LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Thank you for joining us at our Fall Conference in December! We had a full event and are busy planning the Winter event. Don't forget to renew your LACFE membership to enjoy future events and trainings! Membership | (lansingacfe.com)

In This Issue

Fraud Talk Podcast

Decoding the Future: Strategic Foresight for Fraud Examiners - Heather Vescent - Episode 162

In this episode of Fraud Talk, ACFE Communications Director John Duffley sits down with Heather Vescent, a futurist, researcher and CEO of The Purple Tornado, to explore how strategic foresight can empower anti-fraud professionals to anticipate emerging threats and adapt to rapid technological change. The conversation covers the evolving role of AI in fraud detection, the importance of human intuition alongside automation, and the promise and challenges of new technologies such as decentralized identity. Vescent shares practical insights on blending technology and human expertise to build resilient, future-ready anti-fraud programs.

https://acfe.podbean.com/e/decoding-the-future-strategic-foresight-for-fraud-examiners/

UPCOMING EVENTS

LOCAL:

MICPA: Forensic Data Analytics Supercourse for Fraud Prevention and Detection
Webinar
January 15, 2026
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=192596

AGA & SAAABA Combined January 2026 Luncheon
MSUFCU's Community Room @ Farm Lane - 4825 Mt. Hope Road, East Lansing, MI
January 13, 2026 (registration ends January 9th)
Learn more: https://lansing-aga.org/EventCalendar/EventDetails.aspx?ItemID=179&mid=24&pageid=22

NATIONAL:

ACFE Fraud Trends to Watch for in 2026
Webinar
February 18, 2026 (Free to ACFE members in good standing)
Learn more: Event Details

ACFE 2026 Government Anti-Fraud Summit
Webinar
February 24, 2026 (early registration ends January 13th)
Learn more: 2026 ACFE Government Anti-Fraud Summit

ACFE 2026 ACFE Women's Summit
In-Person or Virtual
March 6, 2026 (early registration ends January 21st)
Learn more: 2026 ACFE Womens Summit

The ACFE 36th Annual ACFE Global Fraud Conference is now On-Demand
Webinar
Learn more: Product Detail Page

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

Top Fraud Trends of 2025

December 16, 2025
By Abbie Staiger
https://www.acfe.com/acfe-insights-blog/blog-detail?s=top-fraud-trends-of-the-year

In 2025, fraudsters continued finding new ways to perpetrate schemes. Advanced technology, such as artificial intelligence (AI), is exploiting weaknesses across digital and traditional systems, requiring even more innovation and proactive approaches to combat fraud. Drawing from industry trends, news stories and expert insights from the ACFE staff, this recap highlights some of the most prominent fraud schemes and developments taking place this past year.

Top Frauds of 2025

1. Synthetic Identity Fraud

Synthetic identity fraud has become one of the more sophisticated and persistent forms of fraud, with AI accelerating its growth. Fraudsters continue to combine real consumer data, such as Social Security numbers, with fabricated names, addresses and contact information to construct identities that appear legitimate across financial systems. These synthetic profiles can be used to open accounts, obtain lines of credit or apply for government benefits. Fraudsters can build credit histories over time by making small payments to gain trust before eventually defaulting on high credit limits. In doing so, this leaves financial institutions with massive losses and no real individual to hold accountable.

The scale of synthetic identity schemes was seen in the Toronto Police Service's investigation, Project Deja Vu, where investigators uncovered a sophisticated synthetic identity ring that began in 2016. The perpetrators are alleged to have created more than 680 unique synthetic identities to attack banks and financial institutions in Ontario, Canada, resulting in approximately $4 million in losses.

2. Cryptocurrency Scams

Cryptocurrency-related fraud remained a popular illicit activity amongst fraudsters, as well-organized networks targeted both consumers and larger platforms. Large-scale investigations continued throughout the year, including findings from "The Coin Laundry" investigation by the International Consortium of Investigative Journalists (ICIJ). Their investigation revealed a network of international groups using crypto assets to move illicit funds across borders. In addition, a recent Europol operation busted a crypto fraud network that moved more than $815.75 million through fake investment platforms spanning beyond Europe.

With the increase in cryptocurrency scams, the Federal Trade Commission (FTC) stresses that legitimate businesses should never require or demand cryptocurrency as payment, and "investors" promising to quickly and easily make you money in the crypto markets should not be trusted until properly vetted.

3. Account Takeover Scams

Account takeover fraud saw significant growth as criminals used impersonation, phishing and SIM-swapping to gain unauthorized access to financial accounts. The FBI's Internet Crime Complaint Center (IC3) warned how fraud attackers will pose as bank representatives and convince victims to divulge login credentials or authentication codes. Once obtained, these credentials are used to reset account access and rapidly transfer or withdraw funds.

Instead of convincing victims to authorize transactions of their accord, technological advancements have given fraudsters the ability to bypass multi-factor authentication, hijack victim accounts and make unauthorized transactions themselves. In November 2025, the FBI reported more than 5,100 complaints and more than $262 million in losses dating back to January, reflecting the massive impact this scheme has across banking, payroll and health savings platforms.

4. Document Fraud

Advances in generative AI helped increase the sophistication of document fraud by giving fraudsters the option to create financial documents that are entirely synthetic and lack any original source file or trail. This includes fraudulent pay stubs, bank statements, invoices and tax records now being constructed with realistic formatting, logos and signatures designed to bypass intense document checks. This trend presents a major verification challenge because detection methods traditionally relied on comparing submitted documents against known templates or prior submissions. However, when the fraudulent document itself does not have a known, traceable origin, verification becomes nearly impossible.

