

The Controller's Role in Internal Controls:

Protection with Simple,
Smart and Scalable Practices

Written By

Robert Berry

MBA, CPA, CIA, CISA



THE
KNOWLEDGE
INSTITUTE



About the Author



Robert Berry, MBA, CPA, CIA, CISA

Robert Berry is a Certified Public Accountant who actually likes people more than he does numbers. With more than 20 years in the risk, audit, and compliance sector, he is an internationally recognized speaker, trainer, author and podcast host. His most recent book, “Ask, Get, Perform: The Auditors Essential Guide to Asking Better Questions, Getting Better Answers, and Performing Better Audits,” is changing the way auditors build relationships with clients. Robert divides his time between Alabama and Texas.

rob@ThatAuditGuy.com



Discussion Question #1

Internal Controls – Your Opinion

What's one word that comes to mind when you think of internal controls?



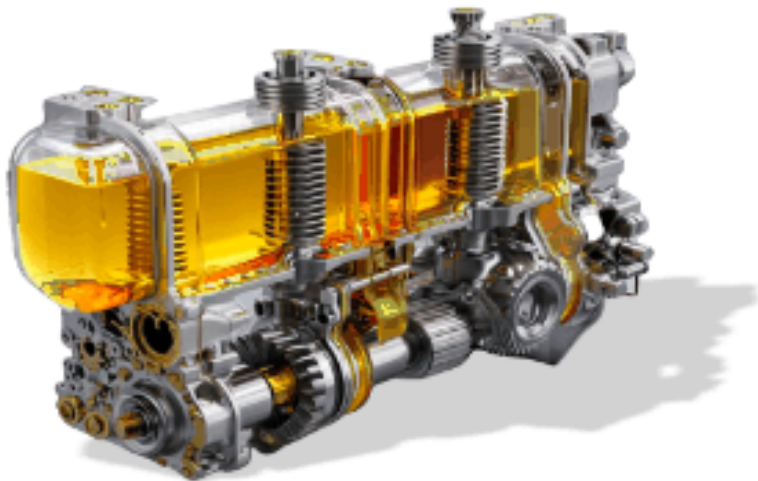


Why Internal Controls Matter



Let's Get One Thing Straight...

- Internal controls $\neq$ bureaucracy
- Internal controls = confidence, clarity, and prevention





What Internal Controls Are - And What They're Not



What Internal Controls Really Are

Internal controls are how you make sure what's supposed to happen...actually happens.

- Systems and processes that reduce risk
- Tools to ensure operations run as intended
- A way to protect assets, data, and decisions
- Scalable — not one-size-fits-all



A Control is:

A policy, process, or activity that helps an organization achieve its goals, avoid risk, and protect resources.





What Internal Controls Are NOT

Myth	Reality
Just for auditors	Actually for everyone
Expensive software	Many are human-based
Bureaucracy	Can streamline processes
A one-time setup	Require ongoing attention



Controls Are

- ✗ Not just accounting rules
- ✗ Not a punishment
- ✗ Not optional
- ✗ Not perfect
- ✗ Not one-size-fits-all



Polling Question #1

Controls At Your Company?

Which of these apply to your organization today?

- a) We have some controls, but they're informal
- b) We have formal controls, but they're outdated
- c) We're unsure what counts as a control
- d) We review and monitor controls regularly



Polling Question #2

Why Internal Controls Matter

Why do internal controls matter most to an organization?

- a) They help auditors complete their work faster
- b) They ensure every error is prevented
- c) They reduce risk and increase consistency in decision-making
- d) They exist to satisfy regulatory requirements



Why Even Small Organizations Need Controls

“We’re too small for formal controls.”

– Said before every preventable disaster



Real Case: The \$89,000 Reimbursement

- A small nonprofit trusted its office manager,
- who reimbursed themselves \$89,000 in “expenses,”
- over 3 years, and
- no one noticed.



Right-Sized, Not Red-Taped

Big Company	Small Company
9-step purchase order system	Simple budget limit + email approval
Full ERP role-based access	Single login with 2FA and password rotation
Monthly control self-assessments	Quarterly review by outside CPA, etc



Polling Question #3

Why Even Small Organizations Need Controls?

Why are internal controls especially important in small organizations?

- a) Small organizations face more regulations
- b) Errors are more likely to occur
- c) Fewer people means less need for controls
- d) Risk is often concentrated in fewer hands



COSO Simplified



COSO - A Fancy Name for Common Sense

- 1) Are we serious about doing things right?
- 2) Do we know what could go wrong?
- 3) Do we have guardrails in place?
- 4) Is everyone doing what they're supposed to?
- 5) Are we paying attention to what's working and what's not?



COSO's 5 Components Made Simple

The 5 components of internal control;

- 1) Control environment
- 2) Risk assessment
- 3) Control activities
- 4) Information & communication
- 5) Monitoring





Control Environment: Where It All Starts

- Code of conduct
- Ethical leadership
- Job descriptions with responsibility clarity
- Clear expectations and consequences



Risk Assessment: What Could Go Wrong?

- Risk of theft if only one person opens the mail
- Risk of error if manual entries are common
- Risk of bias if AI tools go unchecked



Control Activities: The “Doing” Part

- Dual approvals
- Reconciliations
- Password protections
- Inventory counts
- Audit trails





Information & Communication: Who Needs to Know What?

- Do employees know the rules?
- Are control exceptions reported?
- Is training provided and documented?
- Can people raise concerns safely?



Monitoring: Are We Still in Control?

- Spot checks
- Control reviews
- Internal audits
- Feedback loops
- Exception reports





Discussion Question #2

Let's Look at Your Organization

- a) Which COSO component is strongest in your organization?
- b) Which component is most overlooked?
 - 1) Control environment
 - 2) Risk assessment
 - 3) Control activities
 - 4) Information & communication
 - 5) Monitoring



Polling Question #4

COSO Simplified

What is the primary value of the COSO framework when applied correctly?

- a) It provides detailed control checklists
- b) It guarantees compliance with all regulations
- c) It helps organizations think systematically about risk and control
- d) It replaces the need for professional judgment



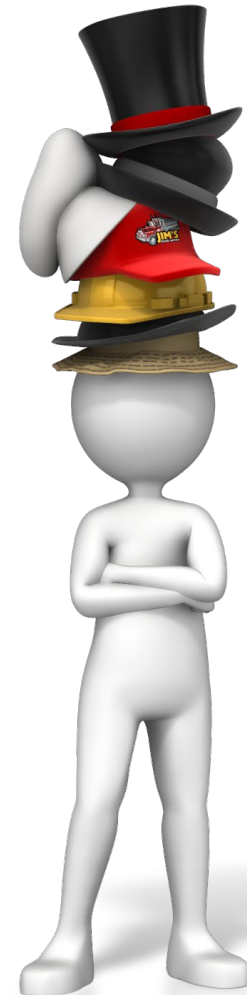
Common Control Failures



Common Breakdown #1

No Segregation of Duties

- One person handles everything
- No oversight, no double checks
- High risk for error, abuse, or fraud





Common Breakdown #2

Lack of Documentation

- Verbal approvals only
- No audit trail
- Hard to prove what happened





Common Breakdown #3 Over-Reliance on People

- “Trust-based” systems
- Key processes in one person’s head
- No backup if they leave





Common Breakdown #4 Inadequate Oversight

- Managers too busy to review
- Approvals rubber-stamped
- No one watching the watchers





HEADLINES: When It All Goes Public

- Embezzlement in a school district
- Local nonprofit loses donor funds
- Small biz accountant charged with theft
- All due to basic control failures





Discussion Activity #1

Can You Spot the Failure?

