LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Please don’t forget to renew your LACFE membership by January 31st! [Membership | (lansingacfe.com)](lansingacfe.com)

The LACFE is seeking scholarship applications from persons that are preparing to sit for the CFE Exam. The scholarship is designated toward the exam fee. If you are planning for the exam, or know of someone else who is, please let us know so you can be considered.

In This Issue

Fraud Talk Podcast

Catching Up With the ACFE: Fraud Week 2022, Board of Regents Voting and More_Episode 126

International Fraud Awareness Week provides space to highlight fraud prevention and detection initiatives at companies around the world. Thousands of groups have pledged as Supporting Organizations over the past 22 years, with more doing their part ahead of Fraud Week 2022, held on November 13-19. Bruce Dorris, President and CEO at the ACFE, sits down with John Duffley, the ACFE’s Communications Manager, to discuss how you can participate in Fraud Week, the annual ACFE Board of Regents voting cycle, and what lies ahead as the ACFE enters its 35th year.

https://acfe.podbean.com/e/catching-up-with-the-acfe-fraud-week-2022-board-of-regents-voting-and-more-_-bruce-dorris-president-and-ceo-_-fraud-talk-_-episode-126/

UPCOMING EVENTS

LOCAL:

ACFE South Florida Chapter presents Hodge-Podge of Fraud: 2023 Kick-off Event
Webinar
January 26th, 2023
9:30am – 3:30pm EST
Learn more: https://acfesouthflorida.org/event-4876848

MICPA - Michigan Specific Ethics -
The Impact of State Statute & Administrative Rules on Your CPA License
Pinnacle Center Hudsonville, MI
January 18, 2023 (alternate dates available)
7:00 am - 7:50 am
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=141377

Lansing Chapter of the ACFE
The February conference will be a webinar. We are working to set the date and will send details soon!

ACFE South Florida Chapter #11 presents 2nd Annual Golf & Fraud Training
Webinar/In-Person
May 4, 2023
Learn more: https://acfesouthflorida.org/event-4876828

NATIONAL:

ACFE Data Integrity – Fraud in Unexpected Places
Virtual Seminar
January 31, 2023
9:00 a.m. EST
Learn more: Event Details (acfe.com)

2023 ACFE Women's Summit
Washington D.C. or Online
March 8, 2023
Learn more: 2023 ACFE Women's Summit (fraudconference.com)

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com

Fraud of the Day: Twenty-Six Years Too Late

December 13, 2022
https://fraudoftheday.com/social-security-and-income-fraud/twenty-six-years-too-late/

On December 1, 2022, Reginald Bagley, of Dellwood, Missouri, admitted in court to stealing his dead mother's Social Security payments over a twenty-six year period accumulating nearly $197,329 in the process.

Our fraudster actually claims he didn't mean to steal his mothers Social Security benefits. But things happen…right? And for Mr. Bagley he apparently didn't know what to do when the benefit money that kept getting deposited got used up. Then more money came and that got used up. A quarter of a century later and almost $200,000 spent, Mr. Bagley says he was over his head. But Mr. Bagley knew what to do once he received a letter of inquiry from the SSA requesting more information. He immediately closed the bank account and got a cashier's check for the rest of the balance.

The case against Mr. Bagley underscores a longstanding problem in which people collect benefits meant for their dead relatives. The Social Security Administration is responsible for issuing about $1 trillion in benefit payments every year, with an infrastructure so complex and archaic that even the slightest error in the overall payment process can result in millions of dollars in improper payments. SSA's financial reports from 2021 estimate that the agency had spent about $8.3 billion in improper payments in 2020; with overpayments about $6.8 billion of that.

What is startling in Mr. Bagley's case was how long it took for SSA to investigate. This scheme could have continued on if it weren't for the Department of Medicare and Medicaid, who noticed that Mrs. Bagley was not using her Medicare benefits. The Medicare office sent out inquiries to SSA and an investigation was started. About twenty-six years too late.

Kudos to the Department of Medicare and Medicaid for noticing that someone wasn't using their benefits!

Today's Fraud of the Day is based on an article "Missouri man admits 26-year Social Security fraud" published by the Washington Post on December 2, 2022

An eastern Missouri man has admitted that he stole almost $200,000 by collecting his mother's Social Security benefits for 26 years after her death.

Reginald Bagley, 62, of Dellwood, pleaded guilty Thursday to a felony charge of stealing money belonging to the United States, the U.S. Attorney's Office in Eastern Missouri said in a news release.

