LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Reignite Your Passion

Many LACFE members were in attendance at the Fall Fraud Conference, which was a great opportunity to learn about and/or brush up on techniques and tools applicable to internet investigations. Thanks again to Mark and Melanie for organizing the event and to the LACFE board for their generosity!

As we began the conference, I was quickly reminded how fun it can be to dive into internet sources while investigating leads. After the conference ended each day, as I tested out new tools I was quickly reminded of how easy it is to lose all track of time when following numerous leads and uncovering additional information!

Training such as this event often serves to re-invigorate your passion to prevent, deter and/or investigate fraud. Other ways to light your fire may be to learn about the depth and intricate details of fraudulent schemes, the harms perpetrated upon victims, the determination of whistleblowers to reveal the truth despite discrimination and threats, or the resulting news coverage and legal resolution(s) after the deception(s) have been exposed. Personally, learning of large-scale frauds uncovered by whistleblowers and their allies is simultaneously infuriating and intriguing, which is why I highly recommend the title featured in the *Book Nook* below.

As fraud fighters we all feel the call to uphold the values of truth and fairness. However, at times we may lose sight of the reasons we do this important work. I challenge you to seek out that which reignites your fraud-fighting passion this fall and winter!

IN THIS ISSUE

Fraud Talk Podcast

The Rise of Cybercrime During COVID-19

In this episode, Arpinder Singh, CFE, partner and head of India and emerging markets, Forensic & Integrity Services at EY, highlights how cybercrimes like BEC scams, phishing and account takeover have risen and will continue to rise over the next year.
https://www.podbean.com/media/share/pb-9qw5i-eda5a9?utm_campaign=w_share_ep&utm_medium=dlink&utm_source=w_share

UPCOMING EVENTS

LOCAL:

Michigan Association of Certified Public Accountants
Webcast – Governmental Accounting & Auditing Conference
December 3, 2020 (early registration ends November 4th)
Morning and Afternoon sessions
Learn more about the morning session: https://store.micpa.org/Product/Details?productId=20128 and afternoon session: https://store.micpa.org/Product/Details?productId=33309

NATIONAL:

ACFE *Free Seminar*
Virtual – Pandemic-Driven Pressure: Impacts of the Coronavirus on Digital Fraud
November 18, 2020
11:00 am
Learn more at https://www.acfe.com/webinar_live_sponsored.aspx?evtid=a3Y1Q000002kgCdUAI

ACFE
Virtual – Advanced Fraud Examination Techniques
December 14-16, 2020 (early registration ends November 13th)
Learn more at https://www.acfe.com/events.aspx?evtid=a3Y1Q000002kXMGUA2

INTERNATIONAL:

International Fraud Awareness Week –
The 20-Year Anniversary
November 15-21, 2020
Virtual summits, Zoom discussions, training webinars and podcasts all week
Learn more and register for individual events at https://fraudweek.com/fraudweek/events

Other ways to spread Fraud Awareness:
https://fraudweek.com/fraudweek/what-you-can-do

INTERNATIONAL FRAUD AWARENESS WEEK
November 15-21, 2020

If you have an event that you would like posted in our newsletter or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com

Crisis of Conscience: Whistleblowing in an Age of Fraud

By Tom Mueller

We live in a period of sweeping corruption - and a golden age of whistleblowing. Over the past few decades, principled insiders who expose wrongdoing have gained unprecedented legal and social stature, emerging as the government's best weapon against corporate misconduct - and the citizenry's best defense against government gone bad. Whistleblowers force us to confront fundamental questions about the balance between free speech and state secrecy, and between individual morality and corporate power.

In *Crisis of Conscience,* Tom Mueller traces the rise of whistleblowing through a series of riveting cases drawn from the worlds of healthcare and other businesses, Wall Street, and Washington. Drawing on in-depth interviews with more than two hundred whistleblowers and the trailblazing lawyers who arm them for battle - plus politicians, intelligence analysts, government watchdogs, cognitive scientists, and other experts - Mueller anatomizes what inspires some to speak out while the rest of us become complicit in our silence. Whistleblowers, we come to see, are the freethinking, outspoken citizens for whom our republic was conceived. And they are the models we must emulate if our democracy is to survive.

