LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Did you know?

According to Statista, in the year 2025, the projected revenue in the Application Development Software market worldwide is expected to reach over $195 billion.

Keep that in mind as you read the last article featured in the newsletter - and the statistic that Apple is working hard to prevent about $2 billion in app fraud annually. For their part, Apple and Google are policing their platforms and stopping fraud, but the question that comes to mind: how much ***aren't*** they finding and preventing?

Board Positions

We still have a couple remaining board positions that need to be filled in our upcoming election. Keep in mind that the average time commitment is minimal for an at large board member, but could increase if you choose to hold an officer position or serve on the various committees (Newsletter, Social Media, Website, Membership, and Scholarship).

In This Issue

Fraud Talk Podcast

Fraud Prevention in Action: How Students Are Gaining Real-World Experience

In this episode of Fraud Talk, ACFE Content Manager Rihonna Scoggins speaks with Victor Cardona, adjunct professor of forensic accounting at California State Polytechnic University, Pomona, to discuss their "Day in the Life of an IRS Agent" program. The initiative immerses students in real-world forensic accounting and criminal investigation scenarios, offering a hands-on look at careers in fraud prevention and compliance. Cardona shares how interactive education, mentorship and networking are key to inspiring the next generation of anti-fraud professionals—and why promoting ethical standards early on is essential in shaping the future workforce.

https://acfe.podbean.com/e/fraud-prevention-in-action-how-students-are-gaining-real-world-experience-victor-cardona-fraud-talk-episode-155/

UPCOMING EVENTS

LOCAL:

Southeast Michigan Chapter of the ACFE Monthly Dinner Meeting
In-person: Vistatech Center at Schoolcraft College
June 5, 2025
Learn more: https://semcacfe.org/meetinginfo.php?id=109&ts=1746548283

MICPA: Fraud, Internal Controls and Ethics: Best Practices and Case Studies
In-person: Embassy Suites by Hilton Grand Rapids Downtown Grand Rapids, MI
June 10, 2025
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=178035&return=3~1

Michigan Chamber of Commerce: Leading with Conviction:
Navigating Change with Clarity and Integrity
Webinar
June 12, 2025
Learn more: Event Details

NATIONAL:

ACFE 36th Annual Global Fraud Conference
In-Person, Nashville Tennessee, or Virtual
June 22 - June 27, 2025
Learn more: https://www.fraudconference.com/36th-home.aspx
** Please let Mark Lee know (president@lansingacfe.org) if you plan to attend either in-person or virtually, as there is a group rate discount if 5 or more LACFE Chapter members attend**

ACFE Research Institute Annual Meeting
Nashville, Tennessee
June 26, 2025
Learn more: Event Details

ACFE Uncovering Fraud with Financial and Ratio Analysis
Virtual Seminar
July 16-17, 2025 (early registration ends June 18th)
Learn more: Event Details

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at newsletter@lansingacfe.com

The LACFE is always looking for volunteers to serve on the board, help with events, recommend training topics/speakers, grow our network to alert students to the LACFE scholarship, and more! Let us know if you can help be part of our growth!
Email: newsletter@lansingacfe.com

5 Key Trends in AI-Enabled Fraud Schemes Internal Auditors Must Watch in 2025

April 23, 2025
By Richard Chambers
https://www.richardchambers.com/5-key-trends-in-ai-enabled-fraud-schemes-internal-auditors-must-watch-in-2025/

Over the past few years, I've written and spoken extensively about the transformative impact of artificial intelligence (AI) on internal audit. From analytics and automation to risk sensing and assurance, AI has undoubtedly been a game changer. But as with any powerful tool, AI's potential cuts both ways. In 2025, we continue to witness a disturbing evolution—AI is no longer just enabling internal auditors to uncover fraud. It is increasingly being weaponized to commit fraud.

For internal auditors, the stakes couldn't be higher. AI-enabled fraud schemes are sophisticated, fast-moving, and often invisible to traditional controls. If we're not evolving alongside the threat, our organizations facing increasing exposure to these emerging risks.

