Grant Thornton

Session # 2

Unicorns and Camels

Navigating the Fraudtech Landscape

March 15, 2022

Speakers

James Ruotolo
Senior Manager
Fraud & Financial Crimes
james.ruotolo@us.gt.com
@jdruotolo

Taylor Larimore
Senior Manager
Fraud & Financial Crimes
taylor.larimore@us.gt.com

What We Will Cover

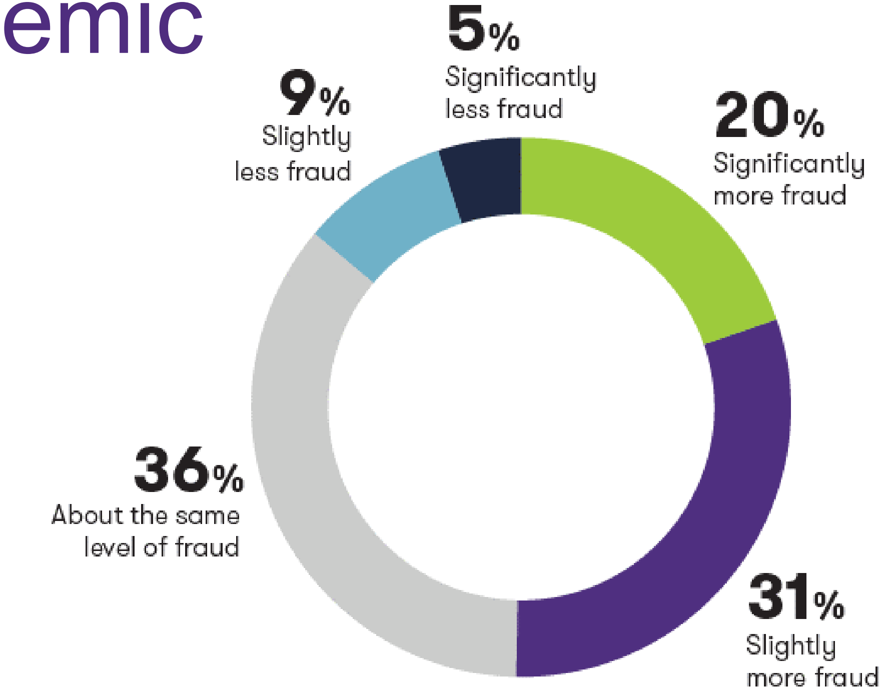
1. The Current State of Fraud
2. Recent Trends in Fraudtech
3. The Fraudtech Marketplace
4. Challenges of Navigating the Marketplace
5. Recommendations and Leading Practices

