LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

From the ACFE:

Are you looking to advance your career, change your profession or sharpen your leadership skills? The **ACFE Mentoring Program** can help you navigate all stages of your career.

As a CFE, you have the option to enroll as either a mentor or a mentee. The second session of 2022 begins July 12 and runs until December 31, 2022, and you can now **enroll in the upcoming session.**

Consider becoming a mentor.

- Give back to the anti-fraud community
- Share and reinforce your own knowledge
- Broaden your anti-fraud network
- Earn CPE and equip fellow fraud fighters with skills to fight fraud

Hugh Penri-Williams, an ACFE Mentor said, "It is never too late to seek the advice and counsel of those who are willing to freely give their time and expertise to assist you. In the process, both sides can find illuminating moments of mutual worth."

Set your goals high, and achieve them with a mentor. According to a Gartner study, mentees are five times more likely to be offered a promotion if they participate in a mentoring program.

Transform your career and **enroll in the ACFE Mentoring Program.**

In This Issue

AARP Take on Today Podcast

The Passage of the Fraud And Scams Reduction Act

Scams targeting seniors have increased during the pandemic. Today, we'll hear about new legislation called the Fraud and Scams Reduction Act. To discuss what exactly the bill entails, we sit down with Cristina Martin Firvida, AARP Vice President of Financial Security and Consumer Affairs.

We also hear from AARP's Mary Liz Burns about AARP Money Map, a new digital financial tool for all ages to build a budget, save money and manage unplanned expenses.

https://www.aarp.org/podcasts/take-on-today/info-2022/fraud-scams-reduction-act.html

UPCOMING EVENTS

LOCAL:

Michigan Association of Certified Public Accountants
Fraud & Embezzlement: Case Studies from the Trenches
Webinar
Tuesday, June 14, 2022
2:30 pm - 4:30 pm
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=131451

ACFE South Florida Chapter #11 presents 7th Annual Ethics Seminar
In Person and Webinar (*Only $35 for Associate Chapter Members*)
July 14, 2022
8:30 am – 11:00 am
Earn up to 2 hours of Ethics CPE
Learn more: https://southfloridaacfe.org/page-18098

NATIONAL:

ACFE
Global Fraud Conference Virtual Sponsor Showcase
Virtual
June 8, 2022
The event is free, but space is limited.
Register and learn more: http://pages.acfe.com/2022VSS.html#register

ACFE
ACFE Research Institute Summer Meeting
Webinar
Jun 23, 2022
9:00 a.m.
Learn more: https://www.acfe.com/training-events-and-products/all-events/calendar-of-events/event-detail-page?s=ACFE-Research-Institute-Summer-Meeting-0622Virt

ACFE
Investigating Conflicts of Interest
Webinar
Aug 17, 2022 (early registration ends July 18th)
9:00 a.m.
Learn more: https://www.acfe.com/training-events-and-products/all-events/calendar-of-events/event-detail-page?s=Investigating-Conflicts-Interest-0822Virt-ICI

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

Why It's Hard to Sanction Ransomware Groups

by Renee Dudley
May 23, 2022
https://www.propublica.org/article/ransomware-russia-ukraine-sanctions-ofac-conti

On Feb. 25, the day after Russia invaded Ukraine, a prolific ransomware gang called Conti made a proclamation on its dark web site. It was an unusually political statement for a cybercrime organization: Conti pledged its "full support of Russian government" and said it would use "all possible resources to strike back at the critical infrastructures" of Russia's opponents.

Perhaps sensing that such a public alliance with the regime of Russian President Vladimir Putin could cause problems, Conti tempered its declaration later that day. "We do not ally with any government and we condemn the ongoing war," it wrote in a follow-up statement that nonetheless vowed retaliation against the United States if it used cyberwarfare to target "any Russian-speaking region of the world."

Conti was likely concerned about the specter of U.S. sanctions, which Washington applies to people or countries threatening America's security, foreign policy or economy. But Conti's attempt to resume its status as a stateless operation didn't work out: Within days of Russia's invasion, a researcher who would later tweet "Glory to Ukraine!" leaked 60,000 internal Conti messages on Twitter. The communications showed signs of connections between the gang and the FSB, a Russian intelligence agency, and included one suggesting a Conti boss "is in service of Pu."

Yet even as Putin's family and other Russian officials, oligarchs, banks and businesses have faced an unprecedented wave of U.S. sanctions designed to impose a crippling blow on the Russian economy, Conti was not hit with sanctions. Any time the U.S. Treasury Department sanctions such an operation, Americans are legally barred from paying it ransom.

