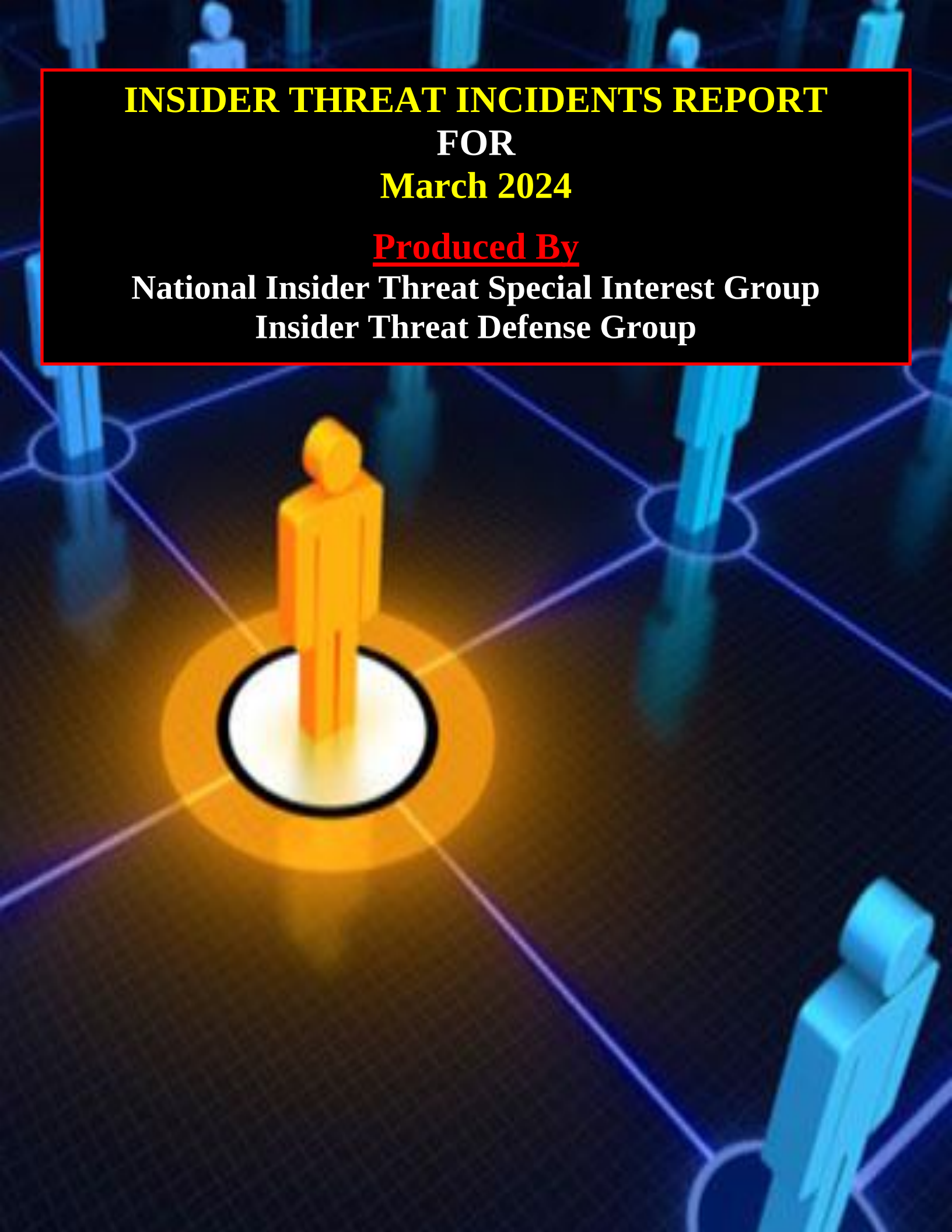
# INSIDER THREAT INCIDENTS REPORT
# FOR
# March 2024

## Produced By

**National Insider Threat Special Interest Group**
**Insider Threat Defense Group**



# TABLE OF CONTENTS

# INSIDER THREAT INCIDENTS

## *A Very Costly And Damaging Problem*

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees' who are negligent, malicious or opportunists. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **5,200+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees', and this very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

According to the Association of Certified Fraud Examiners 2024 Report To the Nations, the 1,921 fraud cases analyzed, caused losses of more than **$3.1 BILLION.**

To grasp the magnitude of the Insider Threat problem, one must look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to **significant underreporting** on the Insider Threat problem.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the **Actual Malicious Actions** employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live a better lifestyle, etc.

Some organizations invest thousands of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of these monthly reports, you might have a different perspective on Insider Threats.

The Human Operating System (Brain) is very sophisticated and underestimating the motivations and capabilities of a malicious or opportunist employee can have severe impacts for organizations.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report and other shows.