On the next slides, you'll see three mini-scenarios. Individually or in your groups, discuss:

- What control(s) is missing?
- What could go wrong?
- What should have been in place?



Discussion Activity #1 a

Can You Spot the Failure?

A small retail company's office manager handles payroll, approves overtime, and reconciles the bank account.



What control is missing?



What could go wrong?



What would you recommend?



Discussion Activity #1 b

Can You Spot the Failure?

A department head approves vendor invoices over the phone while traveling, and the AP clerk pays them without additional review.



What's the risk here?



What could go wrong?



What control could prevent this?



Discussion Activity #1 c

Can You Spot the Failure?

The only person who knows how to run a key report is on vacation. No one else can access the system or interpret the data.



What's the issue?



What's the consequence?



What's the fix?



Case Study #3

Systemic Control Failure in Social Services Grant Oversight

In January 2026, multiple news outlets reported that a state audit found **widespread failures in internal controls and oversight** of the Minnesota Department of Human Services' Behavioral Health Administration grant programs.

The audit found the department did not comply with most grant requirements, had inadequate controls over \$425 million in behavioral health grants, and, in many cases, could not provide complete or accurate documentation.

Now that we've seen how things can go sideways, and sometimes spectacularly, you might be thinking,

'Okay, but how do we actually prevent these failures without creating more work or red tape?'



Polling Question #5

What Internal Controls Are, and What They're Not?

Which statement best describes what an internal control actually is?

- a) A documented policy or procedure
- b) A checklist used during audits
- c) A process that helps ensure objectives are achieved
- d) A rule that prevents all mistakes



Scalable Controls That Work



Why Scalable Controls Matter

- Controls should protect—not paralyze
- Right-sized controls reduce risk without slowing you down
- A little intentionality goes a long way



Simple Financial Control Example

✓ Good control:

Dual approval for payments over \$1,000

✗ Bad control:

Only one person cuts and approves checks



Operational Control Example

✓ Good control:

Inventory checklist at close of business

✗ Bad control:

“We trust our team to keep track”



Compliance Control Example

✓ Good control:

Onboarding checklist for new employees

✗ Bad control:

HR “remembers” to do everything manually



Human-Based vs. Tech-Based Controls

Human-Based	Tech-Based
Dual signatures	Workflow software
Rotation of duties	System-enforced access
Review checklists	Audit logs & alerts



Discussion Activity #2

Redesign a Broken Control

Think of a real control in your organization that feels clunky, weak, or unclear.

In small groups or solo:

- Describe what's wrong with it?
- Redesign it using a scalable alternative (human or tech).
- Share 1 or 2 redesigned controls with the room.



Polling Question #6

Scalable Controls That Work

What makes a control scalable as an organization grows?

- a) It is highly detailed and complex
- b) It can be expanded without redesigning the entire process
- c) It requires specialized software
- d) It is owned by senior management



Tailoring Controls to Fit Your Organization



Why Tailoring Matters?

- Overkill creates friction.
- Under-control invites risk.
- The goal is to have just enough to protect and perform.



A Risk-Based Approach

Ask:

- “What could go wrong?”
- “How likely is it?”
- “What’s the impact if it does?”





The Control Scaling Spectrum

Level	Example: Vendor Payment Control
Minimal	Manager emails approval
Moderate	Dual signature policy for over \$1,000
Maximum	Workflow software + segregation + monthly audit



4 Questions to Right-Size a Control



What's the cost of failure?



How often does this happen?



How complex is the task?



Who's involved, and what's at stake?



Polling Question #7

Tailoring Controls to Fit Your Organization

Why should internal controls be tailored to each organization?

- a) Regulations allow unlimited flexibility
- b) All organizations face identical risks
- c) One-size-fits-all controls rarely address real risk
- d) Tailoring reduces the need for monitoring



Case Discussion #4

What's Too Much?

What's Too Little?

Have you ever worked somewhere where the controls were way too tight or nonexistent?

a) What did that feel like?

b) And what got missed?"



Embedding Controls into Daily Life



Culture Eats Controls for Breakfast

- Great controls fail without great habits.
- Build process memory, not process manuals.
- Make doing the right thing the path of least resistance.

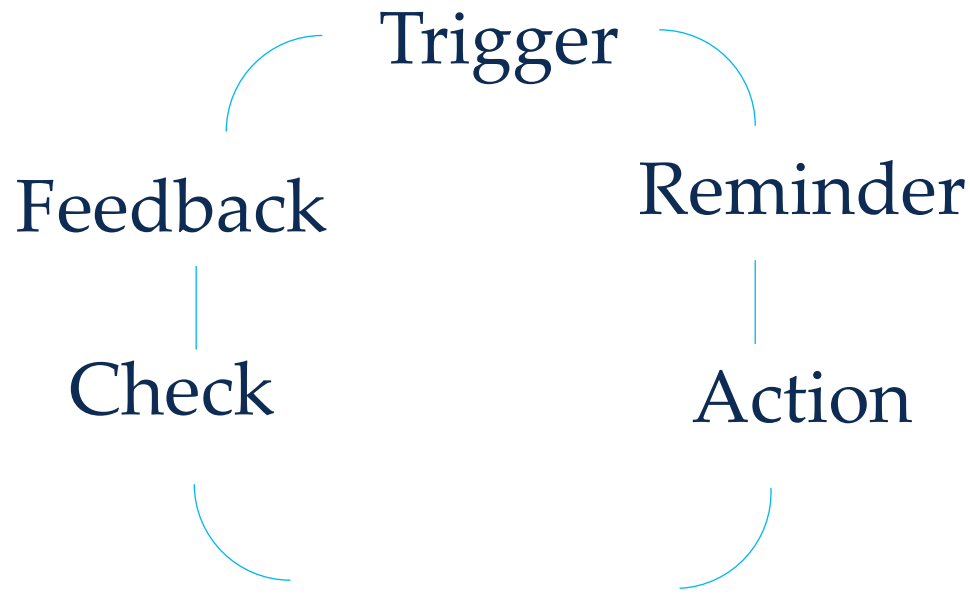


Training + Repetition = Habit

- One-time training $\neq$ control adoption
- Habits form through repeated action
- Controls fail without reinforcement



“Control as Routine” Lifecycle





The Calendar Reconciliation Hack

We didn't need software.

We just needed a calendar.



Reinforcement $\neq$ Policing

- Build accountability into the process
- Celebrate consistency, not just performance
- Visibility beats enforcement



Polling Question #8

Embedding Controls

Which of the following best supports embedding a control into daily operations?

- a) Adding more pages to your policy manual
- b) Sending a one-time company-wide email
- c) Building recurring reminders and tracking behavior
- d) Reprimanding staff after missed deadlines



Monitoring & Adapting Controls Over Time



Controls Aren't Set-and-Forget

- Controls must evolve or they become invisible.