Here are five key trends in AI-driven fraud that internal auditors must stay ahead of in 2025:

1. Deepfake-Fueled Social Engineering
In the early days of fraud, impersonation schemes involved phony emails or spoofed phone calls. As I wrote last year, many fraud schemes today involve hyper-realistic deepfake videos and synthetic voice clones of senior executives. Fraudsters are leveraging generative AI to mimic a CEO's voice or simulate a live video call to authorize illicit transactions, redirect wire transfers, or extract sensitive information.

One of the more legendary cases involved a finance employee wiring millions to a Hong Kong account after "speaking" with what appeared to be the CFO on a video call—only to learn later that the CFO was in a different country entirely. These schemes bypass traditional red flags because the AI is convincing enough to override suspicion.

Internal Audit's Response: We must work closely with cybersecurity, HR, and finance teams to assess controls over communication verification, especially in high-risk areas like treasury and procurement. Multi-channel verification protocols (e.g., voice plus SMS plus in-person confirmation) should be tested regularly. Internal auditors should also evaluate whether their organizations have trained employees on identifying deepfake fraud attempts.

2. AI-Generated Synthetic Identities
AI tools are now being used to create synthetic identities that are indistinguishable from real ones. These digital personas often pass background checks, generate employment histories, and even receive fraudulent benefits or loans. Banks, insurance companies, and government programs are particularly vulnerable to these identity fabrications.

What makes synthetic identity fraud especially dangerous is its latency—it may take years for these “phantom customers” to default or trigger an investigation. By then, the damage is already done.

Internal Audit’s Response: Review identity verification processes, especially in customer onboarding, HR hiring, and vendor due diligence. Are there analytics in place to detect anomalies across seemingly separate but subtly linked identities? Has the organization implemented biometric or behavioral authentication? Internal audit can add significant value by recommending advanced verification mechanisms that go beyond static data.

3. AI-Powered Insider Threats
Insider fraud is not new, but AI is making it more potent. Employees or contractors can now use AI to scrape data, manipulate financial systems, or exploit vulnerabilities at scale. Imagine a malicious actor using a generative AI model to write tailored phishing campaigns against coworkers—or an insider using machine learning to identify and exploit gaps in compliance patterns.

Moreover, generative AI makes it easier to erase footprints. Unlike traditional fraud, which often leaves behind emails, logs, or handwritten records, AI-assisted schemes can self-delete, making forensic reviews more challenging.

Internal Audit’s Response: Internal auditors must broaden their views of insider risk. Look beyond traditional behavioral monitoring and consider the AI tools employees have access to—both formally and informally. Collaborate with IT and HR to monitor privileged access, usage of generative AI platforms, and any deviation from expected digital behaviors.

4. AI-Driven Financial Manipulation
From manipulating market sentiment with fake news to auto-generating fictitious invoices, fraudsters are now using AI to commit fraud at scale. Shell companies can be created and populated with AI-generated documentation. Chatbots can convincingly “communicate” as fake vendors. And perhaps most concerning, AI tools can fabricate documents so well—audits, contracts, bank statements—they pass cursory reviews undetected.

In one case, a mid-sized company unknowingly paid nearly $500,000 to an AI-generated shell entity that had successfully mimicked the look and tone of a legitimate supplier, including cloned email threads and authentic-looking vendor documents.

Internal Audit’s Response: Auditors should evaluate how the company verifies supplier authenticity and invoice legitimacy. Incorporate AI-based tools into audit procedures to perform anomaly detection in payment patterns, vendor creation processes, and invoice formatting. Use your own AI tools to fight AI-driven fraud—this is one battleground where technological parity matters.

5. AI-Augmented Money Laundering and Cryptocurrency Fraud
Cryptocurrency fraud is nothing new, but as Lucinity recently observed, AI is giving money launderers powerful new tools to evade detection. Sophisticated AI algorithms are now being used to layer transactions, obscure crypto flows, and mimic legitimate behavior. These tools can automatically adjust laundering strategies based on real-time feedback, making traditional compliance rulesets increasingly obsolete.