The fact that Conti wasn't put on a sanctions list may seem surprising given the widespread damage it wrought. Conti penetrated the computer systems of more than 1,000 victims around the world, locked their files and collected more than $150 million in ransoms to restore access. The group also stole victims' data, published samples on a dark website and threatened to publish more unless it was paid.

But only a small handful of the legions of alleged ransomware criminals and groups attacking U.S. victims have been named on sanctions lists over the years by the Treasury Department's Office of Foreign Assets Control, which administers and enforces them.

Putting a ransomware group on a sanctions list isn't as simple as it might seem, current and former Treasury officials said. Sanctions are only as good as the evidence behind them. OFAC mostly relies on information from intelligence and law enforcement agencies, as well as media reports and other sources. When it comes to ransomware, OFAC has typically used evidence from criminal indictments, such as that of the alleged mastermind behind the Russia-based Evil Corp cybercrime gang in 2019. But such law enforcement actions can take years.

“Attribution is very difficult,” Michael Lieberman, assistant director of OFAC’s enforcement division, acknowledged at a conference this year. (The Treasury Department did not respond to ProPublica’s requests for comment.)

Ransomware groups are constantly changing their names, in part to evade sanctions and law enforcement. Indeed, on Thursday, a tech site called BleepingComputer reported that Conti itself has “officially shut down their operation.” The article, which cited information from a threat-prevention company called AdvIntel, laid out details about the status of Conti’s sites and servers but was unambiguous on a key point: “Conti’s gone, but the operation lives on.”

The evanescence of the Conti name underscores another reason it’s hard to sanction ransomware groups: Putting a group on a list of sanctioned entities without also naming the individuals behind it or releasing other identifying characteristics could cause hardship for bystanders. For example, a bank customer with the last name “Conti” might pop up as a sanctioned person, creating unintended legal exposure for that person and the bank, said Michael Parker, a former official in OFAC’s Enforcement Division. The government then would have to untangle these snarls.

By imposing sanctions, the federal government would hamstring victimized organizations, such as businesses and hospitals, that might suffer disclosure of trade secrets or other sensitive information, or might have to shut down if they couldn’t recover their locked files. If they could pay the ransom, the hacker would supply a key to unlock the files and pledge to delete stolen data.

But even without sanctions, victims are in a bind. Years before the invasion of Ukraine, OFAC imposed sanctions on the FSB, one of the successor agencies to the Soviet-era KGB. So even though Conti was not listed by name, its possible ties to the FSB or other listed Russian entities may have rendered it sanctioned anyway.

Between that and the bad optics of paying a group linked to Russia, most victims had not paid Conti’s ransom after the February proclamation, according to lawyers and negotiators who work with ransomware victims. They say the situation is confusing. “It certainly would be easier for us if the standard were to add particular ransomware groups to the OFAC list,” said Michael Waters, an attorney who frequently works with victims of ransomware. “Then we simply aren’t going to make payments to those groups. But it is much foggier than that.”

Some American victims continued to pay ransoms to Conti through a Canadian intermediary called Cypfer. CEO Daniel Tobok said Cypher paid Conti on behalf of about a dozen victims, more than a third of them American, after the war began. He said that some companies would have had to lay off employees or shut down entirely if they hadn’t paid Conti. Cypfer follows U.S. sanctions on groups listed by name, such as Evil Corp, Tobok said. “Either they’re on the sanctions list or they’re not,” he said of Conti. “I don't include morals here.”

The lack of clarity puts the onus on victims to discover if their attacker falls into a sanctioned category. Determining whether groups are operating out of North Korea or Iran, for example, or on behalf of the FSB is “very, very challenging because there’s obviously efforts to conceal that on the other side,” said Ryan Fayhee, a sanctions attorney who works with victims.

The government makes it seem “as if this is a traditional commercial enterprise and you can just simply screen the criminal,” he added. “That’s not how it happens.”

The federal government has long discouraged the payment of ransom and in recent years has put the professionals who work with ransomware victims on notice. In October 2020 the Treasury Department issued an advisory saying that “companies that facilitate ransomware payments to cyber actors on behalf of victims” may “risk violating OFAC regulations.” A second advisory, in 2021, seemed to acknowledge that victims sometimes make payments that violate sanctions. In those cases, victims and their representatives may receive leniency if they quickly report the incident and payment to OFAC.

Since many victims in the past have been loath to report attacks to the FBI, fearing that the intrusion would become public or the FBI would instead investigate the company itself, the Treasury Department hoped the guidance would prompt more victims to work with law enforcement. That, in turn, could lead to more indictments and more sanctions.