Three Layers of Monitoring

- 1) Day-to-day oversight
 - Are people following the process?
- 2) Periodic review
 - Is the control still effective?
- 3) Trigger-based review
 - Has something changed that requires reevaluation?



Control Health Dashboard

Control Name	Last Reviewed	Status	Followed?	Still Needed?
Vendor Approval	Jan 2024	 Healthy	 Yes	 Yes
Remote Access Policy	Dec 2022	 Stale	 No	 Yes
Petty Cash Log	Apr 2021	 Obsolete	 No	 No



Story: The Control That Lingered

It was still in the SOP...
but no one had done it in 3 years.





Adapting Without Starting Over

- Start with what's working
- Look for patterns in control failures
- Involve your team in redesign
- Don't fear small changes—they matter



Case Discussion #5

Control Check-In Snapshot

Control Name	Why It Exists	Is It Being Followed?	What's Not Working?	What Could Improve It?
e.g. Petty Cash Log	Prevent unauthorized use	Not consistently	No one reviews it weekly	Add a recurring reminder + signoff



Polling Question #9

Reviewing Controls

What's a trigger-based review of a control?

- a) A scheduled review that happens monthly
- b) A review that only happens during audits
- c) A review that happens when a process, system, or risk changes
- d) A checklist performed by frontline employees daily



Case Study #6 (Optional)

Alabama Motorsports Hall of Fame

A recent audit of the Alabama Motorsports Hall of Fame Commission uncovered 35 compliance failures and financial mismanagement over several years.

The report found that a former accounts manager mishandled nearly \$237,000, including overpaying herself, failing to deposit cash sales, and authorizing questionable transactions.



Wrap up



The Control Commitment Triangle

- One thing I'll re-examine
- One process I'll document
- One person I'll involve in a control conversation this week





Polling Question #10

Controls Over Time

What is the best way to ensure internal controls remain effective over time?

- a) Write detailed policies and never change them
- b) Assign one person to oversee all controls permanently
- c) Regularly evaluate and adapt controls based on risk and changes
- d) Trust employees and avoid too much structure



Thank You!

Please share your thoughts and comments.

Rob Berry
rob@thatAuditGuy.com
Deb Habel
debHabel@comcast.net
Tracy Cooper
tracy@tlbhelp.com
Anita Layton
aplayton2@gmail.com
Rob Angell
rangeLL@angellventures.com

Brian Maturi Brian@
Bob Mims Bob@
Don Minges Don@

TheKnowledgeInstitute.com

You can also connect with us on LinkedIn, or call us at 704-942-0413



**THE
KNOWLEDGE
INSTITUTE**

Internal Controls That Matter

Protection with Simple, Smart and Scalable Practices

Written by
Robert Berry
MBA, CPA, CIA, CISA

A 2 Credit Hour Continuing Professional Education Seminar

©Copyright 2025-2026 By **Robert Berry**

All Rights Reserved

www.TheKnowledgeInstitute.Com

You may not reproduce any part of this material without written permission from the copyright owner.

The opinions expressed in this seminar are those of the author and/or discussion leader and do not necessarily reflect those of the sponsoring organization.



The Knowledge Institute, LLC is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN, 37219-2417. Web site: www.nasba.org. (Sponsor #144545)

Case #3

Systemic Control Failure in Social Services Grant Oversight

Story Summary

In January 2026, multiple news outlets reported that a state audit found widespread failures in internal controls and oversight of the Minnesota Department of Human Services' Behavioral Health Administration grant programs. The audit found the department did not comply with most grant requirements, had inadequate controls over \$425 million in behavioral health grants, and, in many cases, could not provide complete or accurate documentation.

The report highlighted:

- Failure to maintain adequate documentation for 63 of 71 grant agreements
- Early payments issued before formal agreements were signed
- Incomplete or missing oversight procedures
- Allegations of doctored and backdated documents
- Employees lacked required training and accountability structures

As a result, regulators and policymakers criticized leadership and calls for structural reform were widespread.

This case illustrates how **weak controls, lack of training, and absent oversight** can lead to audit findings that ripple out into public governance, political consequences, and loss of public trust.

Discussion

Discussion Questions

1. What types of internal control breakdowns can you identify in this scenario?

Encourage participants to categorize failures, such as:

2. Choose three COSO components that failed and explain how:

Participants should tie examples to:

3. What could have prevented this from escalating into a major public finding?

4. What would you recommend for remediation to restore confidence?

Realistic fixes like:

Case #6 (Optional)

Alabama Motorsports Hall of Fame Audit Finds Financial Mismanagement

A recent audit of the **Alabama Motorsports Hall of Fame Commission** uncovered **35 compliance failures and financial mismanagement** over several years. The report found that a former accounts manager mishandled nearly **\$237,000**, including overpaying herself, failing to deposit cash sales, and authorizing questionable transactions. The audit has been referred to the Attorney General for collection.

<https://abc3340.com/news/local/alabama-motorsports-hall-of-fame-audit-reveals-financial-mismanagement>

Alabama Motorsports Hall of Fame is a nonprofit organization that preserves and showcases the state's motorsports history. An audit by the Alabama Department of Examiners of Public Accounts revealed:

- The *accounts manager* authorized personal overpayments to herself.
- Cash sales totaling \$13,370 were *never deposited* into organizational accounts.
- Nearly \$200,000 in transactions lacked clear justification or documentation.
- 35 major compliance and control failures were identified over a five-year period.

The audit was public, and leadership now must respond to findings and implement remediation plans.

Discussion

1. Which internal controls were clearly absent or weak?
2. How did these weaknesses lead to financial mismanagement?
3. What controls would you prioritize first if you were advising the organization?
Good answers include:
4. How could monitoring be improved without hiring new staff?

[Local News](#)

Audit of Minnesota DHS grant programs finds "widespread failures in oversight"

By [Riley Moser](#)

January 6, 2026 / 8:21 PM CST / CBS Minnesota

 Add CBS News on Google

An audit of the Minnesota Department of Human Services' Behavioral Health Administration grant programs found "widespread failures in oversight," according to a state watchdog.

The Office of the Legislative Auditor says the department "did not comply with most requirements tested for mental health and substance use disorder grants and did not have adequate internal controls over grant funds."

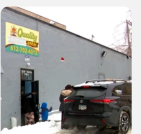
According to [the audit](#), the Department of Human Services distributed more than \$425 million in grants to 830 grantees between July 1, 2022, and Dec. 31, 2024.

Of 51 grant agreements, the report says more than half of the progress reports were missing or past due. The agency also could not prove that it completed 27 of 67 required monitoring visits, and for 24 visits involving 11 grantees, it could not provide any documentation.

One auditor noted that several documents were created by the Behavioral Health Administration only after the audit began and had been backdated in response to document requests.

 CBS NEWS
MINNESOTA

 CBS MINNESOTA
Day care targeted in Nick Shirley video is now closed, records show



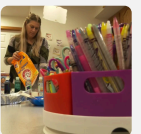
 CBS TEXAS
Abbott orders Texas child care fraud probe after Minnesota scandal raises national alarms



 CBS NEW YORK
NYS mental health services for children to get makeover



 CBS MINNESOTA
Minnesota day cares brace for more compliance measures



 CBS COLORADO
U.S. Fish and Wildlife Service threatens to take control of gray wolf reintroduction





Judge to decide whether to dismiss use of force lawsuit against DHS,



Two grantees were overpaid, and the Behavioral Health Administration paid some grantees for work performed before it fully executed the grant agreements, according to the audit. The agency also made payments to grantees for costs that were either not incurred or not properly supported by source documents.