The scale of this scam was reflected in a research project from Sumsub, which reported a 311% increase in synthetic identity document fraud between Q1 2024 and Q1 2025, signaling how quickly AI tools propped up the scheme.

5. Digital Injection Deepfake Attacks

Deepfake activity advanced substantially in 2025, leading to a rise in digital injection attacks where AI-generated media is fed directly into biometric and identity verification systems. Fraudsters will use synthetic faces, manipulated videos or fabricated voices to complete a "liveness" check or authentication steps required for an account to be created or logged in to. These specific attacks bypass the camera entirely by injecting falsified media at the software level.

This technology supports impersonation scams as well, particularly those involving government agencies. In November 2025, a Canadian retiree lost thousands of dollars after falling victim to a deepfake video of Canadian Prime Minister Mark Carney. The fraudsters leveraged a form of digital injection by successfully feeding the fake interview, which promoted a fraudulent cryptocurrency investment company, into advertising networks and other platforms to directly target their victims.

Top Industries Affected by Fraud in 2025

1. Financial Institutions

Banks and financial Institutions continued to face high exposure as fraud schemes grew more complex and more automated. According to the "2025 State of Fraud and Financial Crime in the United States" report, large banks reported fraud losses nearly four times the industry average. Additionally, 46% of financial institutions noted an increase in fraud sophistication, driven by synthetic identities, account takeovers and more.

2. Health Care

Health care remains one of the more heavily targeted sectors by fraudsters. The U.S. Department of Justice announced significant enforcement actions, including a massive takedown involving 324 defendants connected to $14.6 billion in alleged health care fraud. Common health care schemes included billing fraud, kickbacks, identity theft, fraudulent tele-med operations and misuse of government health programs. Even with consumer scams growing in scale, the health care industry continues to host some of the largest and most complex fraud schemes.

3. Technology

Technology companies faced continued risk from data breaches, vendor compromises and credential exposure. For example, Coinbase released a statement in May announcing a serious breach after cyber criminals "bribed and recruited a group of rogue overseas support agents to steal Coinbase customer data to facilitate social engineering attacks." Incidents such as the Coinbase and Salesforce breach of almost 1 billion records proved how interconnected systems and third-party integrations can amplify and exploit vulnerabilities. These breaches often lead to downstream fraud, including account takeovers, phishing campaigns and identity creation using compromised data.

4. Government and Public Administration

Government agencies faced persistent threats from fraud schemes targeting benefits programs, procurement processes and taxpayer data. Impersonation of government officials remained a frequent tactic in 2025, often being supported by deepfake audio or video. In addition to government employee impersonations, synthetic identities were also used to submit fraudulent applications for government benefits.

5. Retail and e-Commerce

Retail organizations saw continued increases in payment fraud, account takeovers, refund abuse and real-time payment scams. Insights into e-commerce fraud shows online retailers are projected to lose around $52 billion in online payment fraud this year, with a cumulative loss expected to reach $225 billion by 2029. In 2025, global e-commerce fraud losses are projected to reach $138.56 billion, reflecting the growing challenges retailers continued to face throughout the year.

Fraud Genre of the Year: Social Engineering

Social engineering remained a core component of fraud schemes throughout 2025, with AI tools influencing both the scale and execution of these tactics. Fraudsters relied on impersonation, credential theft and manipulation to initiate account takeovers, authorize unauthorized payments and gather sensitive information. This technique was vital towards the growth of schemes like account takeover fraud, in which the FBI reports fraudsters are posing as bank representatives to convince victims to share their login credentials.

AI capabilities increased the speed and consistency of fraud attempts, making them even harder for victims to identify — and easier for fraudsters to execute schemes at a high rate. The combination of traditional social engineering techniques and modern AI-driven tools made this scheme particularly impactful in 2025, affecting nearly every major fraud trend documented this year. Organizations must strengthen fraud prevention measures to defend against complex social engineering schemes, as the prevalence and scale of these tactics in 2025 means passive vigilance is no longer an option.

Looking Ahead into 2026

The top fraud trends of 2025 indicate how fraud is becoming more automated, technically advanced and integrated across illicit fraud networks spanning the globe. To counter these developments, organizations must implement stronger identity verification, better detection models, and updated education and training on AI capabilities across all lines of their fraud risk management programs.