Grant Thornton

The Current State

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

… and 14% saw less fraud

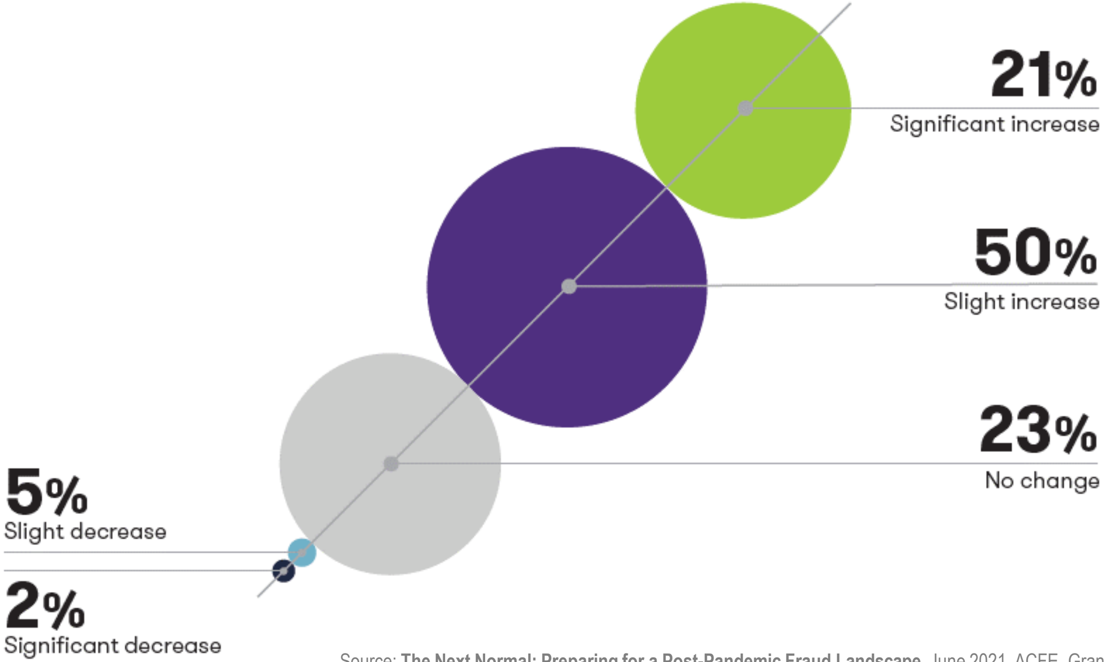


Change in the amount of fraud uncovered

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

Only 7% think fraud will decrease over the next year

Expected change in the overall level of fraud impacting organizations



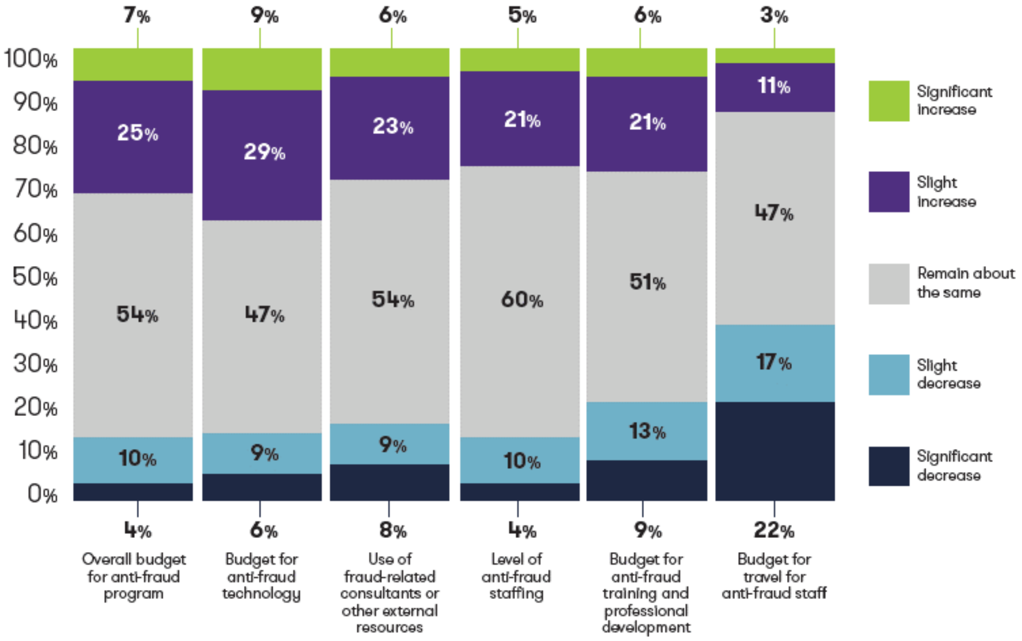
Source: **The Next Normal: Preparing for a Post-Pandemic Fraud Landscape**. June 2021. ACFE, Grant Thornton. https://www.grantthornton.com/library/survey-reports/acfe-survey-report.aspx

The Response is Fraudtech

Bigger Budgets for Fraudtech

38% of organizations increased budget for **anti-fraud technology** for FY21

Technology is the most common area for increased investment in anti-fraud programs

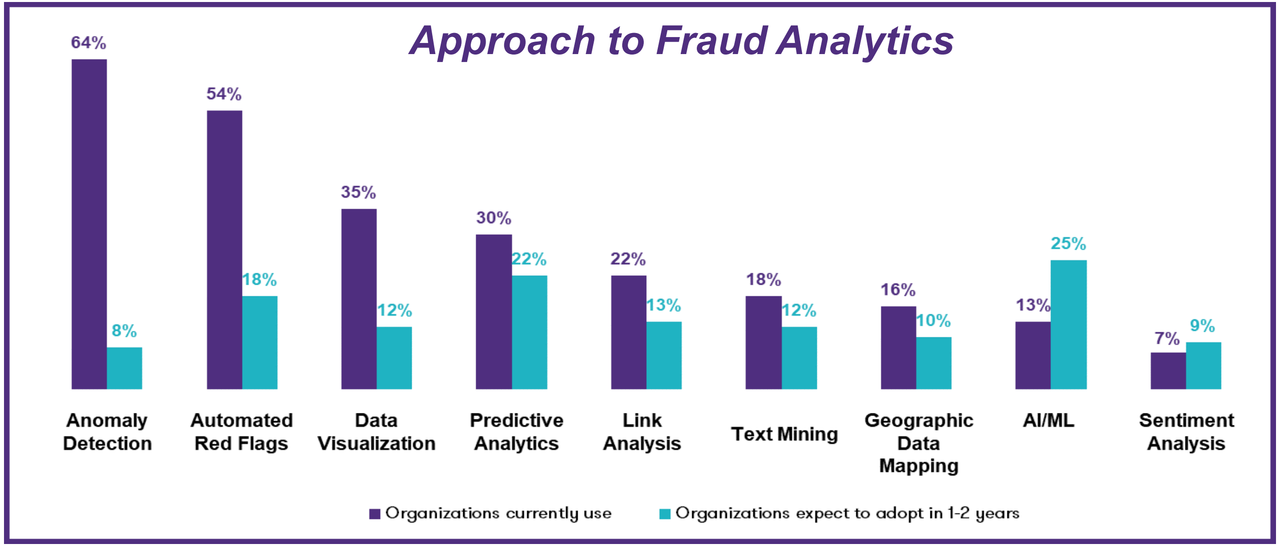


Budgets for fiscal year 2021 compared to pre-pandemic years

The Continued Rise of Fraud Analytics

Using Data to Uncover Fraud

According to the ACFE, “Organizations that used ‘proactive data monitoring’ experienced a **33% reduction** in the total loss and duration of fraud schemes.”



Polling Question #4

Does your organization currently use tools or technology to prevent and detect fraud?

a. Yes
b. No
c. Unsure

Grant Thornton

Grant Thornton

The Fraudtech Marketplace

Highlights and Overview

The Fraudtech marketplace is **complex**. It is full of companies offering similar yet oftentimes distinct products.

The Fraudtech marketplace is **constantly evolving**. We see regular additions, subtractions, and acquisitions of Fraudtech companies.

The Fraudtech market is **diverse**. We see companies with various growth strategies and products make waves in different ways.

Marketplace Complexity

The pure density of the anti-fraud vendor marketplace can leave shoppers stuck in the weeds.

Many times, there are countless companies offering the same or similar products to solve a company's most pressing Fraudtech need.

This makes the ability to distinguish between product types and their capabilities imperative.