In a survey of employees at the Behavioral Health Administration, the report says 73% of respondents said they did not receive sufficient training to manage grants.

"Executive leadership has repetitively shown staff that they won't take the staff's concerns or questions seriously until something serious happens or it makes the news," one employee wrote in the survey.

State Sen. Mark Koran, R-North Branch, a member of the Legislative Audit Commission, says the audit shows that Department of Human Services leadership "failed at every level."



CBS News Minnesota



Advil Liqui-Gels Pain Reliever and Fever...

★★★★★ 5,053

Save 5% with **Subscribe & Save**

\$22³² ~~\$23.49~~ ✓prime

Shop now

"The OLA report shows a complete breakdown in how DHS's Behavioral Health Administration manages hundreds of millions in taxpayer-funded grants," Koran said. "BHA failed to verify that grantees were providing the services they were paid for, failed to

First responders choose us for a reason

Find out why

verizon
frontline

Shireen Gandhi, said she was "shocked" to learn the information included in the audit.

"With respect to the audit report, while it's upsetting that DHS has findings in areas we have placed concerted effort, the OLA's report highlights the importance of the grant compliance work already underway at the department. And the findings provide us with a road map for our focus going forward to continue strengthening oversight and integrity of behavioral health grants," Gandhi said. "I take the report seriously, I accept responsibility for the findings, and I will ensure DHS closes the findings."

The report comes amid a widening fraud scandal in the state. Criticism about Minnesota's fraud caused Gov. Tim Walz to announce on Monday that he is dropping his bid to be reelected to a third term.

On Sunday, the Trump administration began a massive deployment of hundreds of DHS agents to the Twin Cities area. Agents deployed from Homeland Security Investigations are expected to look into alleged fraud cases following last month's investigation by federal agents in Minneapolis that DHS Secretary Kristi Noem said was for "child care and other rampant fraud."

More than 90 people face federal charges as a result of fraud schemes that have been uncovered in Minnesota since 2021. Prosecutors estimate the total amount of fraud could reach \$9 billion. The scandal started with a \$250 million COVID-era scheme involving a nonprofit called Feeding Our Future, which was accused of stealing from the Federal Child Nutrition Program.

Since then, federal prosecutors have uncovered "large-scale fraud" in a housing program for seniors and people with disabilities, and a program that provides services to children with autism. The Trump administration is also probing claims of fraud by day care centers in Minnesota, which gained national attention after a conservative YouTube personality named Nick Shirley posted a video that showed him visiting federally backed child care centers around Minneapolis and finding no children there.

First responders choose us for a reason

Find out why

CBS News visited several of the centers named by Shirley and found that all but two of the facilities have active licenses, according to state records, and all active locations were visited by state regulators within the last six months.

Nicole Sganga, Camilo Montoya-Galvez and Jonah Kaplan contributed to this report.

More from CBS News

CBS MINNESOTA
Day care targeted in Nick Shirley video is now closed, records show



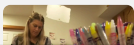
CBS TEXAS
Abbott orders Texas child care fraud probe after Minnesota scandal raises national alarms



CBS NEW YORK
NYS mental health services for children to get makeover



CBS MINNESOTA



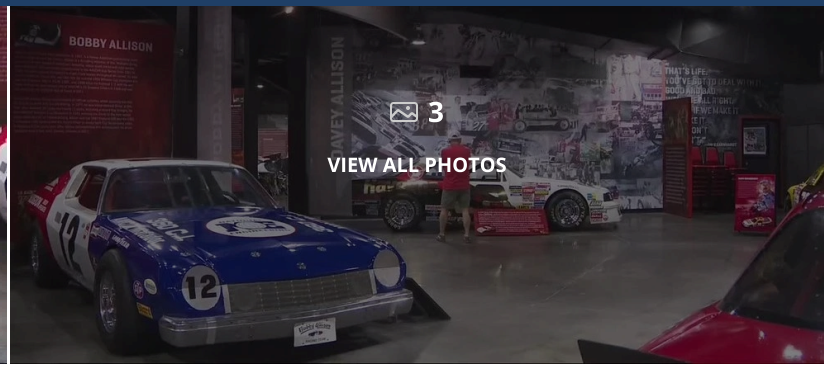
ADVERTISEMENT

Alabama Motorsports Hall of Fame audit reveals financial mismanagement

by ABC 33/40

Fri, October 3, 2025 at 1:29 PM





International Motorsports Hall of Fame (abc3340.com)



The Alabama Motor Sports Hall of Fame Commission is under investigation following an audit by the Alabama Department of Examiners of Public Accounts. The report, filed on Oct. 3, 2025, uncovered 35 compliance failures from October 2019 to September 2024, highlighting financial mismanagement and violations of state law.

A former accounts manager is accused of mishandling nearly \$237,000, including overpaying herself by more than \$26,000, failing to deposit \$13,370 in cash sales, and authorizing nearly \$200,000 in questionable transactions. The case has been referred to the Attorney General's Office for collection as the former manager has refused to repay the funds.

The audit also revealed improper sales of vehicles donated to the museum. A 1968 Camaro Pace Car was sold to the former executive director after \$28,000 in repairs, and the director's spouse purchased a truck under suspicious circumstances. Additionally, some cars were auctioned using a commission member's personal bank account, bypassing state requirements.

ADVERTISEMENT

The Commission was found to have violated the Alabama Open Meetings Act, mishandled contracts, and failed to remit sales taxes on gift shop revenue. Contracts were improperly awarded to insiders, including a company owned by the current director's spouse.

Auditors criticized the Commission for failing to implement basic internal controls, resulting in unreconciled bank accounts and missing inventory records for historic memorabilia. Some funds were improperly deposited into a private nonprofit foundation's account linked to the Commission.

The report describes a culture of weak oversight, exposing public resources to fraud, waste, and abuse. "The Commission failed to design and implement even the most basic internal controls," auditors wrote.

The Attorney General is expected to pursue recovery of the \$236,610.10 owed by the former accounts manager. [The Commission has been directed to overhaul its financial practices](#), comply with state laws, and strengthen accountability measures. As the overseer of the International Motorsports Hall of Fame in Talladega, the Commission faces growing scrutiny over its ability to manage public funds and honor motorsports history responsibly.

SPONSORED CONTENT

by Taboola

Former Jefferson County Schools Superintendent arrested

Report: Alabama QB Ty Simpson Declares for NFL Draft

How much cash should you keep at home?

| SPONSORED

MORE TO EXPLORE

Former Alabama judge sentenced to 51 years for public office abuse

[Here's how you know](#)



Former Santa Cruz County treasurer sentenced to 10 years in prison for stealing over \$38 million in county funds

Date: June 24, 2025

Contact: newsroom@ci.irs.gov 

Tucson, AZ — Elizabeth Gutfahr, of Rio Rico, Arizona, was sentenced on June 23, 2025, by United States District Judge Rosemary C. Márquez to 120 months in prison, followed by three years of supervised release. Gutfahr previously pleaded guilty to Embezzlement by a Public Official, Money Laundering, and Tax Evasion. Gutfahr was also ordered to pay approximately \$51.8 million in restitution to Santa Cruz County and the United States Treasury.