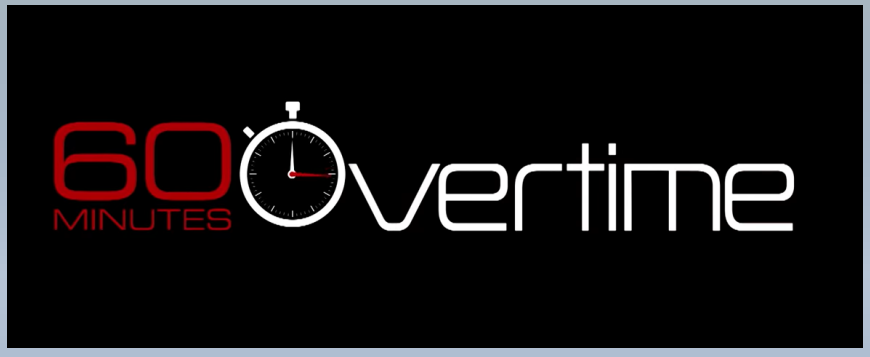
That part of the strategy seems to be working: More victims are reporting incidents to law enforcement, according to Waters. Following the 2021 advisory, many insurers began requesting proof that policyholders making ransomware claims report the incidents to the FBI, he said. The insurers he works with heavily weigh decisions made by intermediaries such as negotiating firm Coveware. Following Conti’s proclamation about Russia, Coveware stopped making payments to the group, said its co-founder, Bill Siegel. Coveware continued to negotiate with Conti, allowing time for the victim to assess the situation, prepare a public relations strategy and make arrangements to notify people affected by the breach.

For its part, Conti laid low following the late February leak of its messages, then launched a final burst of intrusions in April, including a significant one against the Costa Rican government. But that attack, AdvIntel told BleepingComputer, seemed intended to provide cover while Conti protected its online infrastructure. Not unlike the Russian army in Ukraine, it seemed, Conti’s forces were making a tactical retreat in preparation for future attacks.

Video of the Month

How Bellingcat is using TikTok to investigate the war in Ukraine - YouTube

The data detectives at Bellingcat showed 60 Minutes how social media is providing evidence of alleged Russian war crimes and other atrocities.



Documenting Corporate Deceit

May 01, 2022
From The President And Ceo
Bruce Dorris, J.D., CFE, CPA
https://acfeinsights.squarespace.com/acfe-insights/2022/5/1/documenting-corporate-deceit

Alex Gibney has documented many fraud cases in his three decades as a filmmaker. From his first big hit in 2005, “Enron: The Smartest Guys in the Room,” to the more recent documentary about Elizabeth Holmes, “The Inventor: Out for Blood in Silicon Valley,” Gibney has long been exploring the psychology of deceit and why bright and talented people turn to the dark side.

Gibney’s films have laid bare the greed, fraud and corruption that take place across the corporate world. So, it’s fitting that he’s this year’s winner of the Guardian Award, which the ACFE presents annually to a person who shows determination and perseverance in exposing specific acts of fraud and white-collar crime. The ACFE will present the award at our 33rd Annual Global Fraud Conference June 19-24 in Nashville.

Gibney’s work educates and entertains us. But we’re also shocked to see how easily the subjects of his documentaries deceive the public via charm and good narratives. As Gibney points out in this issue’s cover story, Holmes was a superb storyteller. She conned former heads of state and savvy investors who willfully denied her lies because they wanted to believe her inspiring story.

Years after the collapse of her company, Theranos, Holmes was found guilty in January of lying to investors about the capabilities of her blood-testing device, which in retrospect was destined to fail. Fraudsters often succeed for so long, says Gibney, because people fail to ask the simple questions that would expose wrongdoing. Holmes’ investors preferred to believe they were helping to create a revolutionary new technology to improve lives.

Indeed, the driving forces behind fraud, particularly in the corporate world, can be complex. But as Gibney’s films also show, a poor or outright corrupt tone at the top often justifies — in fraudsters’ minds — bad behavior. ACFE research consistently demonstrates that poor tone at the top is a principal internal control weakness. Controls serve no function if those in charge of enforcing them are the primary violators.

Brave whistleblowers who populate Gibney’s films — such as Sherron Watkins, Erika Cheung and Tyler Shultz — unmask and speak out against corrupt executives. Our recently released Occupational Fraud 2022: Report to the Nations shows once again how important hotlines are for organizations — 42% of frauds were detected by tips, with more than half of those coming from employees. (See ACFE.com/RTTN.)

The ACFE is proud to honor Mr. Gibney. We feel he must be a fraud examiner at heart — his documentaries expose fraud, help bring those who commit it to justice and remind everyone to be vigilant in searching for the truth.