Visualization
Data Integration
Orchestration
Text Mining
Link Analysis
Decision Trees
WebAuthN
Link Analysis
Authentication
Network Analytics
Identity Assurance
Predictive Modeling
Text Mining
Identity Proofing
Zero Trust
Heuristic Rules
Biometrics
Orchestration
Verification
Visualization
Data Lake
WebAuthN
Identity Assurance
Image Analysis
Machine Learning
Biometrics
Privacy
Text Mining
Network Analytics
Zero Trust
Biometrics
Predictive Modeling
FraudTech
Link Analysis
Machine Learning
Liveness Detection
Decision Trees
Image Analysis
Device Identity
Voice Technology
Privacy
FraudTech
Privacy
Validation
Zero Trust
Data Integration
Validation
Biometrics
Visualization
Heuristic Rules
Link Analysis
Text Mining
FraudTech
Decision Trees
WebAuthN
Orchestration
Device Identity
Privacy
Data Lake
Verification
FraudTech
Robotic Process Auotmation
Identity Proofing
Artificial Intelligence
Data Lake
Verification
Platform Authentication
Voice Technology
Machine Learning
Platform Authentication
Data Integration
Validation
Identity Proofing
Validation
Predictive Modeling
FraudTech
Liveness Detection
Data Lake
Heuristic Rules
Artificial Intelligence
Verification
Zero Trust
Liveness Detection
Authentication
Image Analysis
Authenticator Assurance
Voice Technology
Visualization
Device Identity
Orchestration
Platform Authentication
WebAuthN
Liveness Detection
Identity Assurance
Heuristic Rules
Authenticator Assurance
Authentication

Grant Thornton

Marketplace Evolution

An everchanging Fraudtech ecosystem

A variety of different start-up companies with unique product offerings and solutions has forced the market to adjust. Big players like the ones listed below are fast at work acquiring new technologies that will allow them to remain competitive and ahead of the curve.

LexisNexis	id:analytics 2020, $375M	emailage 2020, $480M	ThreatMetrix 2018, $817M
TransUnion	neustar 2021, $3.01B	Callcredit 2018, $1.42B	iovation 2018, Undisclosed
EQUIFAX	APPRISS 2021, $1.83B	Kount 2021, $640M	idwatchdog 2017, $63M

Marketplace Diversity

A Zoo of Fraudtech Start-Ups

The sheer number of start-ups in Fraudtech inevitably make the Fraudtech space a web of complexity. Not only are start-ups bringing new products and solutions to market, but they are doing it with a variety of growth strategies.

While everyone has certainly heard of the classic “unicorn” when it comes to a start-up company, you may be less familiar with the market strategies of zebras, camels, and gazelles.

- Maintain Equity
- Be Profitable Immediately
- Collaborate with Competitors

- Profitability Above All
- Lack Investor Base
- Volatile Markets (the desert)

- Profitable and Sustainable
- Lacks Resources
- Often describes African Start-Ups

The Tech

Emerging Fraudtech
Artificial Intelligence

! Ability of a computer to do tasks that are usually done by humans because they require human intelligence

Emerging Fraudtech

Image Analysis

! Identify duplicates, recognize patterns, and compare multiple versions of images to detect similarities or anomalies

Emerging Fraudtech
Voice Biometrics

! **Using voice to help authenticate identity and detect potential deception**

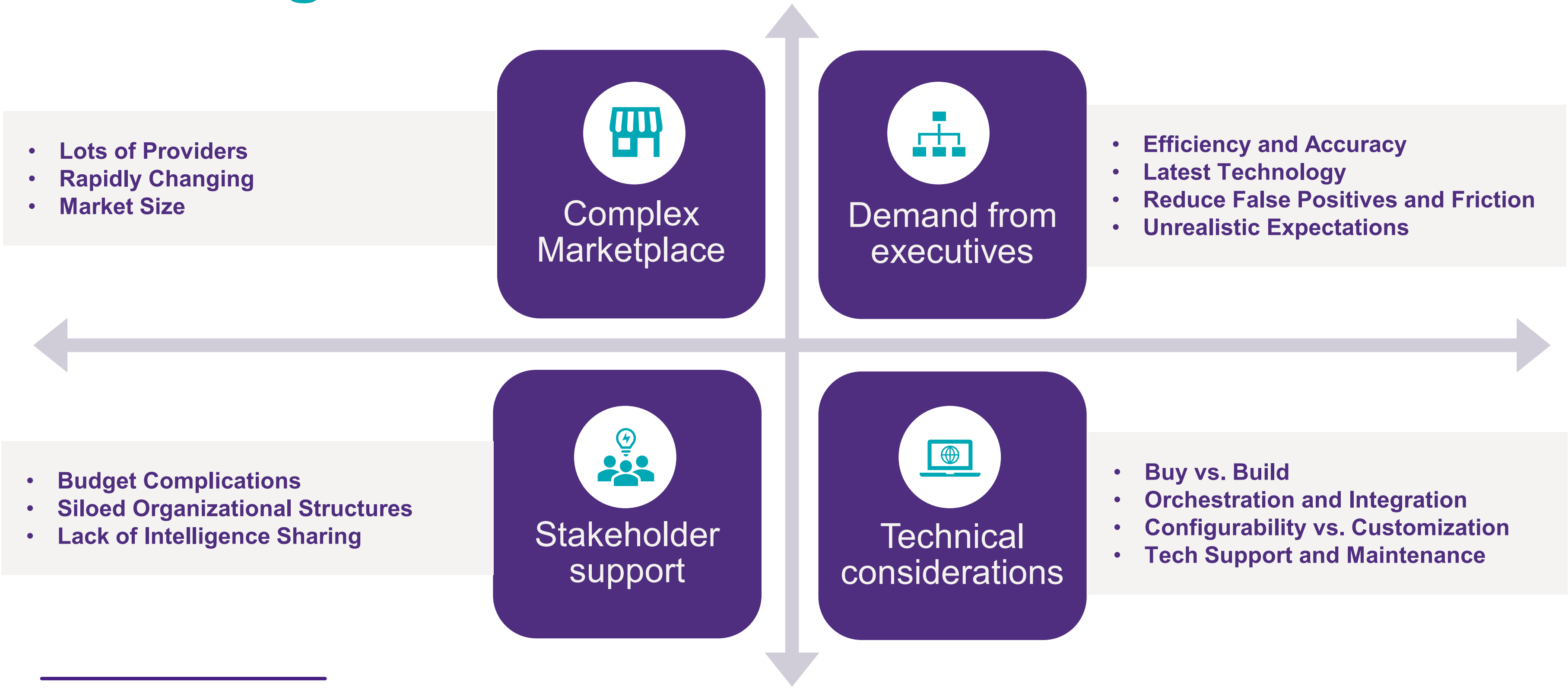
Polling Question #5

Does your organization use fraud detection analytics or scoring technology?