“The people of Santa Cruz County and all Arizonans have a right to expect their elected leaders to serve with integrity and in the best interest of their constituents,” said U.S. Attorney Timothy Courchaine. “Ms. Gutfahr stole more than money from the people of her county, she betrayed the confidence of the voters who elected her. This sentence shows that abuse of public trust will be punished.”

“Ms. Gutfahr violated her sworn duty by enriching herself with the public money she was entrusted to protect,” said Special Agent in Charge Carissa Messick of the IRS Criminal Investigation Phoenix Field Office. “Taxpayers deserve to know that their elected leaders are working in the community’s best interest — not just their own. IRS-CI remains committed to rooting out corruption at every level.”

“Ms. Gutfahr will now be held accountable for using her official position for huge financial gain at the expense of the residents of Santa Cruz County,” said FBI Phoenix Special Agent in Charge Heith Janke. “Each act of greed and dishonor negatively affected fundamental aspects of the county’s operations. The FBI continues to investigate public corruption cases, and we remain committed to identifying and pursuing those who violate the public’s trust.”

According to court documents, Gutfahr, who served as Santa Cruz County Treasurer from 2012 through 2024, embezzled and laundered approximately \$38.7 million by wiring public funds from Santa Cruz County’s account to accounts in the names of fake companies she had created that performed no legitimate business. Gutfahr then used the money to purchase real estate, to renovate her family ranch, to pay expenses for her cattle business, and to buy at least 20 vehicles.

Gutfahr’s 10-year scheme involved approximately 187 wire transfers, which she was able to complete by undermining the two-step approval process required for transfers. Gutfahr used the token of a subordinate Santa Cruz County employee so that she could both initiate and approve the wire transfers. To cover up the scheme, Gutfahr falsified accounting records, cash reconciliation records, and reports of the County’s investment accounts, thereby hiding the millions of dollars that she had stolen from Santa Cruz County. Gutfahr also failed to report any of the stolen funds as income for tax purposes.

IRS-CI and the FBI conducted the investigation in this case. Assistant U.S. Attorney Jane L. Westby for the District of Arizona and Senior Litigation Counsel Nicholas W. Cannon of the Criminal Division’s Public Integrity Section handled the prosecution.

IRS Criminal Investigation (IRS-CI) is the law enforcement arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money laundering, public corruption, healthcare fraud, identity theft and more. IRS-CI special agents are the only federal law

enforcement agents with investigative jurisdiction over violations of the Internal Revenue Code, obtaining a 90% federal conviction rate. The agency has 19 field offices located across the U.S. and 14 attaché posts abroad.

 *News items may not be updated after their release. Please verify the date before relying on the language.*

Former Santa Cruz County Treasurer Elizabeth Gutfahr walks into court

Published: Jun. 23, 2025 at 4:55 PM CDT





Tucson synagogues boost security after attacks in Middle East

Updated: 13 hours ago

The attacks in Iran and the Middle East have sparked concern for some religious communities in Tucson, particularly the Jewish community, who are concerned about possible antisemitic attacks.



US-Israeli strikes spark mixed reactions from protestors, Iranian community in Tucson

Updated: 13 hours ago

Less than 48 hours after the U.S. began airstrikes on Iran, a couple dozen protestors gathered in downtown Tucson Monday evening to speak out against the decision by the administration of President Donald Trump.



Crews battle two-alarm house fire near First, River

Updated: 14 hours ago

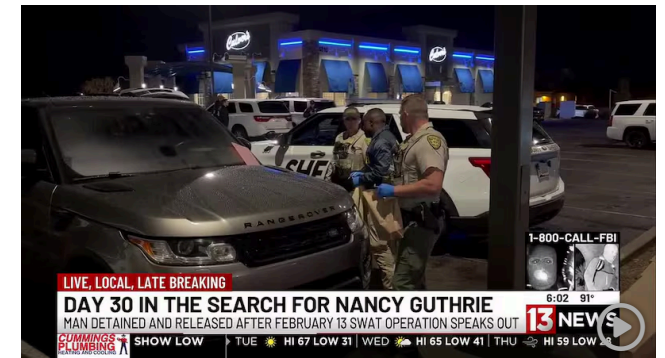
Crews responded to a two-alarm house fire near First and River on Monday, March 2. One person was transported to the hospital with injuries.



Two detained during Nancy Guthrie investigation speak out

Updated: 17 hours ago

Luke Daley and his mom, Mary Daley, sat down for an exclusive one-on-one interview with AZ Family's Briana Whitney.



Pima County opens Votemobile in time for RTA Next election

Updated: 17 hours ago

Pima County debuted its new mobile voting unit, called the "Votemobile," in Sells on Monday, March 2.



[News](#)

[Contact Us](#)

[13 Cares For Health](#)

[Weather](#)

[Community](#)

[Coronavirus](#)

[Sports](#)

[TV Schedule](#)

KOLD

7831 N. Business Park

Drive

Here's how you know



Former CEO of Guam helicopter company sentenced to 405 months in federal prison for criminal aviation violations

Date: June 12, 2025

Contact: newsroom@ci.irs.gov ✉

Hagåtña, Guam — Shawn N. Anderson, United States Attorney for the Districts of Guam and the Northern Mariana Islands, announced that John D. Walker was sentenced on June 9, 2025 by Chief Judge Frances Tydingco-Gatewood in the District Court of Guam to 405 months imprisonment. On September 9, 2022, a jury returned guilty verdicts against Walker and his company, Hansen Helicopters, Inc., on 110 counts involving conspiracy to defraud the Federal Aviation Administration (“FAA”) and National Transportation Safety Board (“NTSB”), aircraft parts fraud that caused serious bodily injury and death, employing a mechanic without a mechanic’s certificate, registration violations involving helicopters, conspiracy to commit wire fraud, wire fraud, and money laundering. Walker was also ordered to pay a \$250,000 fine, and a

\$9,900 special assessment fee. Walker forfeited \$58,407,513, which represented the proceeds of aircraft parts fraud and wire fraud, in addition to \$11,770,000, which represented the amount of money involved in the money laundering offenses.

Hansen Helicopters, Inc., was found guilty of conspiracy to defraud the FAA and NTSB, in addition to aircraft parts fraud that caused serious bodily injury and death. Hansen received a five-year term of probation, a \$4,900,000 fine, and a \$2,000 special assessment fee.

Walker subverted aviation laws and regulations, enforced by the FAA and NTSB, which protect public health and safety. Walker used at least 48 shell companies, most incorporated internationally, to operate an illicit helicopter/pilot/mechanic leasing business in Guam. By concealing that his aircraft were unregistered or illegally registered, unairworthy, and maintained and operated by uncertificated airmen, Walker entered fraudulent lease agreements with numerous tuna boat companies. He earned over \$400 million dollars through his scheme. He concealed his crimes by forging documents, counterfeiting aircraft parts, and bribing aviation officials.

“The defendants built helicopters from an assortment of discarded frames and counterfeit parts,” stated United States Attorney Anderson. “They blatantly disregarded aviation laws to build and operate aircraft that should never have left the ground. Fishing companies throughout the Pacific region relied on these aircraft for spotting tuna. Unfortunately, the defendants’ quest for money resulted in the deaths of many pilots. This was a difficult case to investigate and prosecute, but well worth federal resources. I commend our law enforcement partners on bringing these defendants to justice.”