Scammers in the Spotlight

May 09, 2022
Laura Harris
ACFE Research Specialist
https://acfeinsights.squarespace.com/acfe-insights/2022/5/9/scammers-in-the-spotlight

Grab the popcorn, uncork the wine and settle in for a wild ride. Fraudsters and their schemes are having quite a moment in pop culture. We've compiled a list of the most popular recent limited series, documentaries and films about fraud that can add context to known cases, illustrate some common fraud schemes and provide insight into the fraudsters at the center of these now infamous frauds. Keep in mind, some of these shows may have taken a few liberties with the details of the cases for entertainment purposes.

Fruitcake Fraud (Discovery+)

The year is 1896 — deep in the heart of Texas, in a little town called Corsicana, on a little street called Collin, a bakery was born. Famous for fruitcake, Collin Street Bakery became known worldwide, garnering royal and celebrity clientele. More than a hundred years later in 2013, a nondescript bookkeeper named Sandy Jenkins was discovered to have embezzled nearly $17 million over a decade.

Scheme: Starting in 2004, Jenkins wrote company checks to his personal creditors. Over eight years, he misappropriated 888 checks totaling $16.6 million. Jenkins was charged with 10 counts of mail fraud and three counts of money laundering. His wife, who aided in the embezzlement, was charged with conspiracy to commit money laundering, six counts of money laundering, aiding and abetting, and two counts of making a false statement to a financial institution.

Bad Vegan: Fame. Fraud. Fugitive. (where to watch)

Take equal parts theft, fake identities and gourmet cooking and mix thoroughly with a ridiculous splash of immortality claims to bake this vegan romance fraud. Chris Smith, producer of the popular documentaries "Tiger King" and "Fyre," interviews many involved in the story of Sarma Melngailis in this four-part docuseries.

Scheme: Melngailis wired over $1.6 million from her business — meant for employee wages, investor debt and taxes — to her husband, Anthony Strangis, who was committing fraud under the name Shane Fox. A 24-count indictment charged the couple with grand larceny, criminal tax fraud, scheme to defraud and violation of labor law and related counts.

The Dropout (where to watch)

Amanda Seyfried stars as convicted fraudster Elizabeth Holmes, the deep-voiced, black-turtlenecked founder of Theranos, in this eight-part Hulu Original miniseries, based on the podcast of the same name. Holmes set out to change the health care industry with her biotech startup, once valued at more than $10 billion, but half-truths caught up with her, and Theranos' star-studded board of directors could no longer obscure the facts.

Scheme: Holmes was charged with 10 counts of wire fraud and two counts of conspiracy to commit wire fraud. One conspiracy count addressed defrauding investors while the other addressed allegations of defrauding patients of the Theranos service. The 10 counts of wire fraud addressed similar allegations. Ramesh "Sunny" Balwani, former Theranos president and COO, and Holmes' ex-boyfriend, faces similar charges.

Inventing Anna (where to watch)

"This whole story is completely true ... Except for all the parts that are totally made up." Shonda Rhimes brings her golden touch to the wannabe fairy tale of German heiress Anna Delvey, who turned out to actually be Russian-born Anna Sorokin. She became an Instagram influencer, as well as a fraudster, scamming the social elite of NYC.

Scheme: The dream involved a $22 million loan to create an exclusive private club at 281 Park Avenue in Manhattan. The scheme required stealing money from friends and seemingly bottomless credit from hotels and banks. Was Sorokin "dangerously close" to reaching that dream or not?

The Tinder Swindler (where to watch)

Simon Leviev, posing as the son of the "King of Diamonds" Lev Leviev, was looking for love on the dating app Tinder. Born as Simon Hayut, he procured a tidy $10 million in his Ponzi tour through Europe. Seducing women and their bank accounts, Leviev shrewdly manipulated his victims to support him and help hide him from enemies out to do him harm.

Scheme: Theft, forgery, fraud, oh my! Simon Leviev, as he is legally known, has faced and continues to face multiple charges in countries throughout Europe for his schemes. However, according to experts, his "swindling is an international issue — not a national problem, which is easier to prosecute."

Have You Seen This Man? Season 2 (where to watch)

From podcast to documentary, the outlandish story of John Ruffo's $350 million bank fraud is yet to reach a conclusion. In this series, ABC News Investigates partners with the U.S. Marshals to crowdsource the capture of this top-15 most wanted fugitive. With a 150-count indictment hanging over him for bank fraud, money laundering, wire fraud and conspiracy, and bail set at $10 million, Ruffo was found guilty. In 1998 as he was set to surrender for a 17-year prison sentence in New York, he turned in his ankle monitor and casually fled the state — and possibly the country. The strange tale of Ruffo begs the question: Have you seen this man?

