LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

In This Issue

Fraud Talk Podcast

The Hidden Costs of Speaking Up: What Fraud Examiners Need to Know About Whistleblowers

Whistleblowers are often key to uncovering fraud—but what happens after they report? In this episode of Fraud Talk, Jacqueline Garrick, founder of Whistleblowers of America and the Workplace Promise Institute, shares her journey from whistleblower to advocate. From moral injury to PTSD, Garrick shares how peer support and trauma-informed workplaces can protect whistleblowers and strengthen fraud prevention efforts.

https://acfe.podbean.com/e/the-hidden-costs-of-speaking-up-what-fraud-examiners-need-to-know-about-whistleblowers-jacqueline-garrick-fraud-talk-episode-156/

UPCOMING EVENTS

LOCAL:

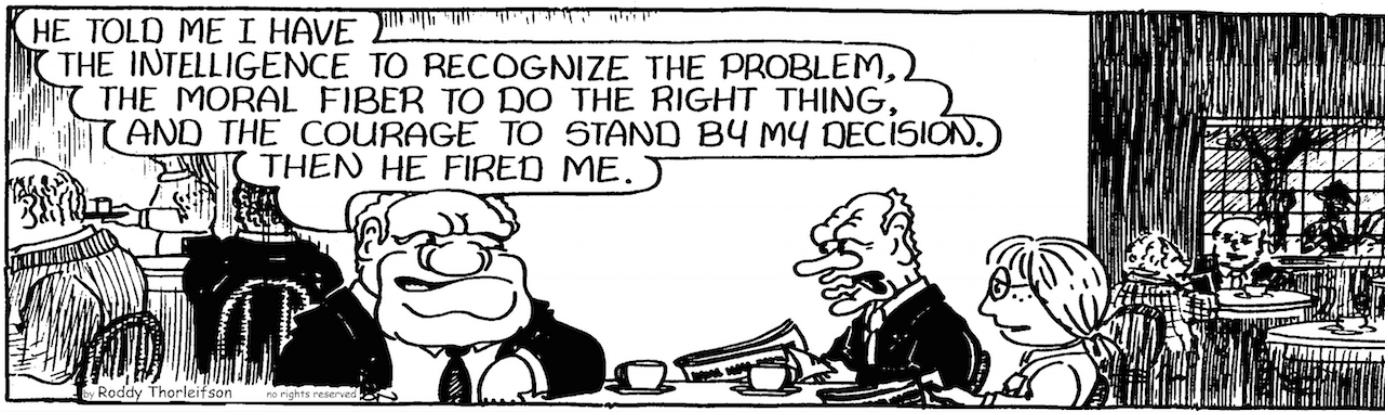
MICPA: 47th Annual Small Firm Practitioners Conference
In-person: Treetops Resort Gaylord, MI
August 13 - 14, 2025 (early registration ends July 16th)
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=1758458&return=1-1

NATIONAL:

ACFE Uncovering Fraud with Financial and Ratio Analysis
Virtual Seminar
July 16-17, 2025
Learn more: Event Details

ACFE Decoding Friendly Fraud: Strategies for Financial Institutions to Combat Emerging Risks
Virtual
July 29, 2025
Learn more: Event Details
This seminar is FREE for ACFEs in good standing!

ACFE Operation Desert Pond: A Case Study for Covert Investigative Techniques
Virtual
August 14, 2025
Learn more: Event Details



Courtesy of Moose Lake Cartoons https://mooselakecartoons.com/

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

Face Off: How Deepfake Identities Are Rewriting The Rules Of Financial Crime—And Why Compliance Must Catch Up

April 17, 2025
By Parya Lotfi
https://www.forbes.com/councils/forbestechcouncil/2025/04/17/face-off-how-deepfake-identities-are-rewriting-the-rules-of-financial-crime-and-why-compliance-must-catch-up/

Financial crime is evolving at a pace that regulators and compliance teams are struggling to match. While most financial institutions have invested heavily in fraud prevention, a new and insidious threat is slipping through the cracks—deepfake-generated synthetic identities.

Fraudsters no longer need stolen documents or hacked credentials; they can now fabricate entirely realistic personas that pass biometric authentication, clear "know your customer" (KYC) checks and gain full access to financial systems.

And they are doing so at scale. In 2023 alone, deepfake-related fraud attempts increased 700% in fintech—a staggering indicator of how criminals are weaponizing AI-powered deception.

Unlike traditional fraud, deepfakes introduce a fundamental identity risk problem for financial institutions. Today, a deepfake-generated selfie can pass liveness detection, a manipulated video can fool facial recognition and a synthetic voice can impersonate a CEO or compliance officer. The result? Unauthorized accounts, fraudulent transactions and systemic vulnerabilities that compliance frameworks were never designed to handle.

How Deepfake Identities Are Used For Money Laundering

Once fraudsters create a deepfake-based account, the real financial crime begins. Money laundering operations are increasingly leveraging synthetic identities to obscure illicit financial flows. Here’s how:

• Synthetic Account Creation: Fraudsters generate a deepfake identity—often a blend of real and fake biometric data—to bypass KYC verification at banks, fintech firms and crypto exchanges.

• Layering Through Digital Transactions: These synthetic accounts engage in seemingly legitimate activities—opening credit lines, initiating high-frequency transactions and routing money through multiple financial institutions to erase the trail.

• Mule Networks And Cashing Out: The laundered funds are ultimately withdrawn through crypto-to-fiat conversions, offshore transfers or ATM withdrawals using synthetic ID-linked payment cards.

• Scaling Through Fraud-As-A-Service (FaaS): Dark web marketplaces now sell ready-made deepfake identities, allowing even low-level criminals to access advanced laundering techniques.