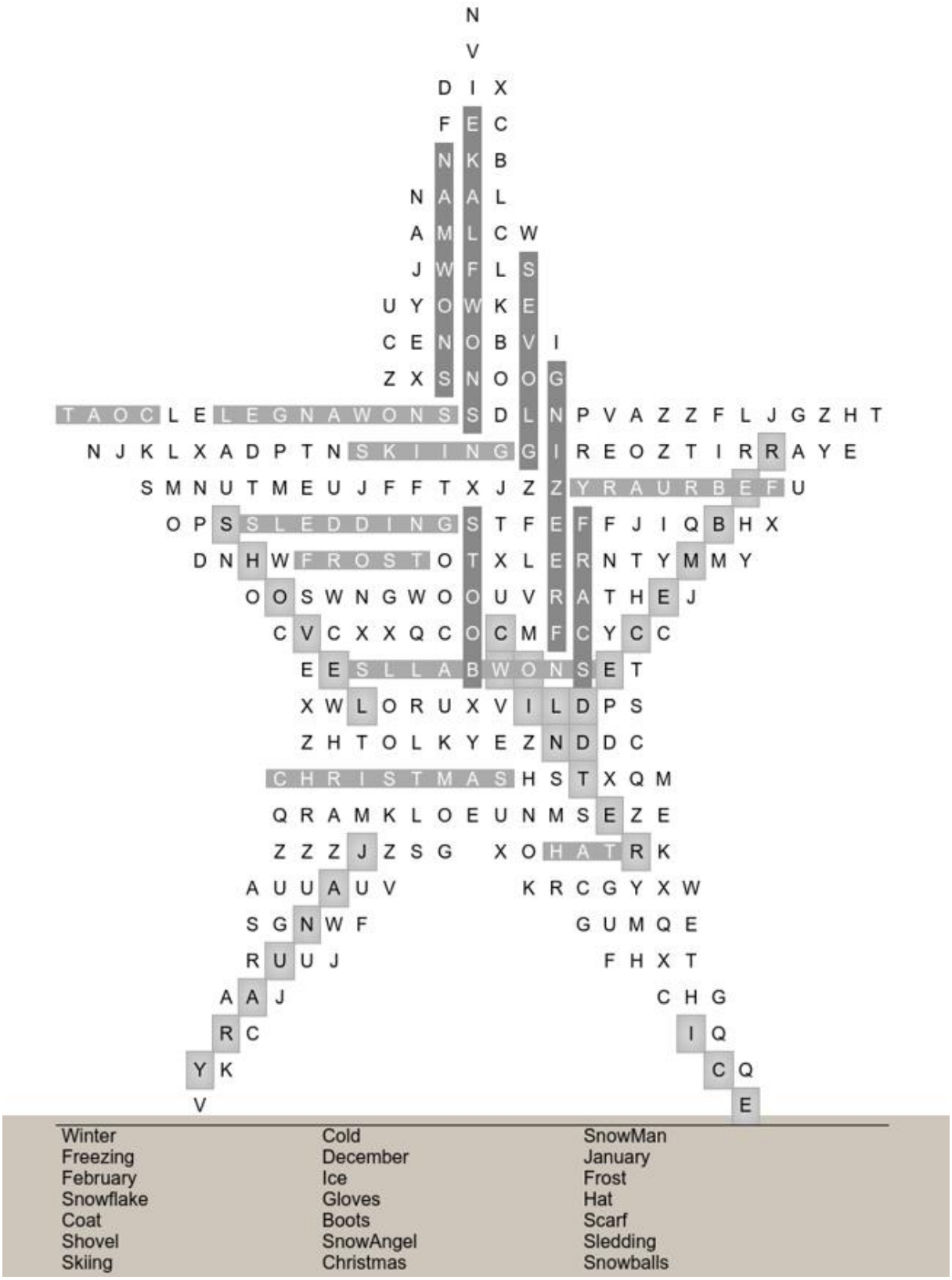
Video of the Month

IRS Scams and Fraud Alerts: How to Protect Yourself and Your Refund

In this eye-opening episode of Resilience and Resolve, tax attorney Lance Drury talks about the growing threat of IRS scams. They uncover the most common schemes, including fake settlement letters, threatening phone calls, and identity theft tactics used to steal personal information. Lance shares real-life examples of victims, explains what the IRS will never do, and offers crucial advice on avoiding scammers who prey on taxpayers—especially seniors and small business owners. Learn how to recognize red flags, why hiring a qualified local attorney is key, and what steps to take if you've already fallen victim.

Reindeer Games

Winter Word Search Answers

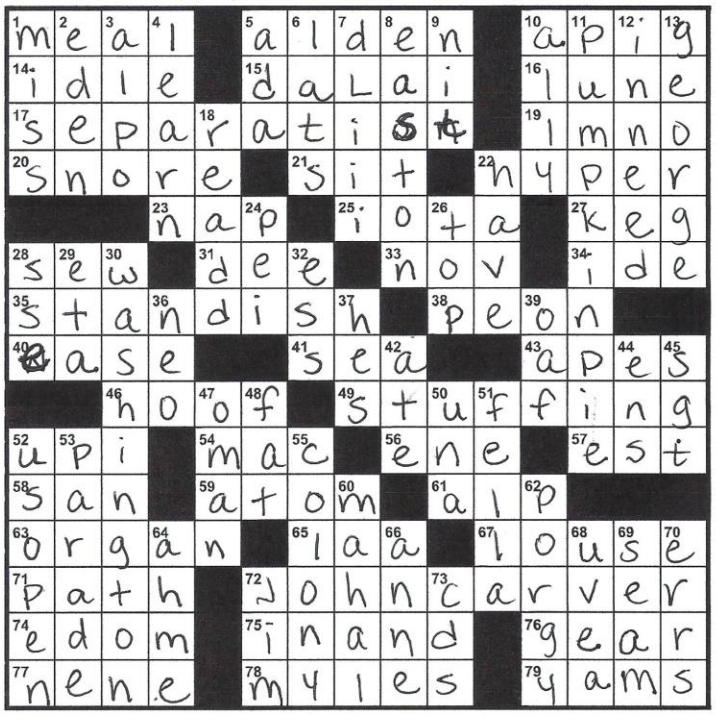


Winter	Cold	SnowMan
Freezing	December	January
February	Ice	Frost
Snowflake	Gloves	Hat
Coat	Boots	Scarf
Shovel	SnowAngel	Sledding
Skiing	Christmas	Snowballs