“How many times have we heard, ‘It’s just money...’ when it comes to financial crime?” asked Special Agent in Charge Adam Jobes, IRS Criminal Investigation (IRS-CI), Seattle Field Office. “This case shows that all too often, innocent people suffer catastrophic harm because of someone else’s greed. Financial crime is not victimless, and IRS-CI will continue to protect our communities from people like Mr. Walker who put their greed above all else.”

“Unchecked greed and flagrant disregard for aviation safety create a recipe for disaster with catastrophic results,” said Special Agent in Charge Cory LeGars of the Department of Transportation Office of Inspector General, Western Region. “This sentencing epitomizes the criminal justice system’s commitment to holding

individuals and companies accountable for egregious illicit conduct. I commend the relentless efforts of our special agents and the outstanding collaboration between our law enforcement, prosecutorial, and regulatory partners, whose collective efforts brought this complex and hazardous fraud scheme to justice.”

“Over several years, Mr. Walker engaged in a multi-layered scheme to bribe public officials and defraud the government, significantly jeopardizing public safety in the process,” said FBI Honolulu Special Agent in Charge David Porter. “The FBI remains steadfast and persistent in our efforts to investigate these schemes and bring bad actors to justice.”

This investigation was conducted by the Internal Revenue Service Criminal Investigation, U.S. Department of Transportation, Federal Aviation Administration, Federal Bureau of Investigation, and in partnership with the Customs and Quarantine Agency of Guam.

Assistant United States Attorney Stephen F. Leon Guerrero, Special Assistant United States Attorney Marie L. Miller, and former Assistant U.S. Attorney Samantha R. Miller prosecuted this case.

IRS Criminal Investigation (IRS-CI) is the law enforcement arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money laundering, public corruption, healthcare fraud, identity theft and more. IRS-CI special agents are the only federal law enforcement agents with investigative jurisdiction over violations of the Internal Revenue Code, obtaining a 90% federal conviction rate. The agency has 19 field offices located across the U.S. and 14 attaché posts abroad.

 *News items may not be updated after their release. Please verify the date before relying on the language.*

Ex-Hansen Helicopters CEO Sentenced to 33 Years

CEO was found guilty of fraud related to unapproved aircraft parts



Hansen Helicopters CEO John Walker was convicted Friday on more than 100 counts related to fraud, bribery, and money laundering related to his Guam-based helicopter operation. A number of accidents have been associated with that operation. © U.S. Attorney's office

June 10, 2025

Former Hansen Helicopters CEO John D. Walker, 60, today was sentenced by federal judge Frances Tydingco-Gatewood to 33 years and nine months of confinement, meaning he likely will spend the rest of his life in federal prison. Walker [was convicted](#) of multiple counts of aircraft parts fraud, bribery, money laundering, and employing unlicensed pilots and mechanics by a jury in the Guam District Court in 2022 after an eight-month trial and has been in custody since. He will be credited for time served.

He was also fined \$250,000 and ordered to serve three years of supervised release and to forfeit all assets connected to the crimes. The government estimated this amount at \$400 million, but used Hansen's net sales over decades to calculate the amount. The actual value of his assets is around \$58 million, according to court documents, including thousands of acres of Missouri farmland and a large collection of personal aircraft.

Hansen operated a fleet of 50 Hughes 369 helicopters for tuna spotting in the northwestern Pacific. The government charged that Walker, who purchased Hansen in 1998, conducted a decades-long, wide-reaching fraud scheme that involved using counterfeit aircraft parts and data plate swapping to create a fleet of "Frankenstein helicopters" registered to a variety of international shell companies.

The U.S. government asserted that his behavior was responsible in part for up to 30 crashes that claimed nine lives. Walker was one of several Hansen executives and suppliers originally indicted in 2018, along with former FAA inspector Timothy Cislo. Other defendants have either died, reached plea deals with prosecutors, or had their cases dismissed.

Walker was the first to be sentenced. He declined to make a statement in court during his sentencing.

https://www.guampdn.com/news/hansen-helicopters-ceo-forfeited-more-than-70m/article_673c1ffc-11a1-4534-890d-725e1bed6a0d.html

TOP STORY

Hansen Helicopters CEO forfeited more than \$70M

Pacific Daily News

Jun 12, 2025



Hansen Helicopter Inc. owner John D. Walker Hansen, left, is escorted away from the District Court of Guam by his attorney, Mack Martin, after his initial appearance before the court on June 8, 2018.

PDN file photo

In addition to an almost 34-year federal prison sentence, Hansen Helicopters Inc. president and CEO John D. Walker forfeited more than \$70 million, according to a news release from the U.S. Attorney's Office.

Walker and his company were sentenced in the District Court of Guam this week after being convicted of 110 counts involving:

- Conspiracy to defraud the Federal Aviation Administration and the National Transportation Safety Board.
- Aircraft parts fraud that caused serious injury and death.
- Employing a mechanic without a mechanic's certificate.
- Registration violations involving helicopters.
- Conspiracy to commit wire fraud, wire fraud, and money laundering.

In addition to a \$250,000 fine and a \$9,900 special assessment fee, Walker forfeited \$58,407,513 representing the proceeds of aircraft fraud and wire fraud, and \$11,770,000 representing money involved in money laundering expenses, according to prosecutors.

“The defendants built helicopters from an assortment of discarded frames and counterfeit parts,” stated U.S. Attorney Shawn N. Anderson. “They blatantly disregarded aviation laws to build and operate aircraft that should never have left the ground.”

Anderson said fishing companies throughout the Pacific region relied on these aircraft for spotting tuna.

“Unfortunately, the defendants’ quest for money resulted in the deaths of many pilots. This was a difficult case to investigate and prosecute, but well worth federal resources. I commend our law enforcement partners on bringing these defendants to justice,” he said.

Hansen Helicopters Inc. was found guilty of conspiracy to defraud the FAA and NTSB, in addition to aircraft parts fraud that caused serious bodily injury and death. Hansen received a five-year term of probation, a \$4,900,000 fine, and a \$2,000 special assessment fee.

Walker used at least 48 shell companies, most incorporated internationally, to operate an illicit helicopter/pilot/mechanic leasing business on Guam.

By concealing that his aircraft were unregistered or illegally registered, unairworthy, and maintained and operated by uncertificated airmen, Walker entered fraudulent lease agreements with numerous tuna boat companies.

He earned more than \$400 million through his scheme, prosecutors said. He concealed his crimes by forging documents, counterfeiting aircraft parts, and bribing aviation officials.

During the trial, prosecutors said the company’s activities were linked to nine deaths and 16 serious injuries.

“Unchecked greed and flagrant disregard for aviation safety create a recipe for disaster with catastrophic results,” said Special Agent in Charge Cory LeGars of the Department of Transportation Office of Inspector General, Western Region. “This sentencing epitomizes the criminal justice system’s commitment to holding individuals and companies accountable for egregious illicit conduct.”

Walker, 60, was sentenced to 33 years and nine months in prison. He has been in custody since September 2022, so with credit for time served, he still has about 31 years left in federal prison.