Some fraudsters are even using AI to identify regulatory gaps in global jurisdictions to exploit weak enforcement environments.

Internal Audit's Response: If your company deals in digital assets or has exposure to cryptocurrency, now is the time to upskill. Ensure your audit team understands blockchain tracing tools, smart contract risks, and the evolving landscape of AI-driven crypto fraud. Evaluate the effectiveness of anti-money laundering (AML) controls and recommend enhancements where traditional models fall short.

Final Thoughts
The rise of AI-enabled fraud isn't just a cybersecurity issue. It's a governance and assurance issue. And it's one internal audit cannot afford to ignore.

We must become more technologically literate, more agile, and more connected to emerging risks than ever before. The fraud landscape of 2025 is dynamic, deceptive, and digitally sophisticated. But internal auditors—armed with curiosity, skepticism, courage, and the right tools—can still stay one step ahead.

We've done it before, and we can do it again. But only if we commit to evolving as fast as the risks we're entrusted to assess.

Stay vigilant. Stay curious. Stay ahead.

Video of the Month

Freedom of Information and Privacy Act · Kohn, Kohn & Colapinto LLP

Whistleblowing for federal employees is complicated by potential conflicts with special interests and political pressures. The Privacy Act of 1974 provides crucial protections by ensuring individuals can access and correct their federal records. This act also serves to limit government sharing of their personal information, and prevents the creation of records on their First Amendment activities. Furthermore, it enables individuals to seek legal redress for violations of these protections.

Heightened False Claims Act Enforcement Risks Highlight the Importance of Compliance

May 21, 2025
https://www.velaw.com/insights/heightened-false-claims-act-enforcement-risks-highlight-the-importance-of-compliance/

Despite signs of a retrenchment in some of the traditional areas of white collar enforcement under the Trump administration, the U.S. Department of Justice's ("DOJ") enforcement of the civil False Claims Act ("FCA") appears likely to proceed at a steady and aggressive pace amid a renewed focus on waste, fraud, and abuse and a recent jump in the number of new qui tam actions.

DOJ's enforcement of the FCA (31 U.S.C. §§ 3729-3733)—the government's primary civil remedy to combat fraud against the government—tends to be relatively stable from one administration to the next, and DOJ has typically recovered billions of dollars of settlements and judgments under the statute every year. There are several indications, however, that the FCA will play an even more central role in a wide variety of areas involving government programs and funds. In the first few months of the Trump administration, DOJ has announced more than 40 settlements with defendants resolving alleged FCA violations in cases alleging fraud involving defense contracting, pharmaceutical manufacturing, health insurance, pandemic relief funds, and customs. DOJ has also filed a brief in a pending case defending the constitutionality of the qui tam statute against attack, signaling DOJ's support for whistleblower suits alleging fraud. Also, a surge in the number of qui tam actions filed in Fiscal Year 2024 (979)—the highest number in a single year—produced a fresh pipeline of new DOJ investigations,1 which often take years to resolve. For government contractors, the picture is gaining complexity based upon the administration's initiatives to overhaul the federal procurement system and streamline regulations on short timetables. In the fast-changing regulatory and enforcement climate, now is the time for companies receiving government funding to strengthen and adapt their compliance programs and internal controls to account for these new risks.

In this update, we highlight key developments under the new administration, provide an overview of recent FCA settlements and enforcement actions in two key areas—cybersecurity and international trade— and summarize high-level takeaways.

Recent Administration Actions Related to FCA Enforcement

Several signs indicate that the FCA will continue, and likely increase, as an important enforcement tool in the new administration.