a. Yes
b. No
c. Unsure

Navigating the Marketplace

Fraud Tech Investment
Challenges



Complex Marketplace

- Lots of Providers
- Rapidly Changing
- Market Size

Demand from executives

- Efficiency and Accuracy
- Latest Technology
- Reduce False Positives and Friction
- Unrealistic Expectations

Stakeholder support

- Budget Complications
- Siloed Organizational Structures
- Lack of Intelligence Sharing

Technical considerations

- Buy vs. Build
- Orchestration and Integration
- Configurability vs. Customization
- Tech Support and Maintenance

Grant Thornton

Recommendations and Leading Practices

Fraud Tech Investment

Solutions

Technology Selection

- Fraudtech Strategy and Roadmap
- Buy vs. Build Analysis
- Business Case/ROI Development
- RFI/RFP Management

Program Management

- Change Management
- Report and Communication Plans

Fraud Tech Investment
Solutions

Implementation & Adoption

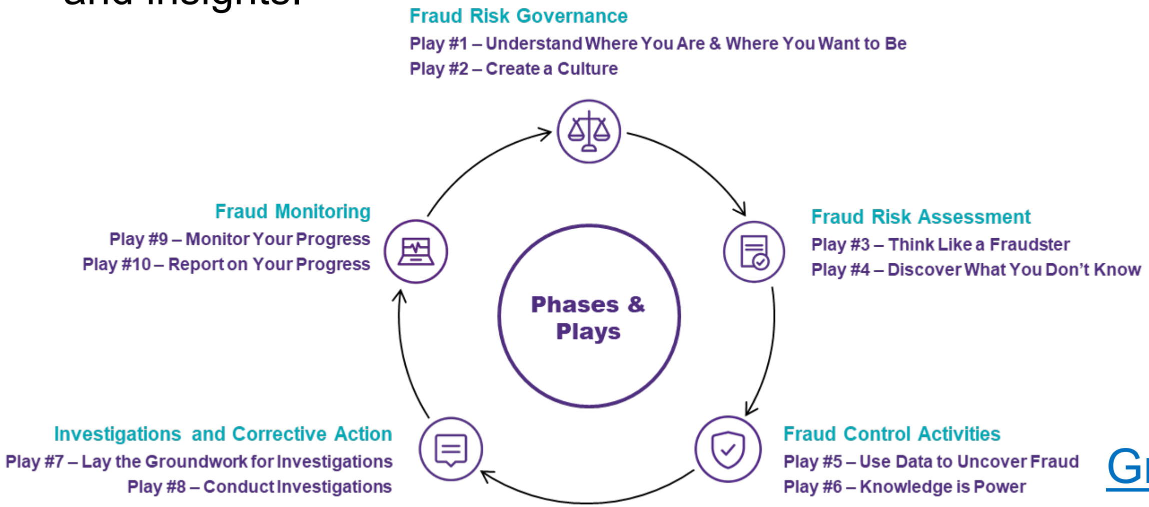
- Business Process and Staffing Advisory
- Employee Training

Technology Maintenance

- Model Validation
- Upgrade and Enhancement Planning
- End-of-Life and Replacement Training

The Anti-Fraud Playbook

The playbook provides **practical guidance for organizations looking to begin, advance, or benchmark their fraud risk management programs against best practices**. The playbook includes key questions, checklists, and insights.



Fraud Risk Governance
Play #1 – Understand Where You Are & Where You Want to Be
Play #2 – Create a Culture

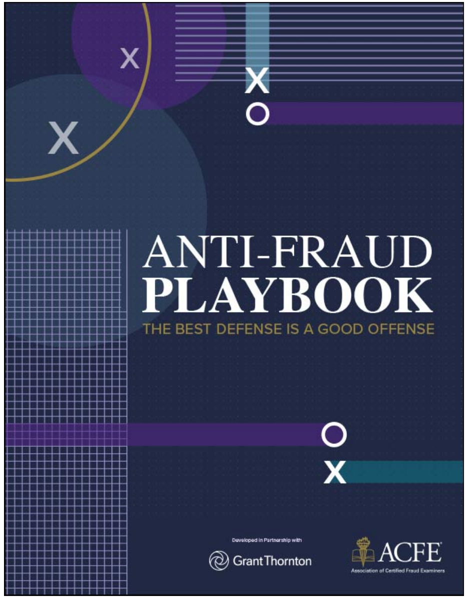
Fraud Risk Assessment
Play #3 – Think Like a Fraudster
Play #4 – Discover What You Don't Know

Fraud Control Activities
Play #5 – Use Data to Uncover Fraud
Play #6 – Knowledge is Power

Investigations and Corrective Action
Play #7 – Lay the Groundwork for Investigations
Play #8 – Conduct Investigations

Fraud Monitoring
Play #9 – Monitor Your Progress
Play #10 – Report on Your Progress

Phases & Plays



ANTI-FRAUD
PLAYBOOK
THE BEST DEFENSE IS A GOOD OFFENSE
Developed in Partnership with
Grant Thornton
ACFE
Association of Certified Fraud Examiners

Download a free copy
GrantThornton.com/fraudplaybook

Grant Thornton

Any final questions?