THANKSGIVING

by Frank Longo |

The Learning Network
Teaching & Learning With The New York Times



ACROSS

1 Thanksgiving feast, for example
5 Mayflower Compact signer John
10 As happy as ___ in mud: 2 wds.
14 Not currently being used
15 ___ Lama (chief Tibetan monk)
16 "Clair de ___" (Debussy composition)
17 One who withdraws, as from an established church in search of religious freedom
19 Letters after K
20 Sleep noisily
21 Use a chair
22 Overly energetic
23 Short sleep
25 Tiny amount
27 Beer barrel
28 Work with needle and thread
31 Grade below a cee
33 Thanksgiving's month: Abbr.
34 Chemical suffix with cyan
35 See 78-Across
38 Lowly laborer
40 Make less harsh
41 The Mediterranean is one
43 Gorillas and orangutans
46 Horse's foot
49 It gets cooked inside a Thanksgiving turkey
52 Major news-distributing org.
54 Apple computer
56 Chemical suffix
57 Approximate amount: Abbr.
58 ___ Francisco
59 Molecule unit
61 Swiss mountain
63 Church instrument
65 When repeated, one of the Teletubbies
67 Small sucking parasite
71 Hiking trail
72 First governor of 55-Down: 2 wds.
74 Biblical kingdom
75 Day ___ day out (constantly): 2 wds.
76 First, reverse or neutral
77 Goose that's the state bird of Hawaii
78 With 35-Across, 55-Down military adviser
79 Thanksgiving side dish

DOWN

1 Fail to notice
2 Adam and Eve's garden
3 Dog food brand
4 What the Plymouth settlers had to do from the Native Americans in order to survive
5 City in central Oklahoma
6 Big back muscles, for short
7 553, in Roman numerals
8 Pop singer Sheena
9 ___-picker (overly critical person)
10 Political friend
11 Thanksgiving dessert: 2 wds.
12 Requiring assistance: 2 wds.
13 With 30-Down, he proclaimed a National Day of Thanksgiving in 1789
18 Total up again
22 Possess
24 Shar-___ (wrinkly-skinned dog)
26 Highest point
28 Direction opposite NNW
29 Greek vowel
30 See 13-Down
32 Suffix with baron
36 Keanu's role in "The Matrix"
37 The Pointer Sisters' "___ So Shy"
39 Big klutz
42 Enjoyed a Thanksgiving feast
44 Military officer: Abbr.
45 Military officer: Abbr.
47 Persian Gulf country
48 It's usually trimmed from a Thanksgiving turkey
50 Spanish article
51 Guy, informally
52 Major golf event: 2 wds.
53 Thanksgiving event with floats
55 Plymouth ___ (what the Pilgrims established in 1620)
60 India's Taj ___
62 "___ and Bess" (Gershwin opera)
64 Words said with a sigh: 2 wds.
66 Poet Bradstreet whose husband was the governor of the Massachusetts 55-Down
68 Eye part containing the iris
69 Sewing line
70 Messes up
72 Carrey of "Dumb and Dumber"
73 Record store purchases

Retailers keep cashing in on crypto ATMs as scams surge

December 17, 2025
By By Ben Dooley, Majlie de Puy Kamp, Curt Devine, Yahya Abou-Ghazala, Kyung Lah and Casey Tolan
https://www.icij.org/investigations/coin-laundry/retailers-keep-cashing-in-on-crypto-atms-as-scams-surge/

In December 2024, criminals stole thousands of dollars from Steve Beckett at a Circle K convenience store in Indiana. The robbery happened in broad daylight.

The thieves didn't use a gun or a knife. There was no getaway car. The instrument of the crime was a machine, much like an ATM, owned by Bitcoin Depot and placed in the convenience store as part of a nationwide agreement with Circle K.

Beckett, 66 at the time, had been paying bills at home when his computer froze and a message directed him to call what turned out to be a phony Microsoft service hotline.

On the phone, a man named "Josh" told Beckett that someone had hacked his computer and used his credit cards and bank accounts to purchase child pornography. Soon, Beckett was speaking to another man, who claimed to work at his bank, and then someone else, who said he represented the Federal Reserve. His life savings were at risk, the men said, and there was only one way to protect them: converting the money into bitcoin.

Over the course of two days, the men cajoled and threatened Beckett, warning him he could go to prison. He had spent years working in management at a casino and selling securities and felt something was wrong, but he was terrified.

"My heart was racing, my blood pressure's going through the roof," he said.

Panicked, Beckett withdrew $4,000 from his bank and, at the men's direction, drove to a Circle K with a Bitcoin Depot ATM. Beckett had never bought bitcoin and knew little about it, but he didn't ask too many questions. On the phone, one of the men walked him through how to deposit the funds. "I was shaking like a leaf," he said. The next day, he deposited another $3,000.

The machine, often called a crypto ATM or bitcoin ATM, converted the cash into bitcoin and transferred it to a digital address the men provided. For completing the transaction, Bitcoin Depot received about $2,000 in fees.

Beckett lost every dime.

The machine at Beckett's local Circle K was one of more than 8,000 operated by Bitcoin Depot in gas stations, grocery stores and other retailers across the United States. In a recent SEC filing, Bitcoin Depot said it had bitcoin ATMs in "approximately 750 Circle K stores" in the U.S. and Canada as of the end of September.

As crypto ATMs have multiplied — there are nearly 40,000 machines operated by companies worldwide, according to the online industry publication Coin ATM Radar — scams have proliferated alongside them. In 2024, the FBI received nearly 11,000 fraud complaints involving crypto ATMs, a 99% increase from the previous year. The complaints represented about $247 million in alleged losses. Those numbers are slated to rise even higher this year, with around $333 million lost to the same type of fraud between January and November 2025.