For example, in a case before the U.S. Court of Appeals for the 11th Circuit focusing on the constitutionality of the qui tam statute, DOJ has defended the qui tam process against challenge.2 In a reply brief filed on April 30, 2025, in United States ex rel. Zafirov v. Fla. Med. Associates, LLC, the government argued that the U.S. District Court for the Middle District of Florida erred when it struck down the qui tam statute as a violation of the Appointments Clause.3 In a novel decision breaking with past precedent issued by the U.S. District Court for

the Middle District of Florida, the district court held that relators pursuing qui tam cases act as officers of the United States that therefore must be appointed by the President. On appeal, DOJ intervened, arguing that, according to the government, relators are not officers of the United States, and do not exercise executive power in a manner inconsistent with Article II of the Constitution. Qui tam suits filed under seal in district courts nationwide produce the large majority of FCA cases year after year. According to DOJ's public statistics, more than $2.4 billion of the more than $2.9 billion in FCA settlements and judgments recovered in Fiscal Year 2024 arose from qui tam cases.4 Zafirov has potentially seismic implications for FCA enforcement. In the meantime, DOJ's position in Zafirov sends a clear message to whistleblowers and their counsel that DOJ will continue to support new qui tam cases.

In a Criminal Division memorandum published on May 12, 2025, DOJ reemphasized its commitment to priority areas of white-collar enforcement, specifically identifying procurement fraud, healthcare fraud, and trade and customs fraud, among other areas.5 Although FCA litigation is overseen by the Civil Division (specifically, the Civil Fraud Section in the Commercial Litigation Branch), the Criminal Division's enforcement priorities and policies are indicative of the administration's approach to general corporate enforcement, including civil FCA cases, which can sometimes involve parallel criminal proceedings.

Also, senior DOJ officials have publicly reaffirmed their commitment to supporting qui tam whistleblowers and enforcing the FCA. In remarks before the Federal Bar Association's annual Qui Tam conference in February 2025, the recently departed Deputy Assistant Attorney General ("DAAG") of Commercial Litigation in DOJ's Civil Division, Michael Granston, emphasized that DOJ will pursue "aggressive" enforcement of the FCA "consistent with the new administration's stated focus on achieving governmental efficiency and rooting out waste, fraud, and abuse."6 DAAG Granston, who has been a steadfast leader in the FCA space during his three decades of public service at DOJ, highlighted areas of focus to include illegal foreign trade practices. The FCA could thus play a prominent role in the context of the administration's high-profile tariff policies.

Another significant development is the administration's recent focus on enforcement regarding alleged discrimination related to diversity, equity, and inclusion ("DEI") policies and certifications. In a recent memorandum issued by Deputy Attorney General Todd Blanche, DOJ announced a Civil Rights Fraud Initiative that will use the FCA to pursue claims where illegal discrimination is alleged to have occurred, strongly encouraging qui tam lawsuits in this area.7 Relatedly, President Trump has reinforced this commitment by specifically referencing the FCA in an Executive Order ("EO") targeting DEI programs and certifications among government contractors.8 The EO, titled "Ending Illegal Discrimination and Restoring Merit-Based Opportunity," contains specific language directing the inclusion of new terms in government contracts and grants making compliance with "applicable" federal anti-discrimination laws "material" for FCA purposes, and calling for a new requirement that contractors certify that they do not "operate any programs promoting DEI that violate any applicable Federal anti-discrimination laws."9 Enforcement of the EO is the subject of pending litigation and injunction orders, thus the timing regarding enforcement remains in judicial limbo. Nevertheless, it is notable that the administration included specific references to the FCA in an Executive Order.

The prospect of heightened FCA risks comes at a time of significant regulatory change for government contractors. A series of additional EOs implemented by President Trump focusing on overhauling the federal procurement system and the Federal Acquisition Regulation ("FAR") is likely to result in major changes for contractors, underscoring the importance of robust compliance programs.10

Recent FCA Settlements & Enforcement Actions

Several recent DOJ enforcement actions highlight two areas of increased FCA enforcement risk: cybersecurity for government contractors and international trade.

Cybersecurity

United States ex rel. Berich v. MORSECORP Inc. et al.