“How many times have we heard, ‘It’s just money..’ when it comes to financial crime?” asked Special Agent in Charge Adam Jobs, IRS Criminal Investigation, Seattle Field Office. “This case shows that all too often, innocent people suffer catastrophic harm because of someone else’s greed. Financial crime is not victimless.”

The investigation was conducted by the U.S. Department of Transportation, Federal Aviation Administration, Internal Revenue Service Criminal Investigation, the Federal Bureau of Investigation, and in partnership with the Guam Customs and Quarantine Agency.

Walker and other company officials were indicted in the case in 2018.

Could not connect to the reCAPTCHA service. Please check your internet connection and reload to get a reCAPTCHA challenge.

Here's how you know



Arizona woman sentenced for \$17M information technology worker fraud scheme that generated revenue for North Korea

Date: July 24, 2025

Contact: newsroom@ci.irs.gov ✉

An Arizona woman was sentenced today to 102 months in prison for her role in a fraudulent scheme that assisted North Korean Information Technology (IT) workers posing as U.S. citizens and residents with obtaining remote IT positions at more than 300 U.S. companies. The scheme generated more than \$17 million in illicit revenue for Chapman and for the Democratic People's Republic of Korea (DPRK or North Korea).

Christina Marie Chapman, of Litchfield Park, Arizona, pleaded guilty on Feb. 11 in the District of Columbia to conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to launder monetary instruments. In addition to the 102-month prison term, U.S. District Court Judge Randolph D. Moss ordered

Chapman to serve three years of supervised release, to forfeit \$284,555.92 that was to be paid to the North Koreans, and to pay a judgment of \$176,850.

“Christina Chapman perpetrated a years’ long scheme that resulted in millions of dollars raised for the DPRK regime, exploited more than 300 American companies and government agencies, and stole dozens of identities of American citizens,” said Acting Assistant Attorney General Matthew R. Galeotti of the Justice Department’s Criminal Division. “Chapman made the wrong calculation: short term personal gains that inflict harm on our citizens and support a foreign adversary will have severe long-term consequences. I encourage companies to remain vigilant of these cyber threats, and warn individuals who may be tempted by similar schemes to take heed of today’s sentence.”

“North Korea is not just a threat to the homeland from afar. It is an enemy within. It is perpetrating fraud on American citizens, American companies, and American banks. It is a threat to Main Street in every sense of the word,” said U.S. Attorney Jeanine Ferris Pirro for the District of Columbia. “The call is coming from inside the house. If this happened to these big banks, to these Fortune 500, brand name, quintessential American companies, it can or is happening at your company. Corporations failing to verify virtual employees pose a security risk for all. You are the first line of defense against the North Korean threat.”

“Today’s sentencing brings justice to the victims whose identities were stolen for this international fraud scheme,” said Special Agent in Charge Carissa Messick of the IRS Criminal Investigation (IRS-CI) Phoenix Field Office. “The scheme was elaborate. If this sentencing proves anything, it’s that no amount of obfuscation will prevent IRS-CI and our law enforcement partners from tracking down those that wish to steal the identities of U.S. nationals, launder money, or engage in criminality that jeopardizes national security.”

“The North Korean regime has generated millions of dollars for its nuclear weapons program by victimizing American citizens, businesses, and financial institutions,” said Assistant Director Rozhavsky of the FBI’s Counterintelligence Division. “However, even an adversary as sophisticated as the North Korean government can’t succeed without the assistance of willing U.S. citizens like Christina Chapman, who was sentenced today for her role in an elaborate scheme to defraud more than 300 American companies by

helping North Korean IT workers gain virtual employment and launder the money they earned. Today's sentencing demonstrates that the FBI will work tirelessly with our partners to defend the homeland and hold those accountable who aid our adversaries.”

“The sentencing today demonstrates the great lengths to which the North Korean government will go in its efforts and resources to fund its illicit activities. The FBI continues to pursue these threat actors to disrupt their network and hold those accountable wherever they may be,” said Special Agent in Charge Heith Janke of the FBI Phoenix Field Office.

The case involved one of the largest North Korean IT worker fraud schemes charged by the Department of Justice, with 68 identities stolen from victims in the United States and 309 U.S. businesses and two international businesses defrauded.

According to court documents, North Korea has deployed thousands of highly skilled IT workers around the world, including to the United States, to obtain remote employment using false, stolen, or borrowed identities of U.S. persons. To circumvent controls employed by U.S. companies to prevent the hiring of illicit overseas IT workers, the North Korean IT workers obtain assistance from U.S.-based collaborators.

Chapman helped North Korean IT workers obtain jobs at 309 U.S. companies, including Fortune 500 corporations. The impacted companies included a top-five major television network, a Silicon Valley technology company, an aerospace manufacturer, an American car maker, a luxury retail store, and a U.S. media and entertainment company. Some of the companies were targeted by the IT workers, who maintained a repository of postings for companies that they wanted to employ them. The IT workers also attempted to obtain employment at two different U.S. government agencies, although these efforts were generally unsuccessful.

Chapman operated a “laptop farm” where she received and hosted computers from the U.S. companies at her home, deceiving the companies into believing that the work was being performed in the United States. Chapman also shipped 49 laptops and other devices supplied by U.S. companies to locations overseas, including multiple shipments to a city in China on the border with North Korea. More than 90 laptops were seized from Chapman’s home following the execution of a search warrant in October 2023.

Christina Chapman organized and stored U.S. company laptops in her home, and included notes identifying the U.S. company and identity associated with each laptop.

Much of the millions of dollars in income generated by the scheme was falsely reported to the IRS and Social Security Administration in the names of actual U.S. individuals whose identities had been stolen or borrowed. Additionally, Chapman received and forged payroll checks in the names of the stolen identities used by the IT workers and received IT workers' wages through direct deposit from U.S. companies into her U.S. financial accounts. Chapman further transferred the proceeds from the scheme to individuals overseas.

This case was investigated by the IRS-CI Phoenix Field Office, and the FBI Phoenix Field Office. Assistance was provided by the FBI Chicago Field Office.

Trial Attorney Ashley R. Pungello of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Karen P. Seifert for the District of Columbia prosecuted the case, with assistance from Paralegal Specialist Jorge Casillas. Assistant U.S. Attorney Joshua Rothstein for the District of Columbia, the Victim Witness Unit, the U.S. Attorney's Office for the District of Arizona, and the National Security Division's National Security Cyber Section also provided assistance.

In a coordinated effort, FBI Phoenix also issued guidance for HR professionals on detecting North Korean IT workers, and the Department of State issued guidance on the North Korean IT worker threat.

Prior guidance was issued by the FBI, State Department, and the Department of the Treasury on this threat in a May 2022 advisory, and by the United States and the Republic of Korea (South Korea) in October 2023. The FBI issued updated guidance in May 2024 regarding the use of U.S. persons acting as facilitators by providing a U.S.-based location for U.S. companies to send devices and a U.S.-based internet connection for access to U.S. company networks and in January 2025 concerning the extortion and theft of sensitive company data by North Korean IT workers, along with recommended mitigations.

IRS Criminal Investigation (IRS-CI) is the law enforcement arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money laundering, public corruption, healthcare fraud, identity theft and more. IRS-CI special agents are the only federal law

enforcement agents with investigative jurisdiction over violations of the Internal Revenue Code, obtaining a 90% federal conviction rate. The agency has 19 field offices located across the U.S. and 14 attaché posts abroad.