The surge has become a problem for the entire crypto ATM industry and raises questions about whether the retailers that host the machines are doing enough to protect consumers. Circle K's deal with Bitcoin Depot is one of the largest collaborations between a retail chain and a bitcoin ATM operator in the world.

Circle K has made millions of dollars off the deal and continued the relationship even as complaints — both from customers and employees — have mounted, an investigation by the International Consortium of Investigative Journalists and media partner CNN found. In January 2025, Circle K extended its contract with Bitcoin Depot through mid-2026.

Since January 2024, more than 150 alleged victims have reported scams involving Bitcoin Depot machines at Circle K and Holiday gas stations — which are owned by Circle K's Canadian parent company Alimentation Couche-Tard — amounting to at least $1.5 million in losses, according to an analysis of police reports, consumer complaints, court cases, news reports, and interviews done by ICIJ and CNN.

After police responded to a scam at a Circle K in Florida, a district manager was recorded on body cam footage telling the officers, "I hate these machines. I'd like to get them out of the stores." The sentiment was shared by other Circle K employees in interviews with ICIJ and CNN. One manager, who spoke on the condition of anonymity, recalled how a victim returned to the store with a sledgehammer and tried to break open the machine and reclaim his money.

Circle K has warned its workers to be on the lookout for scammers; employees said management has sent emails about the problem and conducted training. In one Circle K in Indiana, a sign by the register warned clerks against depositing the store's money into Bitcoin Depot's machines.

In response to detailed questions from ICIJ and CNN, a Circle K spokesperson said that the company's staff receive training on recognizing common scams, but the workers are not responsible for overseeing customer transactions on Bitcoin Depot ATMs, which are "owned and managed solely by third parties." The company said it works closely with Bitcoin Depot "to ensure their services consistently meet our standards, regulatory requirements and customers' needs and expectations."

Bitcoin Depot said in a statement "the vast majority of our customers use our kiosks for legitimate purposes. Protecting consumers is central to our model, which is why we invest heavily in compliance, blockchain monitoring, scam warnings, and partnerships with law enforcement."

The findings about Circle K and Bitcoin Depot are part of The Coin Laundry, an ICIJ-led cross-border investigation that exposes how cryptocurrency companies make money off the

proceeds of scams, theft and other crimes — while those who've lost their savings or livelihoods are left with little hope of justice.

"If we were to eliminate scams 100%, we would be hurting," according to one of several former Bitcoin Depot employees who asked for anonymity to discuss the company.

In a lawsuit against Bitcoin Depot filed in early 2025, Iowa's attorney general wrote that an analysis of transactions conducted in the state on the company's machines between October 2021 and July 2024 suggested that more than half involved scams.

Authorities have also accused other crypto ATM industry leaders of facilitating high levels of scam transactions. About 90% of transactions on the CoinFlip ATM network examined by Iowa's attorney general were scam-related, according to court filings. And prosecutors in Washington, D.C., drew similar conclusions about transactions in their jurisdiction made on machines operated by Athena Bitcoin. The companies are the second- and third-largest ATM operators, respectively, according to Coin ATM Radar.

A CoinFlip spokesperson told ICIJ that the company invests heavily in preventing scams and fraud. Athena did not respond to requests for comment. In court filings, Athena Bitcoin said that it was a "neutral intermediary" that is not liable for abuse of its system by criminals.

Industry representatives say that their customers buy bitcoin to send to family abroad, make online purchases and as an investment, among other reasons. Some critics of the machines, however, question whether they are useful for anything other than money laundering and scams.

"When we talk to Bitcoin Depot and we talk to these other places, they're insistent that their ATMs are investment machines, that they're for people to make legitimate investments," Gerard Lotz, a police detective in Louisiana who has investigated many scam cases involving the company, said in a recent interview. "Yet, I don't know any investment firm anywhere that charges 30%."

In 2024, Bitcoin Depot collected between 15% and 50% of each transaction made through its ATMs, according to corporate filings. Its relationship with Circle K accounted for nearly a quarter of its revenue that year.

For Bitcoin Depot and Circle K, the $7,000 Beckett lost isn't even a rounding error on their annual earnings. But for the Indiana senior, who is an ordained minister and volunteer firefighter, the funds meant security.

"That money was our livelihood," he said. "That's how we were living. Paying for things, paying for bills, paying for our mortgage, buying our daughters stuff for their birthdays for Christmas. We can't do any of that."

Both the crypto ATM companies and the stores that host them need to be held responsible, Beckett said. He is suing Bitcoin Depot as part of a lawsuit, one of at least three aimed at the industry's major player.

Bitcoin Depot has denied any wrongdoing, saying that it "cannot be held liable for the criminal

acts of third-party scammers, especially considering the robust warnings and safeguards provided" on its machines and during transactions. In February, a federal judge sent one of the cases, which also included allegations against Circle K, to arbitration.

Circle K is not named in Beckett's suit, but he still believes the retail chain shares responsibility for what happened to him and others.

"I think they do know what's going on," he said. They're "reaping the benefits of having the machine in there and making the money from it."

'The biggest deal'

From the early days of the crypto ATM industry in 2013, the machines were largely hosted at small, independently owned businesses such as liquor stores, gas stations and corner groceries.

Bitcoin Depot's founder and CEO, Brandon Mintz, installed the company's first ATM in 2016 at a vape shop in Atlanta.

Mintz's pitch to retailers was simple: Businesses would get a monthly payment and increased foot traffic. Customers would get convenience and privacy.