On March 26, 2025, DOJ announced a $4.6 million settlement with MORSECORP Inc. ("MORSE") over allegations that MORSE failed to comply with cybersecurity requirements in various contracts with the Departments of the Army and Air Force in violation of the FCA.11 In the complaint, DOJ alleged that MORSE knowingly submitted false or fraudulent payment claims despite having knowledge of non-compliance with required Department of Defense ("DoD") cybersecurity measures for safeguarding sensitive government information.12 In turn, DOJ stated that these false representations and false submissions fraudulently induced the government to award MORSE tens of millions of dollars in contracts with DoD.13

In this qui tam case filed under the FCA's whistleblower provision, the relator will receive an $851,000 share of the settlement amount.

United States ex rel. Doe v. Raytheon Co. et al.

On May 1, 2025, DOJ announced a $8.4 million settlement with Raytheon and other affiliated entities ("Raytheon") stemming from purported violations of the FCA related to cybersecurity non-compliance in contracts with DoD.14 More specifically, the government alleged that Raytheon failed to implement and comply with federal cybersecurity regulations—such as those contained in the Defense Federal Acquisition Regulation Statement ("DFARS") and the FAR—in their performance of cyber offense capabilities and other services, despite certifying its compliance to DoD.15 These false certifications or representations of compliance allegedly fraudulently induced DoD to enter into and renew the contracts at issue and were material to DoD's decision to reimburse otherwise ineligible claims for payment.16

Because this was also a qui tam lawsuit initially filed by a former employee of Raytheon, the whistleblower will receive approximately $1.5 million of the settlement.

International Trade

United States ex rel. Urban Global LLC v. Struxtur, Inc, et al.

On March 25, 2025, DOJ announced a $8.1 million FCA resolution with Evolutions Flooring Inc. ("Evolutions"), a California-based importer of multilayered wood flooring, and its owners.17

According to the government, Evolutions knowingly submitted false information to U.S. Customs and Border Protection ("CBP") regarding the country of origin and identity of wood flooring manufactured in China and imported into the United States. This alleged conduct allowed the company to avoid paying applicable antidumping, countervailing, and Section 301 duties (which are extra tariffs imposed on imports to address unfair, unreasonable or discriminatory trade practices). The complaint invoked the "reverse false claims" provision of the FCA,18 which imposes liability on persons who knowingly conceal or improperly avoid payment obligations to the government.19

The case originated from a qui tam lawsuit filed by a competitor. Under the settlement, the relator will receive approximately $1.2 million of the settlement proceeds.

United States ex rel. Lee v. Barco Uniforms Inc., et al.

In another recent case signaling a potential uptick in customs fraud cases, on April 18, 2025, DOJ announced that it was intervening in a case in district court in California alleging that Barco Uniforms Inc. ("Barco"), two of its executives, and several affiliates, were involved in a scheme to underpay customs duties on imported apparel.20

According to the government's allegations, the defendants conspired to misrepresent the value of goods purchased from foreign suppliers in order to avoid or reduce the amount of customs duties owed.21 Specifically, the complaint asserts that the defendants used a double-invoicing scheme, submitting false entry summaries to CBP that deliberately undervalued imported products, thereby reducing their reported duty obligations.22

As with the Evolutions Flooring matter, this case was initiated through a qui tam lawsuit (this time brought by a former Barco employee).

Key Takeaways

By all indications, FCA risks remain significant for companies doing business with the government or receiving government funds. This is especially true in light of the continued role of whistleblowers in driving FCA investigations. As a result, businesses should remain vigilant and forward leaning in their compliance efforts. Especially with major changes in the federal procurement system underway, it is critical for government contractors to proactively strengthen their internal controls and focus on advancing compliance to specifically address new risks.

Likewise, companies involved in imports need to consider FCA risks. Companies importing goods subject to antidumping, countervailing, or Section 301 duties are particularly exposed, as even inadvertent errors or misstatements on import documentation can give rise to potential investigations and allegations of fraud, even if ultimately without merit.

The following best practices can help mitigate FCA risk:

- Review Compliance Programs: Conduct targeted assessments of existing compliance programs and consider engaging counsel to assist with updating policies and procedures to ensure alignment with evolving regulatory requirements and risk areas.