Bagley did not report his mother's death on March 12, 1994, to the Social Security Administration.

Case Study: The Employee and Vendor Nexus

December 23, 2022
GUEST BLOGGER, Mohit Jain, CFE
https://www.acfeinsights.com/acfe-insights/2022/12/22/case-study-the-employee-and-vendor-nexus

Recently, I worked on a case wherein a whistleblower raised allegations on two employees that the company was engaging in unethical practices. The allegations included bribery and corruption, conflict of interest, breach of code of conduct, misappropriation of assets, high prices and poor quality of products supplied and abuse of position.

While the whistleblower had not indicated the names of employees in the whistleblower letter, they mentioned the name of the department of the company under which such unethical practices were being followed. An auditor conducted the preliminary investigation based on the whistleblower letter.

How the Auditor identified the Employees and Carried Out the Investigation

- The auditor requested the purchase data of the department in question and started analyzing the transactions conducted during the past years. Next, they created a detailed profile of the employees working in the department.
- During the review of transactions with the vendor, the auditor performed transactions testing of the vendors using samples and requested the supporting documents required, as per company policy, such as purchase requisition, quotation, comparative statement, goods receipt note, gate pass, invoice, payment voucher and any other supporting available for the transaction.
- The auditor performed analytics on the vendor master of the company and listed the type of vendors, such as existence of vendor, turnover of the vendor over the years and type of products supplied by the vendor.
- The auditor conducted public domain searches on the vendor and noted the owner of vendor, address of the vendor, related parties of the vendor, establishment date of vendor firms, etc.
- The auditor also performed fuzzy logic on employee master and vendor master based on scenarios like common name, common address, common phone number, etc.

Based on the above analysis, the auditor listed the suspected vendors and reviewed all the transactions of the suspected vendors to identify the potential wrongdoings. The auditor noticed the following issues in the suspected vendor's analysis:

1. Conflict of interest between vendor and employee, wherein employee's spouse was the partner in the suspected vendor's company/firm
2. Communications indicating vendor favoritism by the employee, such as preferential treatment of payments to suspected vendor and quotation only obtained from suspected vendor
3. Sharing of confidential information with the suspected vendor

4. Kickbacks by the suspected vendor to employee family member’s account
5. Inexistent manufacturing facilities declared by the suspected vendor at the time of onboarding (Site visits on the manufacturing facilities revealed the results.)

Based on the above findings, the auditor prepared the questionnaire and interviewed the employees indulged in unethical practices.

The top red flags to identify corruption in the organization include:

1) Red flags to identify corrupt vendor/supplier:

- Supply poor quality of goods despite no questions raised, or they are continually awarded the work
- Charges unjustified high prices or raises additional cost invoices frequently
- Offers inappropriate gifts or provides lavish business entertainment
- Close nexus with an employee (Address of supplier/vendor matches with the employees address or employee's relative address, know-your-customer [KYC] documents of vendor match with the employee's KYC), etc.
- Provides an incomplete address or contact details
- Provides multiple addresses
- Works with competitors and passes confidential information to the competitor in exchange for awards/contracts
- Has various companies in the same industry and uses them for bid rigging
- Displays indicators such as poor performance record, history of fraudulent contract, family ties with an employee, lack of qualification or experience, etc.

Although detecting and preventing vendor fraud is not easy, identifying key areas where there is a lack of control and implementing stronger controls and measures can go a long way in preventing vendor fraud cases.

2) Red flags to identify corrupt employee:

- Lifestyle is not commensurate with the income earned
- Forces subordinates to bend the rules for personal gain
- Circumstances arise that generate extreme personal pressures, such as ill family members, huge personal liabilities, etc.
- History of not filing conflict of interest forms or Global Anti-Bribery and Anti-Corruption (ABAC) declaration
- Close association with suppliers

- Inclination to make excuses for deficiencies in supplier's products or services, such as poor quality, late deliveries or high prices

The presence of one or two red flags does not necessarily imply the presence of wrongdoing and may highlight some other external pressure or challenge exists in a person’s life. Understanding and recognizing red flags is an important fraud prevention strategy and can be unlocked through investing in regular fraud awareness education for the employees.

Video of the Month

[Meet the ACFE Board of Regents - YouTube]

The Association of Certified Fraud Examiners (ACFE) maintains its high standards for excellence and professional conduct through its Board of Regents.
Annual elections are open only to Certified Fraud Examiners (CFEs) who are in good standing. Regents serve two-year terms, may only serve one term, and are tasked with ensuring the future of the organization as a whole.

