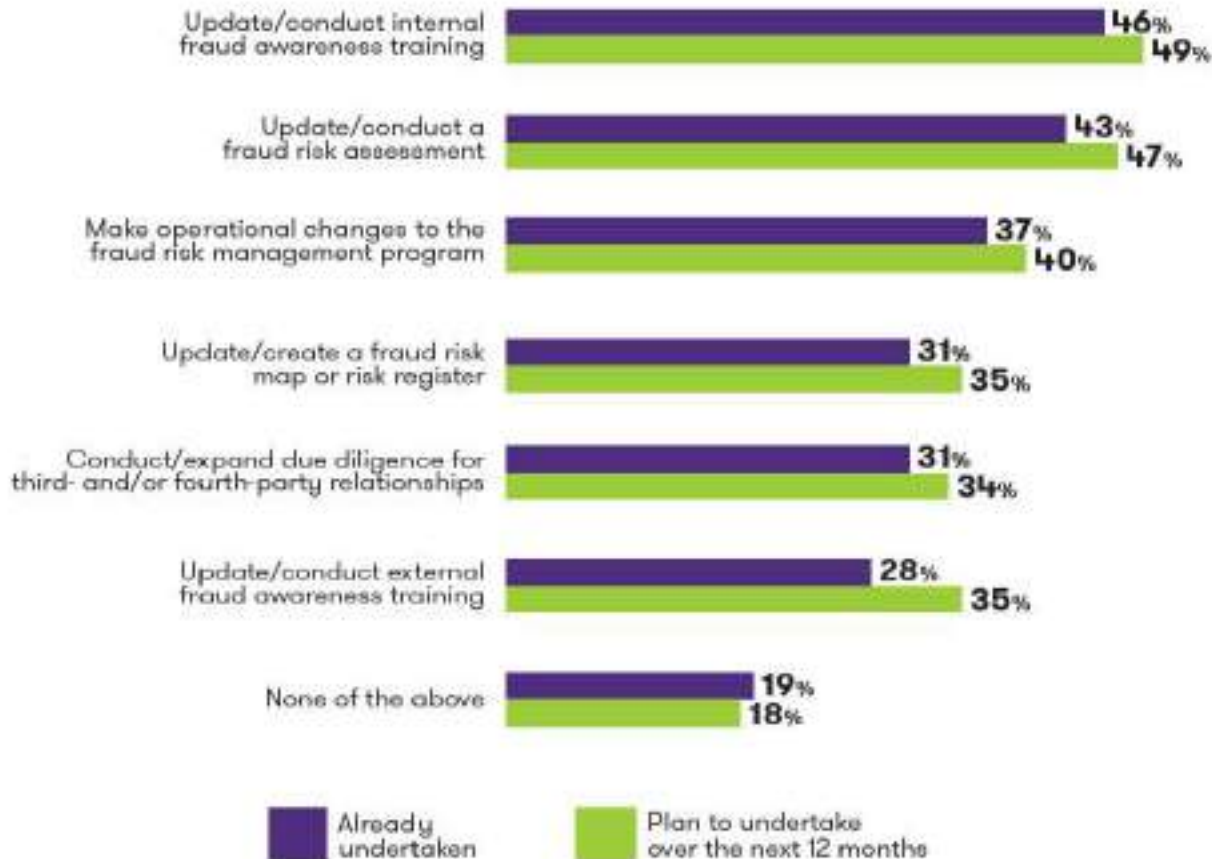
Top challenges facing anti-fraud programs



The next normal: Preparing for a post-Pandemic fraud landscape

How the COVID-19 pandemic has affected the level of fraud and how organizations are tackling it

Changes to anti-fraud programs



More than 80% of organizations have already implemented one or more changes to their anti-fraud programs in response to the pandemic.

Behavioral Red Flags of Fraud

Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses

85%

OF ALL FRAUDSTERS displayed at least one **BEHAVIORAL RED FLAG** while committing their crimes.