Q & A

Grant Thornton

Trial by Fire

Lessons learned fighting fraud during a pandemic

March 15, 2022

What We Will Cover

1. Pandemic Fraud Overview
2. Lessons Learned
3. Recommendations
4. Q&A

State of Fraud

Overview

Fraud is on the rise, both in frequency and in cost

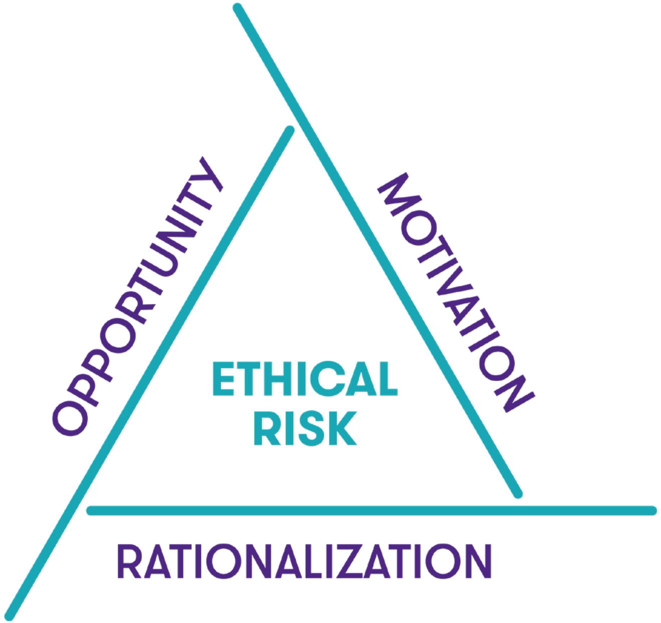
Risks continue to shift as technology and security evolve

Organizations need to focus on both internal and external fraud threats

Why Does Fraud Occur?

Fraud occurs in a variety of fashions is generally due to three specific factors that make up the *Fraud Triangle*:

- **Motivation** – the reason for committing fraud (greed, revenge, survival)
- **Rationalization** – the mindset of the fraudster that justifies them to commit fraud
- **Opportunity** – the situation that enables fraud to occur, often when internal controls are weak or nonexistent



Pandemic Fraud Triangle

Opportunity

- Access to systems and data necessary to perpetrate fraud
- Ineffective controls for a remote work force
- Reduced focus on segregation of duties

Pressure

- New employees or current employee's spouses may have been unemployed recently
- Funding sources may have decreased, making it more difficult to obtain funding required to hit employee targets

Rationalization

- Justification that the money is only being borrowed or will be paid back when situation improves
- May feel entitled to more compensation after a year without raises or bonuses

Pandemic Fraud Schemes

The Association of Certified Fraud Examiners (ACFE) found that the top five fraud schemes currently observed due to the economic impact of the COVID-19 pandemic include:

Cyber Fraud

Identity Theft

Payment Fraud

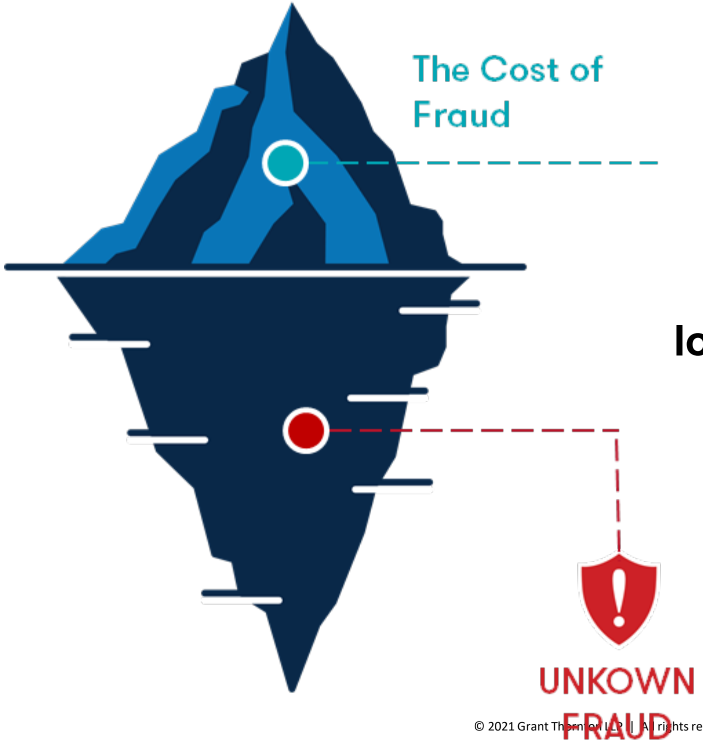
Unemployment Fraud

Vendor & Seller Fraud

The cost of fraud

Fraud is like the proverbial iceberg; the deceptive nature of fraud means that it is unknown until discovered, leading to potential 'submerged' or unknown frauds beneath the surface.

According to the Association of Certified Fraud Examiners (ACFE), CFEs estimate that organizations around the world lose an estimated 5% of their annual revenues and funding to fraud. Applied the 2019 Gross World Product (GWP), this amounts to $4.3 **trillion** in potential global fraud losses.