A congressional report says financial technology companies fueled rampant PPP fraud

December 6, 2022
by Austin Fast and Sacha Pfeiffer
https://tinyurl.com/yc3djb7h

A sprawling congressional report accuses several little-known financial technology companies, or fintechs, of reaping "billions in fees from taxpayers while becoming easy targets for those who sought to defraud the PPP," or Paycheck Protection Program.

PPP provided more than 11 million potentially forgivable low-interest loans to small businesses to help them keep employees on the payroll as COVID-19 shutdowns decimated profits. Congress hastily rolled out the program in spring 2020, eventually racking up a price tag of nearly $800 billion.

Fintechs, a nebulous term broadly defined as businesses that use technology to improve or automate financial services, told Congress they could issue PPP loans to struggling small businesses faster than traditional banks — and they did. Fintechs also reached more independent contractors, as well as businesses run by women and people of color, than long-established banks did. They were lauded for those efforts.

But that speed and reach came at an expense, says Samuel Kruger, an assistant professor of finance at the University of Texas at Austin.

"While they were doing that, did they also open up the system to potential fraud and abuse?" he asks. "If you look at the data, the answer seems to be yes."

Kruger and his colleagues reported in a study they published last year that 1.4 million PPP loans show signs of fraud. That amounts to $64 billion in potentially wasted taxpayer money. This week's congressional report appears to confirm those allegations of widespread fraud.

During an 18-month-long investigation preceding Thursday's report, the House Select Subcommittee on the Coronavirus Crisis reviewed about 83,000 pages of internal emails, messages and other documents from more than a dozen fintechs and interviewed former employees, executives and lending partners.

Congressional investigators filled 130 pages of the report with their findings, including:

- Many fintechs "failed to stop obvious and preventable fraud" because they had little to no fraud prevention efforts in place.
- Fintechs profited off processing fees for each approved loan, meaning they had little incentive to find fraud that would cut into their revenues.
- Banks and lending partners collaborating with fintechs admitted doing little to check for fraud in fintech-approved loan applications.

Fintechs invested little in fraud prevention

In the spring of 2020, a fintech called Kabbage furloughed half of its workers who were dedicated to assessing risk and reviewing accounts, yet Kabbage funded billions of dollars in PPP loans by relying on temporary contractors, the report says.

The fintech Womply had fraud prevention systems described in the report as "put together with duct tape and gum." Meanwhile, Womply's CEO had been convicted of insider trading yet was leading the company's fraud prevention efforts.

The fintech Blueacorn spent just a few million dollars on fraud prevention even as it raked in more than $1 billion in PPP processing fees. Blueacorn employees claim they received no training on the loan underwriting process or how to spot fake driver's licenses and tax documents, according to the report.

Blueacorn's loan reviewers were told "the faster the better" by managers who recommended spending no more than 30 seconds on each application. Internal documents encouraged Blueacorn workers to only flag applications with "extremely obvious fraud" because the Small Business Administration, or SBA, "would handle any fraud we didn't stop."

On the contrary, as NPR previously reported, the SBA was hardly an effective backstop for fraud. It had limited ability to police the program and did vanishingly few fraud checks during the loan application or forgiveness process. It also made loans increasingly easy to forgive even as evidence of widespread fraud became clear.

"Monster loans will get everyone paid"

As Congress hurriedly unveiled PPP in April 2020, it offered to pay a percentage of each loan to banks and lenders. These processing fees were meant to incentivize their participation, and page after page of internal communications included in the report shows the incentive worked.

"The more you submit, the more we get paid," Blueacorn managers allegedly told employees.

The report also claims that Blueacorn offered preferential treatment and less scrutiny to large-dollar loans they dubbed "VIPPP."

"Closing these monster loans will get everyone paid," wrote Blueacorn co-founder Stephanie Hockridge in internal company messages included in the report, adding that loan reviewers should "delete" certain smaller loans.

"Who f***ing cares?" she allegedly wrote. "We're not the first bank to decline borrowers who deserve to be funded."

Not only did several fintechs earn billions of dollars in processing fees, but PPP loans were 100% guaranteed by the government.

"The risk here is not ours — it is SBA's risk," a manager at Kabbage told his fraud specialists, according to the report. Investigators say this comment refers to SBA's promise that it wouldn't pursue penalties against lenders whose borrowers had attested that their loan documents were accurate.