7 KEY WARNING SIGNS



42%

Living beyond means



26%

Financial difficulties



19%

Unusually close association with vendor/customer



15%

Control issues, unwillingness to share duties



13%

Irritability, suspiciousness, or defensiveness



13%

"Wheeler-dealer" attitude



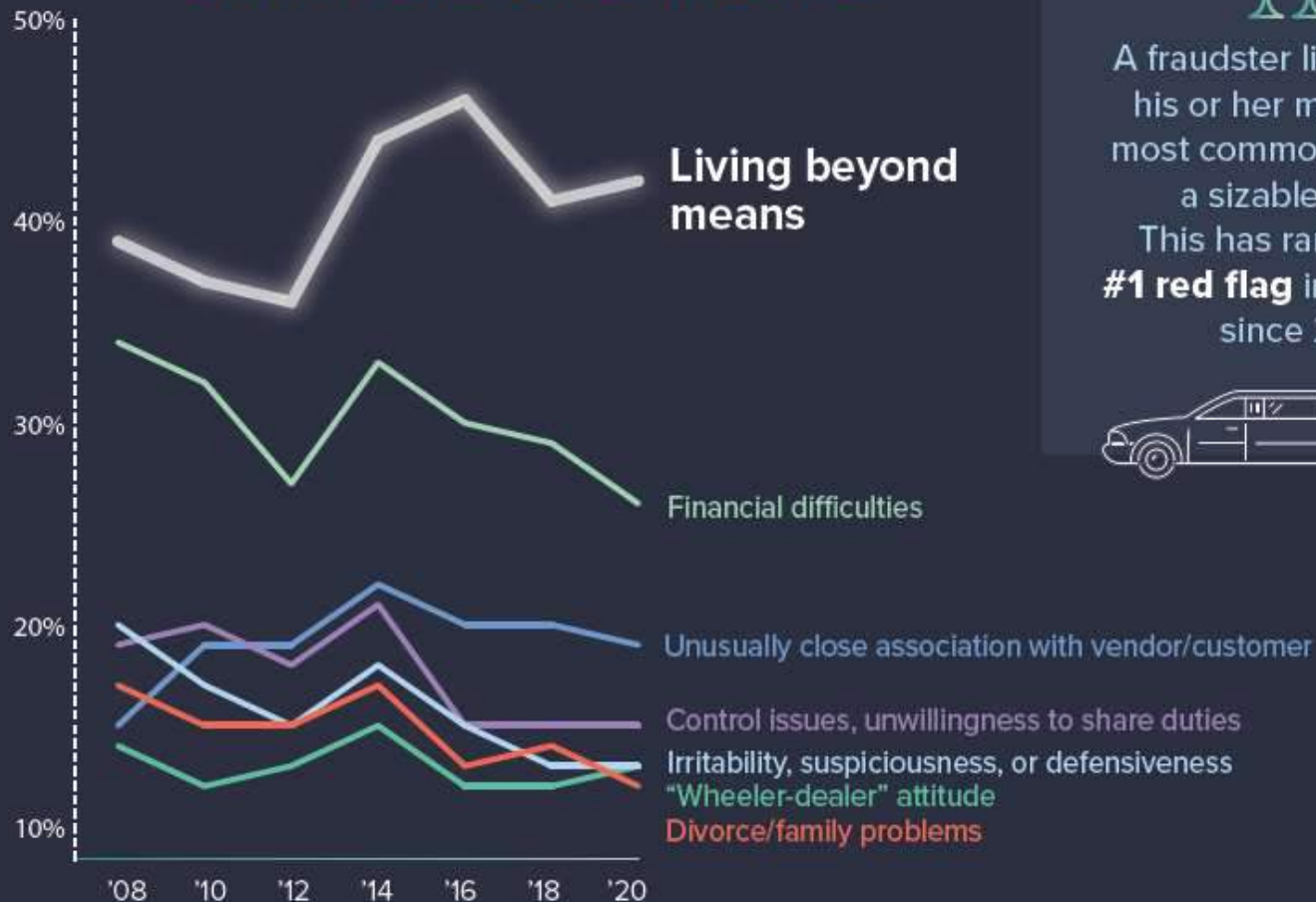
12%

Divorce/family problems

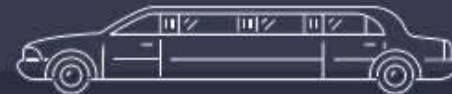
Behavioral Red Flags of Fraud

Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses

LIVING BEYOND MEANS



A fraudster living beyond his or her means is the most common red flag by a sizable margin. This has ranked as the **#1 red flag** in every study since 2008.



Behavioral Red Flags of Fraud

Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses

CLASSIFYING RED FLAG BEHAVIORS

In **52%** of cases, the fraudster exhibited red flags connected to their **work duties**



JOB PERFORMANCE AS A WARNING SIGN

A fraud perpetrator's job performance will often suffer while the scheme is taking place. Each of these performance-related issues were cited in at least 10% of cases.