The company was also selling trust, Mintz believed. People were understandably suspicious of exchanging cash for virtual currency, he said at an Atlanta bitcoin conference in 2019. But that would change "once you have a physical machine sitting somewhere next to an ATM that you've used all the time at a store you always go to," he said.

In the summer of 2021, with bitcoin rapidly becoming mainstream, Bitcoin Depot and Circle K signed an exclusive agreement, a major step toward achieving Mintz's vision.

"It was the biggest deal and remains the biggest deal in that space," according to a former Bitcoin Depot employee.

With the deal, Circle K became "the first major retail chain to deploy Bitcoin ATMs within its stores," Bitcoin Depot said in a press release.

That gave the chain "an important, early presence in the fast-growing cryptocurrency marketplace," Denny Tewell, a Circle K senior vice president, said in the release.

The agreement with Bitcoin Depot was lucrative for Circle K, which was initially paid as much as $700 a month in rent per machine, according to two people familiar with the payment system and notes reviewed by ICIJ.

With more than 6,300 stores in the U.S. alone, Circle K represented a potential goldmine for Bitcoin Depot. By the end of 2021, the convenience chain's stores accounted for over 20% of the company's transaction volume.

Bitcoin Depot also gained something potentially even more valuable than increased revenue: the opportunity to move the business to locations with high name recognition.

Problems soon surfaced, however, as store managers began reporting issues with scams involving the machines and asking Bitcoin Depot for guidance, according to two people familiar with the situation.

Scams and money laundering had been a problem since the crypto ATM industry's early days. In a 2018 post on its website, Bitcoin Depot warned that it had "stopped fraudsters that use many different scams to steal, and new routines are used daily."

Seeking to protect customers and reduce their own liability, crypto ATM operators placed scam warnings on machines and increased network monitoring. Bitcoin Depot's 2019 compliance handbook required employees to keep detailed records of known scams that occurred on its ATM network and, when cases topped $2,000, send a suspicious-activity report to the U.S. Treasury Department's Financial Crimes Enforcement Network, according to a copy obtained by ICIJ. The company would blacklist known scammers and close victims' accounts.

Still, the problem continued to grow, and by 2021 crypto ATMs had become the preferred tool for tech-support and government-impersonation scams — the same kind that targeted Beckett — according to Mike McGillicuddy, a special agent at the FBI who specializes in financial crimes and led a task force aimed at recovering scam victims' funds.

Scammers favor the machines over other methods because there is no need to use intermediaries, he said, explaining that "the money can instantaneously be put into a wallet under their control and transferred overseas," where it is beyond law enforcement's reach.

The prevalence of scams made it clear that the industry needed to reform itself, according to Marc Grens, whose business DigitalMint operated a nationwide network of the machines for nearly a decade.

Grens tried to establish an industry group to self-regulate the machines and improve compliance standards. But other ATM operators weren't interested, he said. Ultimately only one other company joined his campaign. Today, both DigitalMint and that company have abandoned the business.

Grens concluded it was impossible to remain profitable without facilitating scams. The more money his company spent on fraud prevention, the more fraud it found, he said. When it came to the largest transactions on the network, "95% of the customers you end up talking to were victims," he said.

Moeses Streed, who worked at Bitcoin Depot's customer service hotline in 2021, said 40% of the calls he received on any given day would be scam-related.

"Some days it would be the only call you would get," he said. "The job felt more like live scam prevention than customer service." (Bitcoin Depot told ICIJ that it does not agree with this description.)

Nevertheless, marketing materials on Bitcoin Depot's website assured potential ATM hosts that the machines would create "ZERO RISK. ZERO COST. MONTHLY REVENUE," an archived version of the site shows.

That wasn't the case for Circle K.

On the surface, things appeared fine: In March 2022, a Circle K vice president told a trade publication that the machines were a "big hit" and that customer feedback had been "overwhelmingly positive." That August, Bitcoin Depot reported that it had placed more than 1,900 ATMs in the chain's stores in the U.S. and Canada.

But behind the scenes, the volume of scams was becoming impossible to ignore and frustrated Circle K employees were flooding Bitcoin Depot with complaints, recalled two people familiar with the situation.

CNN and ICIJ spoke to a total of 30 Circle K current store clerks and managers who were aware of crypto ATM scams. Of those, 17 said they witnessed scams happen in their stores; 13 employees mentioned communication from corporate about crypto ATM scams either in the form of emails or employee training, according to a CNN analysis.

One store manager, who asked for anonymity to discuss their employer, said that nearly all of the clients who used the ATM were being defrauded. This manager said "98% are on the phone being scammed one way or the other."

Scammers even snared Circle K workers, according to interviews with current store employees and police records. Pretending to be Circle K management, scammers persuaded clerks in multiple locations to put money in the Bitcoin Depot machines. The convenience store chain was forced to caution its staff to not fall for the schemes. At a store in Indiana, a sign behind the register warned clerks, "Don't save money in the register to drop in the Bitcoin machine."

Inside Bitcoin Depot, employees had long debated how to address the broader problem of scams, according to people familiar with the issue. In early 2023, the company changed the refund policy on its website, writing that scam victims would be eligible to have fees returned to them on a "case-by-case basis." By late October that year, the language had been removed.

In response to questions about the situation, Bitcoin Depot said that "bad actors attempt to misuse many types of financial self-service terminals," and "the issue is not unique to any one retailer." The company said it has "refunded millions of dollars in attempted scam transactions" and that the language was removed because it "prompted individuals who were not victims to seek refunds for legitimate, completed transactions."