In The News

Widespread Unemployment Fraud Is Overwhelming State Systems
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/widespread-unemployment-fraud-is-overwhelming-state-systems.html

FBI Warns of Potential Charity Fraud Associated with the COVID-19 Pandemic
https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-potential-charity-fraud-associated-with-the-covid-19-pandemic

Brazil holding company agrees to pay $285 million to settle FCPA violations
https://fcpablog.com/2020/10/14/brazil-holding-company-agrees-to-pay-285-million-to-settle-fcpa-violations/

With J&F, 2020 becomes the biggest year in FCPA history
https://fcpablog.com/2020/10/19/with-jf-2020-becomes-the-biggest-year-in-fcpa-history/

Berkshire Hathaway to pay $4.14 million to settle Iran sanctions violations claims
https://www.reuters.com/article/berkshire-hathaway-usa-iran/berkshire-hathaway-to-pay-4-14-million-to-settle-iran-sanctions-violations-claims-idUSKBN2752ET

Justice Department Announces Global Resolution of Criminal and Civil Investigations with Opioid Manufacturer Purdue Pharma and Civil Settlement with Members of the Sackler Family
https://www.justice.gov/opa/pr/justice-department-announces-global-resolution-criminal-and-civil-investigations-opioid

Auditor: Iowa misallocated at least $21 million in COVID-19 funds
https://www.desmoinesregister.com/story/news/2020/10/19/covid-19-funds-iowa-auditor-warns-reynolds-cares-act-millions-missing/5982318002/

Former Columbus mayor charged with bank fraud
https://www.channel3000.com/former-columbus-mayor-charged-with-bank-fraud/

Detroit couple charged in $2.5 million unemployment fraud scheme
https://www.abc12.com/2020/10/27/detroit-couple-charged-in-25-million-unemployment-fraud-scheme/

Farmington Hills man charged with unemployment fraud showboated lavish lifestyle on social media https://www.wxyz.com/news/farmington-hills-charged-with-unemployment-fraud-and-show-boating-lavish-lifestyle-on-social-media

Kalamazoo doctor gets prison time in Medicare fraud case
https://wkzo.com/2020/10/30/61335/

Without More Enforcement, Tax Evasion Will Spread Like a Virus
https://www.nytimes.com/2020/10/30/business/tax-evasion-virus-IRS.html

An avalanche of fraud buried a small-business relief program

By Michelle Davis, Zachary Mider and Polly Mosendz
October 30, 2020, 10:22 a.m. EDT
https://www.accountingtoday.com/articles/an-avalanche-of-fraud-buried-a-small-business-relief-program

For a few months this year, a U.S. government aid program meant for struggling small-business owners was handing out $10,000 to just about anyone who asked. All it took was a five-minute online application. You just had to say you owned a business with at least 10 employees, and the grant usually arrived within a few days.

People caught on fast. In some neighborhoods in Chicago and Miami, it seemed like everyone made a bogus application to the Small Business Administration's COVID-19 Economic Injury Disaster Loan program. Professional thieves from Russia to Nigeria cashed in. Low-level employees at the agency watched helplessly as misspent money flew out the door.

Even after the $20 billion in funding for grants dried up in July, the fraud continued, as scammers looted a separate $192 billion pot of money set aside for loans. "I've never seen anything like it," said an SBA customer-service representative who spoke on the condition of anonymity to protect her job. "I don't think they had any processes in place. They just sent the money out."

This account of the disaster-aid program is based on interviews with frontline SBA workers and outside fraud investigators, and on a review of thousands of social-media postings. The unprecedented scale and urgency of the pandemic response made some missteps inevitable, and lawmakers explicitly ordered the agency to prioritize speed over thrift. But decisions by agency leaders contributed to the chaos.

The SBA's much-vaunted new computer system, built by an outside contractor for $750 million, proved blind to certain types of fraud and sometimes awarded grants even when it spotted disqualifying features. The agency pressured loan officers with little training to churn through applications quickly, while making it difficult for them to detect or report suspicious ones. When officials eventually tightened fraud controls, the result was often delays and rejections for legitimate applicants.

The amount stolen from the program, if it's ever tallied, will almost certainly be measured in the billions of dollars. But that's only part of the cost. Many legitimate applicants were denied grants because scammers got the money first. And identity thieves pocketing loan proceeds left an unknown number of Americans saddled with bogus debts.

"It's too bad that it got this far," said Richard Maier, an investigator at a credit union in Florida who documented dozens of cases of disaster-aid fraud involving his customers. "Some of these innocent people are being taken advantage of because someone didn't do the due diligence on the front side."