Regulators have long relied on transaction monitoring and identity verification as cornerstones of anti-money laundering (AML) compliance. But when fraudulent identities appear real, these traditional methods can fall apart.

The Cost Of Inaction: A Multibillion-Dollar Problem

The financial sector has already suffered billions in losses due to AI-driven fraud. Deepfake scams are no longer a future risk—they are here right now:

• Financial institutions will lose an estimated $40 billion to AI-driven fraud by 2027, up from $12.3 billion in 2023.

• According to a Deloitte poll, 25.9% of financial executives reported experiencing at least one deepfake-related fraud incident in the past year (pg. 3).

• Almost 52% of financial executives expect deepfake-enabled fraud to increase in the next 12 months, highlighting the urgency for action (pg. 4).

• Despite this, 9.9% of organizations surveyed have taken no action against deepfake threats, leaving them wide open to risk (pg. 5).

Fraudsters are moving faster than financial institutions, and every delay in adapting compliance frameworks leaves organizations more vulnerable.

The Compliance Gap: Why AML And KYC Need An Urgent Upgrade

While banks and neobanks invest heavily in digital security, deepfake detection remains an overlooked gap in fraud prevention strategies. The challenge is that most KYC and AML compliance programs were designed for human fraudsters, not AI-generated identities.

• KYC verification needs AI-powered defense. Traditional KYC relies on document checks, facial recognition and liveness detection—all of which deepfakes can now bypass with shocking accuracy. Advanced AI-based detection can help identify synthetic identities before they infiltrate financial systems.

• Transaction monitoring alone isn’t enough. AI-generated fraud can mimic legitimate transaction behaviors, making it invisible to traditional monitoring tools. Compliance teams should integrate behavioral analysis and biometric authentication audits to flag anomalies.

• Manual review is unsustainable. A high-quality deepfake can be indistinguishable to human reviewers. Automated deepfake detection technologies can accelerate operational efficiency gains, allowing compliance teams to focus on real threats instead of false positives.

A Call To Action: The Time To Act

Financial institutions can no longer afford to ignore the deepfake threat. Fraudsters are already deploying synthetic identities at scale, and regulatory frameworks are years behind in addressing this risk.

To maintain trust, compliance and security, banks and fintech firms must:

• Embed deepfake detection into KYC and fraud prevention workflows to preempt synthetic identity fraud before accounts are approved.

• Conduct deepfake audits as part of AML compliance reviews to assess vulnerabilities across onboarding, authentication and transaction monitoring.

• Leverage AI-driven solutions that can adapt to evolving deepfake threats—because fraudsters are already doing the same.

The financial industry is at an inflection point. Deepfakes are no longer an emerging risk—they are here, reshaping financial crime in real time. Institutions that fail to adapt could face not only financial losses but also regulatory scrutiny, reputational damage and customer trust erosion.

The question is no longer if banks should act, but how.

And in the fight against financial crime, waiting is the worst strategy of all.

Video of the Month

Fraud as a Service: The Digital Crime Wave You Need to Know About

Discover how Fraud as a Service (FaaS) is revolutionizing cybercrime and what it means for your online security. This video exposes how criminal enterprises have industrialized fraud through subscription-based models that mimic legitimate businesses.

FBI warns scammers are posing as fraud investigators to steal sensitive healthcare info — what you need to know

July 2, 2025
By Anthony Spadafora
https://www.msn.com/en-us/news/technology/fbi-warns-scammers-are-posing-as-fraud-investigators-to-steal-sensitive-healthcare-info-what-you-need-to-know/ar-AA1HNcbm?ocid=BingNewsVerp

Scammers are targeting both patients and health care providers in a new phishing attack designed to steal your sensitive personal and financial data, according to a new alert from the FBI.

As reported by BleepingComputer, the federal law enforcement agency recently put out a public service announcement warning that scammers and other cybercriminals are currently impersonating health insurance companies and their respective fraud investigators in an effort to steal customer data.

According to the FBI, the scammers behind this new campaign are sending out phishing emails and text messages with the hope that potential victims will disclose their “protected health information, medical records, personal financial details” or even provide “reimbursements for fake service overpayments or non-covered services.”

Brand impersonation is nothing new for cybercriminals, but by targeting patients directly, they might be able to trick some people into giving up the kind of information that can be used to commit fraud or even medical identity theft.

Given that providing sensitive healthcare information via email or text is a clear HIPPA violation in most cases, this is a major red flag that you’re not dealing with an actual health insurance company or even their fraud investigators.

Still, for the FBI to issue a public service announcement, this means that this isn’t the type of threat to take lightly and that some patients and even health care providers have fallen for this phishing attack.

To help Americans avoid falling victim to this new phishing scam, the FBI has provided some guidance on the matter in its public service announcement.

For starters, you should always be wary of unsolicited emails, text messages and calls asking for your personal information. Likewise, if you do come across one of these emails or messages, you shouldn't click on any links they contain as they could be malicious.

To keep your medical accounts safe from scammers and hackers, you want to use strong and unique passwords for all of them. You never want to reuse a password and if you have trouble coming up with complex passwords for your accounts or remembering them, you might want to consider using one of the best password managers instead.

Since phishing messages could contain malware or other viruses, you want to make sure that you're using the best antivirus software on your Windows PC or the best Mac antivirus software on your Apple computer.

There's a lot that hackers and scammers can do with sensitive medical information and personal data, so I doubt this is the last time we will see an attack like this. For this reason, you want to make sure that you're extra careful when dealing with any emails or text messages claiming to come from your healthcare provider.

Courtesy of Moose Lake Cartoons https://mooselakecartoons.com/