- Oversee Third Parties: Closely monitor third parties (including subcontractors, vendors, and partners) to ensure that contractual agreements require adherence to your company's compliance standards and flow-down requirements under prime contracts.
- Employee Training: Implement comprehensive training programs for employees to ensure awareness of applicable regulations and FCA exposure.
- Internal Reporting and Whistleblower Protections: Establish robust internal reporting mechanisms and whistleblower protections to identify and address potential violations before they escalate.
- Mandatory Disclosures and Contractor Code of Business Ethics and Conduct: Companies with government contracts subject to standard acquisition clauses should be familiar with their obligations to timely disclose to the government when they possess "credible evidence" of an FCA violation (and certain criminal violations) in connection with the award, performance, or closeout of their government contracts (FAR 52.203-13). Failure to report a mandatory disclosure can be grounds for potential suspension or debarment. Contractors subject to this clause are also required to have a written code of business ethics and conduct.

By adopting these measures, companies can reduce their risk of FCA liability and demonstrate a strong commitment to compliance with applicable laws, regulations, and contract requirements.

Apple Blocks $9 Billion in Fraud Over 5 Years Amid Rising App Store Threats

May 28, 2025
by Ravie Lakshmanan
https://thehackernews.com/2025/05/apple-blocks-9-billion-in-fraud-over-5.html

Apple on Tuesday revealed that it prevented over $9 billion in fraudulent transactions in the last five years, including more than $2 billion in 2024 alone.

The company said the App Store is confronted by a wide range of threats that seek to defraud users in various ways, ranging from "deceptive apps designed to steal personal information to fraudulent payment schemes that attempt to exploit users."

The tech giant said it terminated more than 46,000 developer accounts over fraud concerns and rejected an additional 139,000 developer enrollment as part of efforts to prevent bad actors from submitting their apps to the App Store.

Furthermore, the company said it rejected over 711 million customer account creations and deactivated nearly 129 million customer accounts last year with an aim to block these accounts from conducting nefarious activity, such as spamming or manipulating ratings and reviews, charts, and search results that could compromise the integrity of the App Store.

Some of the other noteworthy statistics shared by Apple for 2024 are listed below -

- Detected and blocked more than 10,000 illegitimate apps on pirate storefronts, which include malware, pornography apps, gambling apps, and pirated versions of legitimate apps from the App Store
- Stopped nearly 4.6 million attempts to install or launch apps distributed illicitly outside the App Store or approved third-party marketplaces
- Rejected more than 1.9 million App Store submissions for failing to meet its standards for security, reliability, privacy violations, or fraud concerns
- Removed more than 37,000 apps for fraudulent activity and rejected over 43,000 app submissions for containing hidden or undocumented features
- Rejected over 320,000 submissions that copied other apps, were found to be spam, or otherwise misled users, and another 400,000 app submissions for privacy violations.
- Removed more than 7,400 potentially fraudulent apps from App Store charts and nearly 9,500 deceptive apps from appearing in App Store search results
- Removed more than 143 million fraudulent ratings and reviews from the App Store
- Identified nearly 4.7 million stolen credit cards and banned over 1.6 million accounts from transacting again

In comparison, Apple said it prevented more than $1.8 billion in potentially fraudulent transactions in 2023 and over $2 billion in potentially fraudulent transactions in 2022. In 2023, Apple terminated close to 118,000 developer accounts.

The disclosure follows a similar report from Google earlier this year that it blocked over 2.36 million policy-violating Android apps from being published to the Google Play app marketplace in 2024 and banned more than 158,000 bad developer accounts that attempted to publish such harmful apps.

Apple's annual App Store fraud analysis also comes at a time when the company is facing increasing scrutiny over its App Store policies. A recent ruling in the United States ordered the iPhone maker to allow iOS apps to show links or buttons that direct customers to make purchases outside of the App Store.

Quote of the Month

“If you have integrity, nothing else matters. If you don't have integrity, nothing else matters.”

— Alan K. Simpson was an American politician from Wyoming. A member of the Republican Party, he served as a member of the United States Senate from 1979 to 1997.