Scheme: With help from a former Philip Morris executive Edward Reiners, Ruffo pitched "Project Star" — a bogus project for Philip Morris's smokeless cigarettes — to banks for financing. Ruffo's computer company, CCS, would provide the hardware and consulting for five offices. Forged documents were also discovered in due diligence research. Strict confidentially agreements stipulated that Reiners, not Phillip Morris, was to be contacted in any communication. Not suspicious at all…

Trust No One: The Hunt for the Crypto King (where to watch)

QuadrigaCX was once one of the biggest crypto exchanges before the owner mysteriously died, leaving all access to funds lost — about $250 million in the crypto wallet. On his honeymoon in India, founder Gerald Cotten died from Crohn's disease complications, but many people do not believe this is the truth. Then, five Quadriga cold wallets were found empty.

Scheme: While no charges exist and answers are unavailable, many believe Cotten faked his own death and absconded with the money in an exit scam. Others believe Cotten may have been running a Ponzi scheme.

How To Catch a Fraudster That Doesn't Exist

May 12, 2022
Neil Dubord, CFE, Chief of Delta Police Department
https://acfeinsights.squarespace.com/acfe-insights/2022/5/12/how-to-catch-a-fraudster-that-doesnt-exist

With the development of websites such as This Person Does Not Exist, anti-fraud professionals are continuing to see a rise in synthetic identity fraud.

Synthetic identity fraud occurs when perpetrators combine piecemeal and, at times, factual information to create a new identity. These identities are cheap, quick and easy to produce, and may include a factual piece, or pieces, of information from sources such as breached data sites. Synthetic identity fraud is reportedly the fastest-growing type of financial crime, costing online lenders more than $6 billion annually. With the explosive growth of decentralized finance, synthetic identity fraud will continue to rise. Besides its insidious nature, synthetic identity fraud is also becoming one of the most challenging frauds to detect, investigate and prosecute.

Fraudsters may take years to build good credit with their synthetic identity through a series of small purchases or loans that they pay off quickly. All this time, they are working to build trust and creditability with lenders so they can take out a large withdrawal — or in other words, one big payday. Once they have successfully defrauded their victim and obtained the asset they were pursuing, the fraudster will abandon the synthetic identity and never use it again. Abandoning the identity is called "busting out." Investigations are further complicated because the information is fragmented, and often identifying pieces of information, such as social insurance numbers, belong to real people.

With the growth of decentralized finance and online lending processes, a proactive, multilayered approach is recommended for Know Your Customer (KYC) assessments. To put a spin on a time-honored phrase, the best offense is a good defense, and that defense for synthetic identity fraud is KYC.

In today's era, determining if a thief uses a synthetic identity can involve implementing advanced technology. The implementation of technology such as artificial intelligence and blockchain will serve to assist in preventing individuals from building and using synthetic identities. Many believe that blockchain technology used in some areas of decentralized

finance allows individuals to remain anonymous and to commit their criminal acts undetected. However, this is not true, and companies such as Chainalysis have developed a platform that powers investigations, compliance and risk management, and ultimately helps solve crimes. Not all organizations have the sophistication or resources to implement technology to assist with synthetic identity fraud detection, which begs the question of what organizations can do right now to defend against this type of fraud.

A thorough KYC process is still an effective and efficient tool for recognizing synthetic identities. If a thief is going to go through the effort of creating a synthetic identity, they typically do not provide a picture of themselves. A vigilant compliance officer undertaking a methodical KYC process should use as many tools as possible to validate that the information received, including the person's picture, is accurate. Open-source intelligence (OSINT) is a tool that is often used to provide additional information.

A new free tool to add to your KYC toolkit involves a free, easy-to-use Chrome extension, PetaPixel, which can be used to detect fake pictures like those produced by This Person Does Not Exist. This new tool claims to distinguish fake pictures with 99.29% accuracy. It is quick and straightforward to use. First, you install the PetaPixel Chrome extension. Once it has been installed, photos can be scanned in seconds and the results can then be used as part of your KYC process. It is important to note that currently PetaPixel extension only works on GaN-generated images, such as those images from This Person Does Not Exist. Although I recommend using PetaPixel, it should not be the sole source of information in your KYC assessment, as high-quality deepfakes will not be detected.

KYC assessments are an iterative process, and compliance officers should always be looking for new ways to protect their organizations against fraud. While tools like PetaPixel are not a silver bullet, fraud examiners should explore such offerings to aid in the assessment process.

Quote of the Month

“We believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.”

- **Ginni Rometty, IBM Corp.’s Chairman, President and CEO**