Kruger, the University of Texas researcher, told NPR that the prospect of lucrative processing fees became a substantial inducement "to try and generate as many loans as possible."

Few backstops existed for fintechs with little lending experience

Fintechs often sent approved loan applications to other banks and lenders to issue the loans, and the report claims these partners also did little to check for fraud.

"Multiple lenders described their oversight as being limited to 'spot checks' conducted at random on a small percentage of fintech-referred application files," the report states.

One such lender is Prestamos, which grew to be PPP's third-largest lender, with nearly a half-million loans rapidly issued after it contracted Blueacorn to screen applications in 2021.

Prestamos said that its random spot checks of Blueacorn-referred loans didn't involve "digging into every file" and were "not formally logged or documented."

Nearly every lender the subcommittee investigated admitted delegating fraud prevention and eligibility verification to fintechs. These lenders reported "windfall profits" for participating in PPP despite "this lack of oversight," according to the report.

Fintechs place the blame for rampant fraud on the government

As PPP wore on, fintechs tried to deflect responsibility onto the Trump administration for the significant amount of fraud occurring, the report says.

"It's the SBA's s***** rules that created fraud," wrote Kabbage's head of policy in an internal email quoted in the report. In a separate internal email, Celtic Bank's CEO wrote that "the industry should push hard to make sure the SBA accepts the fraud risk."

NPR reached out to five companies named prominently in the report. Two of them — Blueacorn and Womply, which investigators found were involved in about a third of all PPP loans funded in 2021 — did not respond. The other three — Bluevine, Celtic Bank and Kabbage — told NPR they cooperated with the committee's investigation and are proud of the work they did during an unprecedented situation.

"Celtic made extensive and effective efforts to combat fraud, while at the same time adhering to Congress' and SBA's direction to get money out to companies quickly, in a time of national emergency," wrote Celtic Bank's general counsel, Leslie Rinaldi.

The report says that Celtic Bank pushed fintech partner Bluevine to improve fraud controls, likely reducing fraud, a fact Bluevine highlighted to NPR.

"As the subcommittee noted, all fintech companies are not the same, and Bluevine 'adapted to the ongoing threats better' than some of the other fintech companies examined in the inquiry," Bluevine spokesperson Sarah Jewett wrote.

Kabbage's spokesperson, Alison Miller, said her company adhered to PPP's rules in good faith and remains committed to borrowers.

"Unfortunately, the report does the American people a disservice by parsing bits of information out of context to reach a predetermined conclusion," Miller wrote.

Kabbage, as well as an affiliated company called K Servicing, recently declared bankruptcy and is facing a class-action lawsuit that alleges it failed to process forgiveness applications in a timely manner.

Government officials from the Trump and Biden administrations are well aware of PPP's shortcomings. Michael Faulkender, an assistant Treasury secretary under Trump, unapologetically told NPR that speed took precedence over safeguarding against fraud when the government designed PPP.

"What would bread lines during a pandemic have looked like? Do we want to know? I didn't. And so we were going to get that program up and running," Faulkender said.

The report makes several recommendations for the future, including that the SBA should review the way it oversees lenders, issue fraud-screening guidelines, and reconsider working with fintechs.

It also recommends that, in any future government aid programs, the SBA aggressively review loans on a wide scale before forgiving them. That didn't happen with PPP; most loans could be forgiven with a simple one-page form and, as NPR previously reported, the SBA has manually reviewed only about 2% of PPP loans for fraud or eligibility. Yet 93% of all loans have been forgiven as of the SBA's latest updated data, issued on Oct. 24.

To catch scammers, the Department of Justice has named a chief prosecutor for pandemic fraud and President Biden has given prosecutors up to 10 years to bring charges in PPP fraud cases, although the SBA's inspector general has expressed doubt about how many fraudulent loans will ever be recovered.

Update: On Dec. 7, the SBA announced that it has suspended Blueacorn and Womply "from working with the SBA in any capacity." The agency also said it "will be investigating appropriate action against their management, owners, and successor companies." The latter is an apparent reference to Womply having recently created a new company called Solo. In addition, the SBA said it has "launched a full investigation" of several other fintechs: Benworth, Capital Plus, Celtic Bank, Customers Bank, Cross River Bank, Fountainhead, Harvest and Prestamos.

Quote of the Month

“If you ask if FIFA can ever get away from corruption, you have to ask if the world can ever get away from corruption”

— Guido Tognoni, former FIFA media director