The ACFE estimates that **organizations lose an estimated 5% of annual revenues and funding due to fraud.**

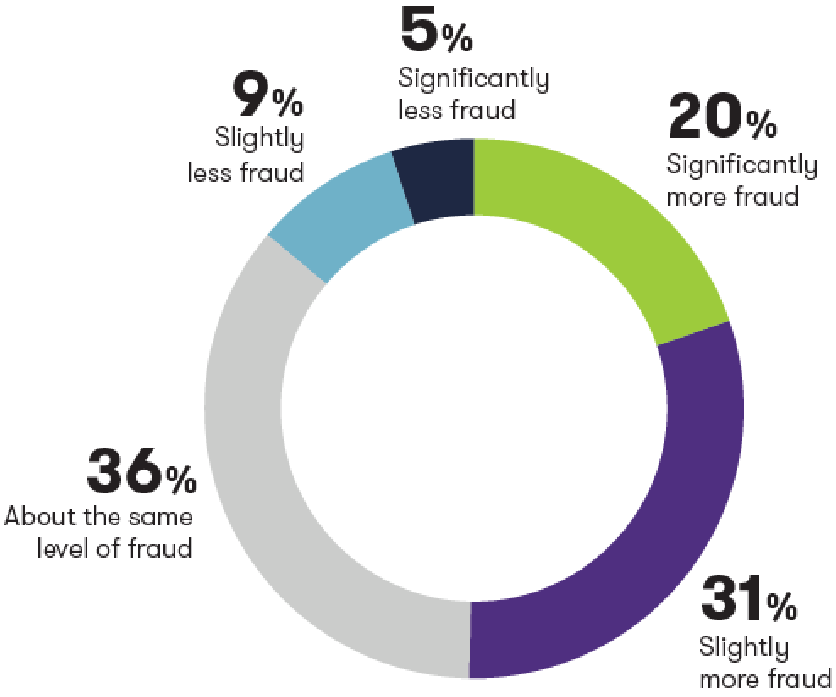
Polling Question #6

Did your organization see a change in the amount of fraud attempts during the COVID-19 pandemic?

a. Yes, it went up
b. Yes, it went down
c. No change

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

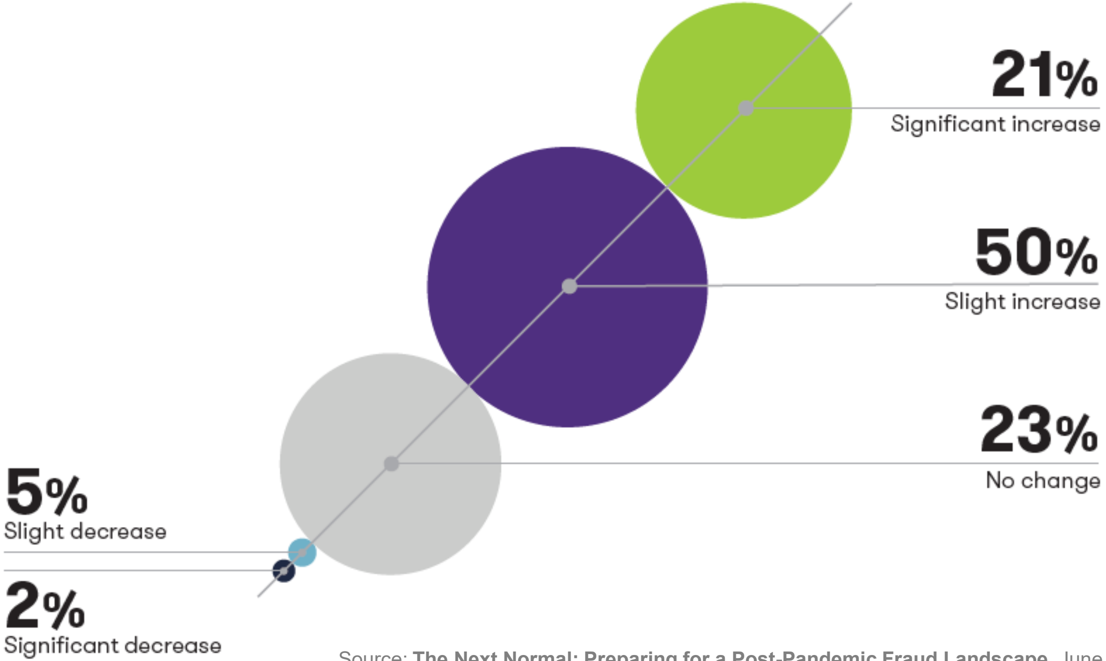
… and 14% saw less fraud



Change in the amount of fraud uncovered

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

Only 7% think fraud will decrease over the next year



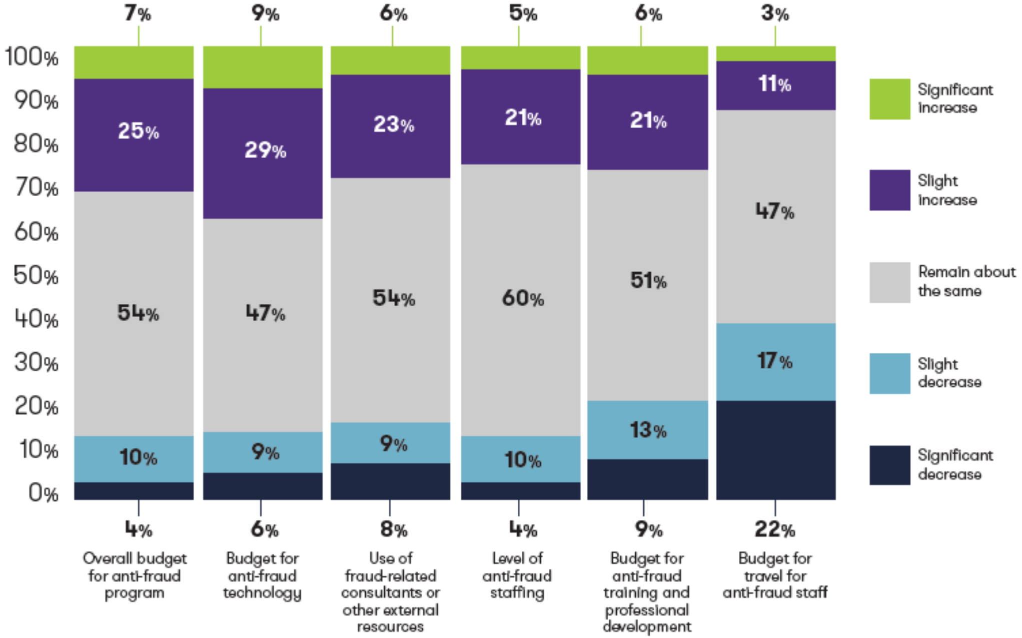
Expected change in the overall level of fraud impacting organizations

Grant Thornton

Source: **The Next Normal: Preparing for a Post-Pandemic Fraud Landscape**. June 2021. ACFE, Grant Thornton. https://www.grantthornton.com/library/survey-reports/acfe-survey-report.aspx

38% of organizations increased budget for **anti-fraud technology** for FY21

Technology is the most common area for increased investment in anti-fraud programs



Budgets for fiscal year 2021 compared to pre-pandemic years

Grant Thornton

Insight into the Next Normal

Observations and Lessons Learned From Pandemic Oversight

LESSON #1

The fraud problem is actually worse than what you read about in the press.