In **63%** of cases, the fraudster exhibited red flag behavior associated with his or her **personal life**.



13%

POOR PERFORMANCE EVALUATIONS



13%

EXCESSIVE ABSENTEEISM



12%

FEAR OF JOB LOSS



12%

EXCESSIVE TARDINESS



10%

DENIED RAISE OR PROMOTION

Response to Fraud

Organizations can respond to fraud internally, through civil litigation, and by referring the case to law enforcement - These are the results of such efforts



Profile of a Fraudster

ACFE's study includes perpetrator data from more than 2,000 fraud cases, which can help organizations assess fraud risk in their own workforces

GENDER

Males committed more frauds and caused higher losses.

MALE



\$150,000
Median loss



FEMALE

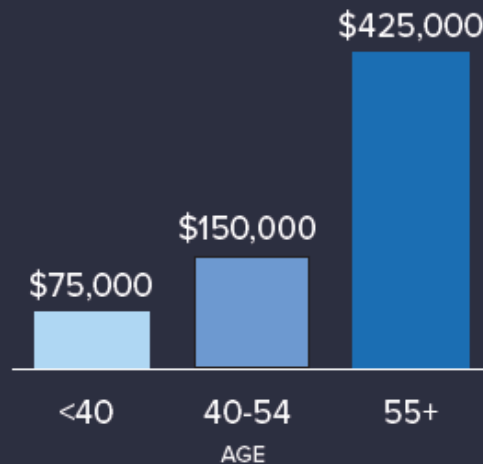


\$85,000
Median loss



AGE

Older fraudsters caused much larger median losses



EDUCATION



64% of occupational fraudsters had a university degree or higher.

No university degree

\$100,000 MEDIAN LOSS

University degree or higher

\$195,000 MEDIAN LOSS

Profile of a Fraudster

ACFE's study includes perpetrator data from more than 2,000 fraud cases, which can help organizations assess fraud risk in their own workforces



How is Technology being used to fight fraud?

NEARLY
2/3 of organizations currently use **exception reporting or anomaly detection techniques** in their fraud-related initiatives

AND

MORE THAN
1/2 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.

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.



of organizations use a formal **case management software program.**

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

PURCHASING (41%)

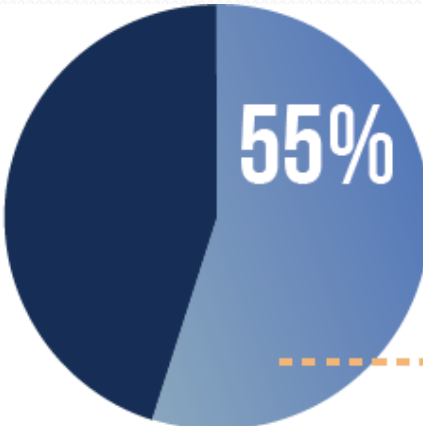
AND

DISBURSEMENTS (38%).



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.

How is Technology being used to fight fraud?



OF ORGANIZATIONS EXPECT TO **INCREASE** THEIR BUDGETS FOR **ANTI-FRAUD TECHNOLOGY** OVER THE NEXT TWO YEARS.

Budget and financial concerns

are the biggest obstacle for many organizations in adopting new anti-fraud technology;



80%

of organizations noted this factor to be a

major
or

moderate challenge.

ONLY **9%** OF ORGANIZATIONS CURRENTLY USE **BLOCKCHAIN/ DISTRIBUTED LEDGER TECHNOLOGY** OR **ROBOTICS** AS PART OF THEIR ANTI-FRAUD PROGRAMS.



THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING AS PART OF ORGANIZATIONS' ANTI-FRAUD PROGRAMS IS EXPECTED TO ALMOST

TRIPLE

Three stylized blue robot figures standing in a row against a dark blue background with vertical lines.

OVER THE NEXT TWO YEARS.



SOURCES:



- The infographics are available by ACFE at <https://fraudweek.com/fraudweek/resources>
- ACFE Fraud in the Wake of COVID-19 - Benchmarking Report: December 2020 Edition
- The ACFE and Grant Thornton's Report, The Next Normal: Preparing for a Post-Pandemic Fraud Landscape
- ACFE Fraud Awareness Training Benchmarking Report
- ACFE Anti-Fraud Technology Benchmarking Report , 2019