The SBA said in a statement that it "proactively initiated stringent fraud-prevention safeguards that have so far prevented the processing of thousands of invalid applications, balancing the

agency's fiduciary responsibilities against the urgent need to provide the small-business sector" with aid. "These rigorous and comprehensive controls included an end-to-end infrastructure of internal controls comprised of automated tools, scores of system rules to validate borrower identity and business eligibility, and an application review process consisting of multiple checks." The agency added that it has been referring suspected fraud to its inspector general. It declined to answer detailed questions for this story.

A report released Wednesday by the agency's inspector general, Hannibal "Mike" Ware, identified tens of billions of dollars in potentially fraudulent transactions, including multiple loans sent to applicants using the same bank account or address. But as the agency pointed out in a rebuttal, many of the loans flagged by Ware were legitimate, and Ware didn't even hazard a guess as to how much fraud actually took place. He disclosed that $450 million in doubtful payments have already been seized by law enforcement.

As the economic threat of the pandemic became clear in March, Congress hatched a two-pronged bailout for small businesses. The biggest was the Paycheck Protection Program, which grew to $525 billion and used thousands of banks to issue forgivable, SBA-backed loans to cover payroll. The other, the disaster-aid program, is run directly by the SBA and is still approving loans of as much as $150,000. More than 3.6 million loans have been issued in addition to 5.8 million grants that don't have to be repaid.

To get money out quickly, Congress instructed the agency to relax its normal fraud safeguards, declaring that applicants should be considered eligible if they swore they were.

Designed for regional calamities such as hurricanes and earthquakes, the SBA's disaster-aid program was unprepared for a nationwide pandemic that disrupted millions of small businesses simultaneously. So in March, it asked one of its contractors, Herndon, Virginia-based consulting firm RER Solutions Inc., to build a computer system from scratch. RER, in turn, subcontracted much of the work to Rocket Loans, an arm of billionaire Dan Gilbert's Detroit-based mortgage-lending empire.

The system developed by RER and Rocket was known as "Rapid Decision," and it lived up to its name. It would take in loan applications submitted to the SBA website and check them against a list of indicators of fraud or ineligibility. Among other things, it was supposed to flag applicants who had already received a loan or submitted a dead person's Social Security number. By late April, Rapid Decision was churning through more than 100,000 applications a day, a rate of more than one per second.

Each application was screened for both a grant and a loan. Grants were meant to provide borrowers with quick cash while they waited for a loan decision. Most went out quickly, with no human intervention, based on Rapid Decision's recommendation. A human sign-off was required for loans, but even then the computer played a crucial role. The results of the program's automated checks would be placed in each loan file. Loan officers were given only a few minutes to process a request.

In a letter defending the program in July, SBA Administrator Jovita Carranza boasted of the "sophisticated technology" behind Rapid Decision, supporting "robust" internal controls. "This is the path forward," one of her deputies, James Rivera, told Congress that month. "It has increased the productivity. It's helped us provide quicker, faster service."

Rapid Decision looked very different to loan officers on the front lines.

The computer system was designed to run fraud checks on the person submitting the application, the bank account designated to receive the money, even the internet address used to submit it. But it had no reliable way of checking to see if a small business actually existed.

No matter how implausible an applicant's business profile, as long as the computerized checks were cleared, a grant would be issued. By the time a human loan officer reviewed the file, it was too late.

Loan officers grew accustomed to seeing ridiculous applications easily score grants. There were purported farmers using an address in the middle of a city and multiple small businesses supposedly located in the same single-family home, each claiming to have 10 employees, the minimum to qualify for the full $10,000. One phony business profile showed up again and again: a sole proprietorship with exactly 10 employees and a mere $24,000 in annual revenue.

In July, while top SBA officials were boasting of Rapid Decision's prowess, one loan officer said he was spotting dozens of grants each day that had clearly gone to scammers or ineligible applicants. The officer spoke on the condition of anonymity because he still works at the agency. At the end of each shift, he'd assemble a list of suspect grants and email it to someone in the SBA's legal department. The list typically had more than 100 grants. He never learned if anyone followed up.

Nicholas Croce, a graduate student in Syracuse, New York, worked remotely as a SBA loan officer for about six weeks this summer, one of more than 5,000 workers hired by the agency to tackle the surge in work. He, too, described the frustration of seeing fraudulent applications that already scored grants.