⚠ The pandemic **delivered soft fraud targets** in the form of government stimulus funding rolled out urgently and without fully realized fraud controls, and companies rapidly adapting their business processes with limited opportunity to deploy new protections.

⚠ While the true scope of fraud in these programs is still being determined, **up to 50% of all pandemic unemployment insurance benefits may have been paid improperly.**

WHAT CAN YOU DO?
Enhance Your Fraud Risk Assessment. Reevaluate how your business processes are operating in the current environment, such as how remote or hybrid work arrangements may change the way existing controls are executed.

LESSON #2

The pandemic indoctrinated a new generation of fraud actors turning to new commercial targets.

⚠ A new generation of fraud actors whet their appetites on the gateway drug of stimulus program fraud and **are turning their attention toward commercial targets** as stimulus funding begins to fade.

⚠ Cyber-enabled fraud risks like ransomware, business email compromise and account takeovers were all on the rise before 2020, and **legions of remote workers have expanded the attack surface.**

WHAT CAN YOU DO?
Improve collaboration between cybersecurity and fraud teams**.** As fraud risks are increasingly enabled by technology, organizations need to improve communication between internal silos, especially between cybersecurity and fraud teams.

Grant Thornton

LESSON #3

Organized crime in the fraud risk landscape is increasing.

⚠ **International organized crime rings** targeted unemployment programs in many states. Fraud rings share intelligence that helps them make more money, better elude detection, and carry out more diverse and complicated strategies for committing fraud.

⚠ It is estimated that **at least 70% of the money stolen by impostors ultimately left the country**, much of it ending up in the hands of criminal syndicates in China, Nigeria, Russia and elsewhere.

WHAT CAN YOU DO?
Monitor fraud threat intelligence. In order to stay proactive, organizations must constantly monitor external fraud threat intelligence for indicators of fraud compromise and take action to mitigate new and emerging threats.

LESSON #4

Regular monitoring and agility proved beneficial to investigating the new fraud landscape.

⚠ Agencies struggled with fraud prevention efforts in many cases because they were **unable to capture the right data** and **struggled with outdated legacy IT infrastructure**.

⚠ **Not every transaction should be treated equal**. High-risk transactions should be correctly identified and measured through risk scoring techniques; allowing enhanced rigor and resources to be applied to the riskiest transactions.

WHAT CAN YOU DO?

Upgrade Your Fraud Management Tools. Organizations need to adapt and monitor their antifraud technologies and systems to deal with the traditional fraud attempts they have always seen while simultaneously reacting to the new wave of fraud brought on by the pandemic.

LESSON #5

Identity-based crimes have skyrocketed, with fraud actors devising new ways to be imposters.

Identity-based crimes became a common method for criminals to apply for multiple benefits simultaneously, dramatically increasing their payday.

Synthetic identity crimes can be especially challenging. Since the fraud actor created the identity, **they have all the answers to circumvent certain fraud controls**, such as knowledge-based authentication or multi-factor authentication codes.

WHAT CAN YOU DO?
Upgrade Your Identity Verification Solutions**.** Evaluate your risk for synthetic identity crime and update your identity verification and authentication technologies over the coming months to help ease into the next normal of business operations.

Polling Question #7

Did your organization update its antifraud strategy based on any changes in the risk landscape resulting from COVID-19?

a. Yes
b. Partially
c. No

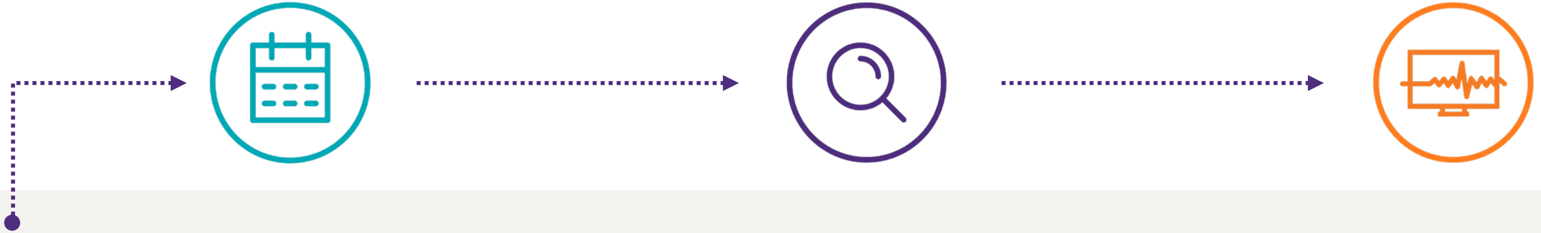
Grant Thornton

Grant Thornton

Recommendations

The best defense is a good offense

Proactive Fraud Solutions



PLAN

Understand the current state of your fraud risk management program compared to leading practices, guidance, and your peers. Develop a roadmap and strategy to close gaps and outline how you will achieve your ideal future state, ensuring resources are effectively utilized in areas of high-impact and high-priority in the future.