 *News items may not be updated after their release. Please verify the date before relying on the language.*

[Here's how you know](#)



In landmark sentence, Feeding Our Future scheme leader sentenced to 28 years in prison

Date: August 6, 2025

Contact: newsroom@ci.irs.gov 

MINNEAPOLIS – Today, United States District Judge Nancy E. Brasel sentenced Abdiaziz Shafii Farah, to 28 years in prison followed by 3 years of supervised release for his role in a \$300 million fraud scheme that exploited a federally funded child nutrition program during the COVID-19 pandemic, announced Acting U.S. Attorney Joseph H. Thompson. Farah was also ordered to pay restitution in the amount of \$47,920,514.

Farah played a leading and role in the Feeding Our Future case, the largest Covid-19 fraud scheme in the United States. According to public documents, Farah and his co-defendants stole more than \$47 million in program funds by claiming to serve 18 million meals to kids at more than 30 food distribution sites. In June 2024, after a seven-week trial before Judge Brasel, a federal jury convicted Farah of conspiracy to commit wire fraud, conspiracy to commit federal programs bribery, false statements in a passport application, conspiracy to commit money laundering, two counts of federal programs bribery, six counts of wire fraud, and 11 counts of money laundering.

Farah was the co-owner of Empire Cuisine & Market, an entity that he enrolled in the Federal Child Nutrition Program in April 2020, during the early days of the Covid-19 pandemic. Farah was among the very first defendants to see an opportunity for fraud and exploit it. Farah immediately opened a number of fraudulent program sites and began falsely claiming to serve meals to thousands of children per day. Many of the purported “sites” served no meals at all and were nothing more than parking lots or vacant commercial spaces.

Farah and his co-defendants “papered-up” the fraudulent scheme, including by creating and submitting fraudulent meal counts and invoices. Farah was likewise involved in the scheme’s use of phony rosters with fake children’s names. Few of the names on the rosters matched the names of real students attending the local school districts, and many of the names used by Farah were absurd and obviously fake, names like “Serious Problem” and “Britishy Melony.” In addition, Farah routinely directed the flow of fraudulent funds so that his co-conspirators got their “cuts” of the stolen taxpayer money. To keep the fraud going, Farah engaged in a corrupt “pay-to-play” system, where he paid thousands of dollars in bribes and kickbacks to personnel at Feeding Our Future and Partners in Nutrition.

Farah profited handsomely from his role in the scheme—he personally pocketed more than \$8 million during his 18 months of involvement in the fraud. As presented at trial, Farah sent text messages to his co-defendants about their ill-gotten gains, stating “in 7 months if things stay the same you are a multi millionaire with 0 debt” and “Bro the next multi legit millionaires will be me and you.”

Using the taxpayer money meant for needy kids, Farah purchased five luxury vehicles for himself in about six months, including over \$300,000 for a Porsche, a GMC truck, and a Tesla. Farah used approximately \$4.2 million in fraudulently-obtained taxpayer funds to purchase real estate throughout the Twin Cities and in Kentucky, which included buying two lakefront lots with the aim of building himself a multi-million-dollar home. Farah further sent the taxpayer money he stole overseas, purchasing real estate in Kenya and a high-rise apartment building in Nairobi. Farah laundered the fraud proceeds through China. This overseas money is beyond the reach of American law enforcement—neither these funds nor Farah’s international real estate holdings have been, or can be, seized or forfeited.

In January 2022, when the Feeding Our Future search warrants were executed, federal agents seized Farah's U.S. passport from his home. In the wake of those searches, Farah retained an attorney and was told he was a target of the federal investigation. Two months later, on March 22, 2022, Farah went to the Minneapolis Passport Agency in downtown Minneapolis to apply for a new U.S. passport. Farah lied on his passport application, falsely claiming his passport was lost, rather than seized by federal agents. Farah obtained a new U.S. passport that day. Less than two weeks later, Farah attempted to leave the country, purchasing a one-way ticket to Kenya, where he owned property paid for by the taxpayer money he stole. Law enforcement acted quickly to charge Farah with passport fraud and take him into custody.

In June 2024, at the conclusion of his 7-week trial, Farah and others attempted to bribe a juror with \$120,000 in cash in exchange for a not guilty verdict. Farah and four others were indicted in a separate federal case for the juror bribery scheme. Farah has pled guilty in the juror bribery case and is pending sentencing in that case before Judge David S. Doty. Today's sentence does not reflect Farah's attempt to bribe a juror; he will face an additional sentence in that case at a later date.

In imposing the 28-year sentence, Judge Brasel explained the defendant "came to this country as a refugee" and that "many of the opportunities" in Farah's life came through public agencies and non-profit organizations, noting that Farah received housing, school, a full-tuition college grant, and worked in the public sector. "Given that background, it is ironic at best that, as the government aimed no child went hungry during the pandemic, you saw the opportunity to fraudulently make money." Judge Brasel continued, "You achieved successes here in the United States and yet you've shown utter and flagrant disregard for the laws of the United States."

Judge Brasel found that Farah's crime was "breathtakingly elaborate" and that he acted out of "pure unmitigated greed." She told the defendant, "The repercussions of your crime will be felt in Minnesota and in your community—the refugee community—for a long time."

In arguing for a long sentence, Acting U.S. Attorney Joseph H. Thompson said, "This country gave Farah everything. A home. Citizenship. A free college education. After that he went on to public employment with the state of Minnesota. And how did he repay this country and this state? By robbing us blind. He has gotten

every opportunity, and this is how he used it. Farah didn't want the American dream. He wanted to be rich. He wanted to be wealthy. He thought he was entitled to it. He won the lottery of life, he was given everything by this country, and he repaid us with a life of crime. He has done untold damage to this state."

"Abdiaziz Shafii Farah's conviction serves as a stark reminder of the moral decay that can arise when individuals exploit systems designed to protect the most vulnerable among us," said Special Agent in Charge Alvin M. Winston, Sr. of FBI Minneapolis. "The egregious actions of Farah, who misappropriated over \$28 million meant to nourish underserved children during a critical time, exemplify a betrayal of societal trust. Today's sentence not only underscores the legal repercussions of such greed, but also sends a resounding message: Justice will not only be swift, but also unyielding. The FBI, in concert with our law enforcement partners and the Minnesota U.S. Attorney's Office remains committed to holding accountable those who prey on the most defenseless in our communities."

The case is the result of an investigation by IRS Criminal Investigation, the FBI, and the U.S. Postal Inspection Service.

Acting U.S. Attorney Joseph H. Thompson, and Assistant U.S. Attorneys Harry M. Jacobs, Matthew S. Ebert, and Daniel W. Bobier prosecuted the case. Assistant U.S. Attorney Craig Baune is handling the seizure and forfeiture of assets.

IRS Criminal Investigation (IRS-CI) is the law enforcement arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money laundering, public corruption, healthcare fraud, identity theft and more. IRS-CI special agents are the only federal law enforcement agents with investigative jurisdiction over violations of the Internal Revenue Code, obtaining a 90% federal conviction rate. The agency has 19 field offices located across the U.S. and 14 attaché posts abroad.

 *News items may not be updated after their release. Please verify the date before relying on the language.*