Emails sent in response to consumer complaints showed that even when refunds were available, onerous requirements made it difficult to get them. One Florida victim said she was denied a refund when she wasn't able to get a police report by Bitcoin Depot's deadline. And refund instructions on the company's website led to a form that didn't exist, one person wrote in a complaint to the Connecticut Department of Banking. Bitcoin Depot ignored a victim's refund request while two of its competitors promptly returned lost funds, according to state records.

In its responses to consumer complaints and lawsuits, Bitcoin Depot repeatedly blamed victims for falling prey to scammers, arguing that they failed to heed the company's warnings and policies, according to court records and documents ICIJ obtained through public records

requests. Scam warnings are prominently placed on Bitcoin Depot's ATMs, and users are shown additional messages during the deposit process, cautioning them against sending money to people they don't know. Users must also verify that they are depositing funds into their own wallet and accept that all transactions are "final and irreversible," the company says.

But the messages often aren't sufficient to deter victims, who are typically distraught and not thinking clearly, according to law enforcement officers, consumer advocates and industry insiders interviewed by ICIJ. That was the case for Beckett, who said that he didn't notice the warnings until after he had lost his money.

It was the same for Danny Foret, who was lured into putting nearly $20,000 into a Bitcoin Depot machine at a Circle K in Louisiana. "I was so upset, I didn't worry about looking at the machine," he said.

"That's where the vulnerability of the victims shows," said Brad Williams, a police detective in Peachtree City, Ga., who has investigated bitcoin ATM scams and is working to regulate the machines. "These scams can go on for days and days and days," he said, and when a victim has been broken down psychologically, "it doesn't matter what's in front of them."

Bitcoin Depot told ICIJ that it believes scam warnings are "beneficial" and that it reviews each scam report. "In many instances, we are able to block a transaction before funds reach a bad actor or provide some relief," the company said, adding that while it believes customers need to protect themselves from scams, it "recognizes that customers should not bear this burden alone."

Refund requirements, it wrote, are "not intended to burden customers, but to ensure requests are handled responsibly and in compliance with applicable legal and regulatory obligations."

'Not our problem'

Some retailers have become disillusioned with the machines and tried to have them removed or turned off.

In April 2024, Fareway Stores, a chain of grocery stores, signed a deal with Bitcoin Depot to install 66 machines in its stores in Iowa and other states. By the following February, it had unplugged them all.

The machines, Fareway alleged, had become "instrumentalities of massive fraud." By the beginning of 2025, customers were being defrauded almost weekly, and not long after Fareway found itself under investigation by both the Iowa Attorney General and the state lottery agency.

Bitcoin Depot sued for breach of contract, demanding Fareway turn the ATMs back on and pay damages for lost business and reputational harm.

As of September, 18 states have passed laws or regulations to protect consumers against crypto ATM scams, and more are considering legislation, according to AARP. The changes include maximum transaction limits and, in some cases, mandatory refunds for victims.

But even heavy restrictions have failed to stop scammers from using the ATMs. After Minnesota introduced a $2,000 daily transaction limit for new ATM users in August 2024 as part of a broader law regulating the machines, the state's Department of Commerce continued receiving complaints about them. In one such instance, the victim wrote that the perpetrator had stolen nearly $15,000 by instructing them to make 15 transactions and use a different name for each one.

New legislation enacted in Iowa, where Fareway is headquartered, has limited transactions to $1,000 a day and no more than $10,000 a month for first-time crypto ATM users. It has also capped operator's fees at $5 per transaction or 15% of the value of purchased cryptocurrency, whichever is greater.

With the law coming into effect in summer 2025 and legal pressure from Bitcoin Depot, Fareway decided to turn the ATMs at all of its stores back on in May, according to court filings. The law, it hoped, would at least limit future damages to its customers.

Fareway and Bitcoin Depot settled the suit in November, shortly after Bitcoin Depot announced that it would begin requiring ID verification for every transaction and would add "additional protections for seniors." The company did not provide details about the measures.

Debbie Joy, an assistant manager at a Circle K in Port Orange, Fla., told CNN that she estimates she has intervened in at least 10 scams involving the Bitcoin Depot ATM in the store during her four years of working there, and now she can spot the warning signs.

"It's usually an older or elderly person on the phone with someone and has a bank envelope with them, but the last person was about my age," Joy said. "She was in her 30s or 40s and she got scammed. I had just walked into work and it was too late. She was outside crying."

The scams happen so often that Joy has saved the cellphone number of a local police investigator. Rather than dialing 911, she calls him directly.

"I don't think as much has been lost in my store because I try to intervene," she said.

The city council gave her an award in April for stepping in to stop an elderly couple from depositing $10,000 into the Bitcoin Depot machine. Joy thinks she has helped three or four other people who were going to be scammed on the machine.

"Circle K policy is it's not our machine, it's not our problem," she told the council, "but I see it all too often."

Wealth Over Well-Being: Case Studies of Behavioral Health Fraud

December 2, 2025
By Colin May
https://www.acfe.com/acfe-insights-blog/blog-detail?s=case-studies-behavioral-health-fraud

What happens when those we trust become the problem themselves? In this blog, the author examines several case studies of psychiatrists, psychologists and other behavioral health providers who have crossed the line into non-compliance and outright fraud.

We trust medical professionals to take care of us when we are sick or suffering; this is true especially for those suffering from anxiety, depression and other mental health challenges. What happens when those we trust become the problem themselves?