One day in July, Croce said, he spotted a $10,000 grant about to be paid out on an obviously fraudulent application. There was still time to cancel the payment, but when he reached out to a higher-up, he said, the manager refused to stop it and ordered him to focus only on his assigned work.

"You'll learn soon how things are done around here," Croce said the manager told him. "People coming to this job, they need to learn what our culture is." As far as Croce knows, the scammer made off with the cash, just like the others.

To Croce, the episode was emblematic of agency dysfunction. He said he quit a few weeks later. "I was like, I can't be a part of this," Croce said. "I felt dirty about it."

It's unclear why the designers of Rapid Decision didn't give it a way of identifying phony businesses. The Internal Revenue Service assigns a unique ID to every U.S. business that pays employees, but the SBA didn't require that all businesses claiming to have employees submit ID numbers.

Croce and the loan officer who requested anonymity said they noticed some grants getting approved even after the system flagged obvious disqualifiers, such as an invalid Social Security number or a checked box saying an applicant wasn't a U.S. citizen. "Everything was getting approved," the loan officer said. "Every single category was getting the money that SBA prohibited."

In separate statements, RER and Rocket both noted that they acted at the direction of the agency and that their work was crucial to the delivery of millions of loans and grants. "The SBA weighed numerous options for fraud detection" against time and legal constraints, Rocket said.

“Rocket Loans then implemented technology with the fraud detection logic as directed by the SBA.”

For Maier, the fraud investigator at MidFlorida Credit Union in Lakeland, Florida, the alarm rang on July 22. That was when a customer showed up at a drive-through window, trying to withdraw $10,000 in cash. The man had just received a $32,000 disaster loan in a new account, and his explanation of his purported business made no sense. “It was just a crazy, all-over-the-place story,” Maier said.

Maier started monitoring SBA payments to customers and found suspicious transactions everywhere. Customers with no apparent connection to a small business were getting loans in personal accounts. An 18-year-old who got $49,000 couldn’t produce evidence she owned a hairdressing business. Others freely admitted they didn’t have a business and claimed they hadn’t realized they’d committed a crime. Still others seemed to be receiving the funds on behalf of professional thieves. Overall, Maier determined that about 60 percent of the deposits that came to his attention were fraudulent. He sent them back to the SBA.

“We had one guy tell us, ‘I’m just here to get my money like everybody else,’” Maier said.

Similar alarms rang at banks across the country. At JPMorgan Chase & Co. and Wells Fargo & Co., two of the country’s largest, customer abuse of the program was so rampant that internal probes caught dozens of the banks’ own employees illegally cashing in. One credit union told the inspector general that it examined 60 deposits and concluded that 59 involved fraud. Official bank reports of suspicious business-loan activity jumped more than tenfold.

As word got out about the program’s vulnerabilities, the SBA began warning staff to look out for applications from certain places where fraud was the worst: Chicago, Miami, parts of Georgia.

Christian Cutrone, a Chicago record-label entrepreneur, knows so many people who stole SBA money in his neighborhood that he warned his Instagram followers in June about potential jail time. “It just kind of went viral here,” he said in an interview. “One house I know, there’s four people that live there, two on one floor, two on the other — everyone in the building did it.”

“Everybody got that free $10k,” a Chicago woman posted on Twitter in late June. “I wanna do that 10k stuff but I’m scared,” another woman tweeted a few days earlier. “What’s gone happen if I get caught?”

A YouTube talk show based in Houston titled a July episode “$10k SBA Loans & GRANTS Got The STREETS Going CRAZY!” A guest, Nu Money, remarked that people he knew must somehow qualify for business aid because they were suddenly flush with cash. The show’s host, Big Ant, replied, “Or just a lot of people finessin’ it.”

A Bloomberg News analysis of SBA data published in August aligns with the gossip and the internal warnings. It found 52 congressional districts, mostly around Chicago, Atlanta, Miami and Houston, where the number of $10,000 grants exceeded eligible recipients, for a total of 128,000 excess grants worth $1.3 billion. In Illinois’s 2nd Congressional District, payouts exceeded the number of eligible recipients by 12 times.

In YouTube posts and Telegram channels, professional scammers shared step-by-step tutorials describing how to defeat the SBA’s defenses. Compared with other scams — unemployment benefits, credit cards — they described this one as particularly easy to pull off.