- Maturity Assessing
- Benchmarking & Peer Analyses
- Strategy & Roadmap

ASSESS

Discover insights into the universe of fraud risks. Identify what areas are well controlled and what areas may need control enhancements. Seek to drive antifraud investment decisions to areas that are both under-controlled and subject to increasing fraud threads, providing the highest ROI.

- Horizon Scan
- Fraud Risk Assessment
- Anti-Fraud Culture Assessment
- Fraud Threat Intelligence

RESPOND & MONITOR

Proactively close identified gaps through targeted mitigating risk response that states on top of both current and emerging risks as the risk landscape continues to evolve.

- Anti-Fraud Training & Awareness Initiatives
- Fraud Performance Metrics & Evaluations
- Fraud Analytics, Model Development & Governance
- Technology Assessment, Selection & Implementation

COSO's Fraud Risk Management Principles

Fraud Risk Governance: The organization establishes and communicates a Fraud Risk Management program

Fraud Risk Assessment: The organization performs comprehensive fraud risk assessment

Fraud Control Activity: The organization selects, develops, and deploys preventive and detective fraud control activities

Fraud Investigation & Corrective Action: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective

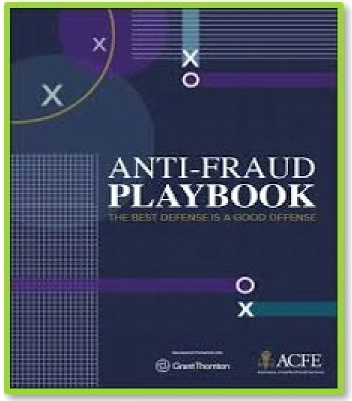
Fraud Risk Management Monitoring Activities: The organization selects, develops, and performs ongoing evaluations

The Anti-Fraud Playbook

The playbook is intended to **provide practical guidance for organizations looking to begin, advance, or benchmark their Fraud Risk Management (FRM) programs against best practices**.

It draws on insights from the COSO Guide and seeks to clarify and operationalize the concepts put forward in that guidance. The playbook includes **key questions, checklists, and insights that will enhance your FRM program and ultimately facilitate effective and proactive FRM at your organization**.

2020



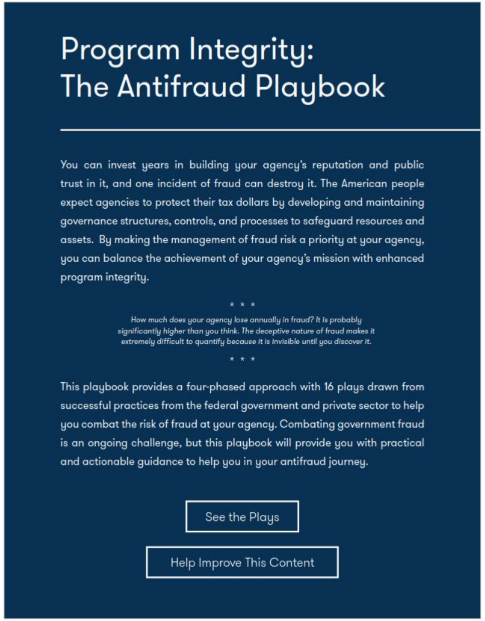
Grant Thornton & ACFE publish the Anti-Fraud Playbook

Available at **GrantThornton.com** or **ACFE.com**

The Anti-Fraud Playbook

The government-wide playbook is intended to **provide practical guidance for looking to begin, advance, or benchmark their Fraud Risk Management (FRM) programs against best practices**.

It draws on insights from the Government Accountability Office (GAO) Framework for Managing Fraud Risks in Federal Programs and seeks to clarify and operationalize the concepts put forward in that guidance. The playbook includes **key questions, checklists, and insights that will enhance your FRM program and ultimately facilitate effective and proactive FRM at your organization**.



Program Integrity:
The Antifraud Playbook

You can invest years in building your agency's reputation and public trust in it, and one incident of fraud can destroy it. The American people expect agencies to protect their tax dollars by developing and maintaining governance structures, controls, and processes to safeguard resources and assets. By making the management of fraud risk a priority at your agency, you can balance the achievement of your agency's mission with enhanced program integrity.

* * *

How much does your agency lose annually in fraud? It is probably significantly higher than you think. The deceptive nature of fraud makes it extremely difficult to quantify because it is invisible until you discover it.

* * *

This playbook provides a four-phased approach with 16 plays drawn from successful practices from the federal government and private sector to help you combat the risk of fraud at your agency. Combating government fraud is an ongoing challenge, but this playbook will provide you with practical and actionable guidance to help you in your antifraud journey.

Available at **https://www.cfo.gov/knowledge-sharing/fraudprevention/**

Threat Intelligence

Your **ATTACK** surface extends far beyond your network perimeter.

Challenging to see what's outside of your network

- Network security tools aren't designed for it.
- Challenging to safely get access to the places that matter.

Lack of context or relevance

- How can I VERIFY that a threat is relevant to my business?
- Lack of expertise.

Difficult decision-making

- What should I do, what is the path forward?
- What is the appropriate response?

Benefits of Threat Intelligence

Proactive

Risk Identification

- Gain access to where the threat actors are
- Visibility into the known, unknown, and emerging schemes facing your organization

Actionable

Intelligence & Insight

- Expert-curated analysis
- Risk-based prioritization of threats facing your organization
- Actionable recommendations on next steps to close weaknesses or gaps

Enhanced

Decision-Making & Planning

- Structured roles and responsibilities for handling digital threats
- Structured communication between contractors, law enforcement, states, and other program partners

Any final questions?

Q & A

Speakers

James Ruotolo
Senior Manager
Fraud & Financial Crimes
james.ruotolo@us.gt.com
@jdruotolo

Taylor Larimore
Senior Manager
Fraud & Financial Crimes
taylor.larimore@us.gt.com

Grant Thornton