This article examines several case studies of psychiatrists, psychologists and other behavioral health providers who have crossed the line into non-compliance and outright fraud. By identifying fraud risk factors detailed in these situations, fraud examiners, auditors and healthcare leaders can better oversee behavioral healthcare providers and staff, leverage stronger internal controls and ensure effective risk mitigation.

A Stimulating Fraud
In October 2023, Gustavo Kinrys, a psychiatrist from Natick, Massachusetts, was convicted of fraudulently billing Medicare and private insurers more than $11 million for treatments he never provided. A jury convicted him of seven counts of wire fraud, six counts of false statements relating to healthcare matters and one count of obstructing a criminal health care investigation.

Kinrys had previously held positions at Mass General Hospital and Harvard Medical School before moving to private practice, where he owned Advanced TMS Associates. His practice focused on transcranial magnetic stimulation (TMS) therapy and psychotherapy; TMS is a non-invasive magnetic brain stimulation to treat patients diagnosed with major depressive disorder.

Kinrys billed insurers more than $10 million for thousands of TMS sessions that never occurred, as well as non-existent face-to-face psychotherapy sessions. The therapy sessions with the TMS machines were the key to this case, as they include a limited number of sessions paid for on a subscription basis. With the machines tracking all the sessions, it proved Kinrys provided 5,587 sessions while billing for more than 26,000. In addition, he billed for sessions with patients when either they or he was out of the country.

Out of Office

Theresa A. Kelly, a 57-year-old psychologist for the Department of Veterans Affairs (VA) from Herrin, Illinois, was sentenced to 10 months of imprisonment for submitting false medical documents, obstructing justice and committing Medicare fraud. She was engaged in a scheme to defraud Medicare and obtain payment for psychiatric services that she did not provide to residents of a Southern Illinois nursing home between May 2016 and January 2018.

In addition to her full-time job at the VA, Kelly owned TS Onsite Mental Health, a company through which she claimed to provide psychotherapy sessions to patients at Shawnee Christian Nursing Center in Herrin. She billed Medicare for more than 400 claims — worth more than $54,000 — for services that she did not provide. Kelly also obstructed justice by submitting fraudulent medical documentation in a federal civil lawsuit to seek a continuance of the judicial proceedings.

If You First Don't Succeed at Fraud, Try Again

Ramon Apellaniz (who also used the name Kristopher Rockefeller) operated The Gemini Project, LLC ("Gemini"), a Newington, Connecticut-based counseling practice to patients with mental, behavioral and emotional disorders. However, Apellaniz is not a licensed healthcare provider.

In 2020, Apellaniz was charged by the state with larceny, health care fraud and identity theft offenses after it was initially discovered that he was providing treatment and services to state Medicaid beneficiaries without a license. In many instances, Gemini billed the state Medicaid and received more than $900,000 for mental health services that were never provided. On April 17, 2024, he was sentenced to eight years in prison, execution suspended after 15 months and five years of parole. He was ultimately released eight months later.

Apellaniz conspired with Suhail Aponte, who was the manager and registered agent of Minds Cornerstone LLC, dba Minds Cornerstone Behavior Therapy Services. Minds Cornerstone was an Autism Specialist Group registered with the State of Connecticut in June 2021. Apellaniz is listed nowhere on Minds Cornerstone's Medicaid enrollment forms and had no ownership interest or signatory authority to any of its bank accounts — but was the driving force behind the company and its fraudulent billing practices.

In November 2021, Apellaniz and Aponte used Minds Cornerstone to defraud the Connecticut Medicaid Program by submitting fraudulent claims for applied behavior analysis (ABA) services to children diagnosed with Autism Spectrum Disorder (ASD). The four-year scheme cost taxpayers $1,876,617.

Additional Examples of Behavioral Health Provider Fraud

- Top Arkansas psychiatrist accused of falsely imprisoning patients and Medicaid fraud.
- Department of Justice targets Neurofeedback Billing in $15 million behavioral health fraud case.
- Mental health services providers pay over a million to settle false claims liability.
- Owner of counseling agency and supervising manager plead guilty to conspiracy to commit healthcare fraud charges.

Telehealth and Mental Health

The explosive growth of telehealth services, especially for mental health, raises serious fraud concerns. While people are increasingly relying on telehealth to provide behavioral health services, it can also be problematic.

A report from the U.S. Department of Health and Human Services, Office of Inspector General, outlined many of these concerns. It found that despite high risks for fraud, waste and abuse, many states lack specific monitoring and oversight for telehealth in the behavioral health area. There are further concerns about quality, costs and oversight of these issues that need to be addressed. For example, the issues of telehealth could facilitate "impossible day" billing schemes.

Mental health services play a vital role in ensuring the well-being of individuals and communities, but the increasing reliance has led to potential vulnerabilities. The accessibility of mental health care through the rapid expansion of telehealth platforms is essential for addressing the widespread need for behavioral health support. However, gaps in monitoring and oversight have created opportunities for unethical practices that can lead to fraud, which undermines the integrity of these services. Improved oversight, robust detection systems and better deterrence will not only protect financial resources but also ensure that individuals receive the quality care they deserve.

Quote of the Month

"It's usually an older or elderly person on the phone with someone and has a bank envelope with them, but the last person was about my age… She was in her 30s or 40s and she got scammed. I had just walked into work and it was too late. She was outside crying."

- **Debbie Joy, an assistant manager at a Circle K in Port Orange, Fla., told CNN that she estimates she has intervened in at least 10 scams involving the Bitcoin Depot ATM in the store during her four years of working there, and now she can spot the warning signs. See ICIJ article above.**