“You can learn everything in 10 minutes and start applying,” wrote one fraudster on a Telegram channel in September, offering a tutorial for $30. He added that he also sells stolen Social Security numbers and other personal information used to create phony applications.

Because loans required a human sign-off, there was a chance an employee would spot a fictional business and reject it. But in the program’s early days, officers were encouraged to process applications quickly, and asking for backup documentation such as tax returns was discouraged. The loan officer who still works at the agency said that to prod faster decisions the names of the slowest performers on a team were sometimes circulated over email.

Cybersecurity researchers began noticing criminals in Russia, Nigeria and elsewhere plundering the program. In Nigeria, long a haven to gangs of cybercriminals known as “Yahoo boys,” U.S. small-business aid became such an important revenue opportunity this year that some are calling themselves “SBA boys,” said Crane Hassold, a researcher at Foster City, California-based Agari Data Inc.

For foreign scammers, the biggest challenge wasn’t tricking the SBA into putting money in a bogus company’s bank account. It was getting the money out. Some used “money mules” in the U.S., Hassold said — often lonely Americans recruited through dating apps, who think they’re doing a favor for an online sweetheart. Other times, he said, fraudsters would just open a new account at an online institution like Green Dot Bank or Chime, using the same stolen identity as in the loan application.

Capers like that explain why Jane Dennington, 67, a former Christian missionary who lives near Erie, Pennsylvania, got a letter in the mail in September. It notified her of the first payment date for a $30,500 SBA loan she never applied for, for a farm that doesn’t exist at an address where she no longer lives. “I don’t even have a garden,” Dennington said in an interview.

She called the SBA, which told her the money went to an account at a bank she’d never heard of. “I’m not sure if they said Green Spot or Green Dot.” After several calls to agency hotlines, an employee in Texas told her the debt would be canceled and said, “This is happening like crazy.” Media reports in Iowa, Florida and Kentucky describe similar cases.

“I don’t understand,” Dennington said. “They are rejecting all these businesses that are legit here in Erie, but they issue one to a farm that doesn't exist.”

The SBA said Wednesday that it has referred more than 80,000 loans for criminal investigation, but so far there’s no sign of a comprehensive push by law enforcement to tackle the fraud. The Department of Justice has announced charges against 23 people, all but one of whom were accused in conjunction with Paycheck Protection Program fraud or other crimes. Agents charged a Brooklyn protester with obtaining a $10,000 grant and a $42,500 loan by pretending he owned a car wash with 10 employees; they say they found evidence of the scam on his phone after he was arrested for cutting a brake line on a police van.

As SBA officials began to comprehend the level of fraud taking place, they issued a blizzard of policy updates, some of them contradictory. At one point, the loan officer still working at the SBA said, the agency told employees to reject any application sent from the same WiFi network as a previous application. Days later, the rule was retracted.

After first discouraging officers from requesting backup documentation such as tax returns, the SBA later allowed it. But it soon became clear that scammers were easily producing fake documents. An Aug. 16 email announced yet another policy: Applicants with no online presence would be given only a few hours to submit supporting documents before being declined.

“We currently have too much fraud as it is, and we are trying not to give applicants additional time to provide fraudulent documentation,” an SBA manager wrote in the email, which was published in September by the Project on Government Oversight, a Washington watchdog group. Of course, the new policy meant plenty of legitimate small business owners would get rejected as well.

After the SBA stopped updating an internal policy manual in July, employees struggled to keep track of which rules were in effect. Some loan officers are now telling applicants that deposits in online-only banks such as Chime and Green Dot are prohibited; others say they’re still allowed.

The pressure for quick decisions, which once worked in fraudsters’ favor, is now hurting legitimate applicants, the SBA workers say. Officers are rapidly declining any loan they can’t be sure about, causing rejected applications to pile up in an appeals process that can drag on for months. The customer-service representative has been telling applicants pursuing appeals not to expect to see any funds until late December at the earliest.

“Applications are still allowed to come in and are further backing up,” said the loan officer. “By the time we get this to businesses, the pandemic will be over.”

— *With assistance from William Turton, Kartikay Mehrotra and William Clowes*

QUOTE OF THE MONTH

"There is always a need for whistleblowers – we don’t live in a society which is transparent, fair and just. Whistleblowers hold people to account."

Katharine Gun, whistleblower