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for IRM. The incidents listed on pages **4 to 31** of this report provide the justification, return on investment and the funding that is needed for an Insider Risk Management Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

# INSIDER THREAT INCIDENTS
## FOR MARCH 2024

**FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS**

**International Commodities Trading Company To Pay $661 Million+ In Criminal Penalties For Employees Roles In Foreign Bribery Case**

Gunvor S.A. (Gunvor), is an International commodities trading company based in Switzerland.

Between 2012 and 2020, Gunvor and its co-conspirators paid more than $97 million to intermediaries knowing that some of the money would be and in fact was used to bribe Ecuadorean officials, including Nilsen Arias Sandoval, a then-high ranking official at Petroecuador. As part of the scheme, Gunvor managers and agents attended meetings in the United States and elsewhere. The bribe payments were routed through banks in the United States using shell companies in Panama and the British Virgin Islands controlled by Gunvor's co-conspirators. Among other things, a Gunvor employee also directed one of the intermediaries to use the money to purchase an 18-karat gold Patek Philippe watch for Arias.

In connection with the resolution, Gunvor entered into a plea agreement with the government and pleaded guilty to an information charging the company with conspiracy to violate the anti-bribery provisions of the Foreign Corrupt Practices Act. The court ordered Gunvor to pay a criminal monetary penalty of $374,560,071 and to forfeit $287,138,444 in ill-gotten gains. The sentence includes credits of up to one-quarter of the criminal fine each for amounts Gunvor pays to resolve investigations by Swiss and Ecuadorean authorities into the same misconduct so long as the payments are made within one year of today's date.

The Department Of Justice also considered Gunvor's history of misconduct. In October 2019, Gunvor reached a resolution with the Office of the Attorney General of Switzerland concerning a corrupt scheme to bribe officials in Congo-Brazzaville and Côte d'Ivoire to secure oil contracts obtained between approximately 2009 and 2012. As part of the 2019 Swiss resolution, Gunvor admitted that it lacked sufficient controls to prevent the underlying misconduct and failed to take "all the reasonable organizational measures" required to prevent Gunvor's employees and agents from engaging in bribery. (Source)

**U.S. GOVERNMENT**

**Former Social Security Administration Employee Charged For Embezzling $1.8 Million+ Of Social Security Funds For 12 Years - March 14, 2024**

Myrna Faria was employed by the Social Security Administration (SSA) from approximately 1991 through 2019 as a Social Insurance Specialist and Claims Specialist" working in the Workload Support Unit in San Juan, Puerto Rico.

From March 2012 through March 2024, Faria embezzled and stole SSA funds, namely Retirement Insurance Benefits, Survivors Insurance Benefits and Auxiliary Benefit payments, to which she knew she was not entitled. In total, Faria stole approximately $1,812,455.10.

Faria utilized her position within SSA to submit false claims on behalf of others, using the identity of individuals she believed to be deceased. She then approved those false claims and submitted her own bank and address information to fraudulently receive the corresponding SSA beneficiary proceeds. Faria proceeded to withdraw, transfer, and spend the money from the accounts that fraudulently obtained the SSA funds. Over the span of twelve years, Faria submitted and approved 13 fraudulent claims. A total of 10 fraudulent claims were still active and receiving funds as of the date of the Indictment. (Source)

**Interior Department Employee Sentenced To 5 Years Of Probation For Embezzling $139,000+ Using Fake Vendor Scheme - March 20, 2024**

Beginning in May 2018 and continuing through April 2020, George Onwiler embezzled approximately $139,000 from the Bureau of Reclamation (BOR), a component of the United States Department of the Interior. Onwiler was employed as an electrician for the BOR, located in Yuma, Arizona. In his employment with the BOR, Onwiler was responsible for purchasing commercial and agricultural grade electrical supplies and materials needed for his government work, and he was issued a BOR credit card to make those purchases.

Onwiler embezzled money from the government by using his government issued credit card to pay fictional electrical company suppliers. Onwiler created fake company names and used PayPal and Block/Square to transfer money to himself. Through 47 unauthorized wire transfers, Onwiler transferred $139,168.02 to his personal bank account. These transactions were fraudulent as he did not purchase electrical supplies for the BOR. (Source)

**U.S. Postal Service Employee Charged With Embezzling $19,000+ / Gave Funds To Boyfriend & Family Members - March 22, 2024**

Christine Hedges began working for USPS around 2020, most recently as a Lead Sales & Service Associate in Brockton.

It is alleged that from approximately October 2021 to August 2023, Hedges engaged in a scheme to steal USPS funds for her personal use. As part of this scheme, Hedges allegedly generated, for her own use, no-fee money orders without a customer physically present at her customer window and which a customer did not request. Hedges also allegedly stole cash from her USPS workstation and often attempted to conceal her theft by replacing the cash with these fraudulent money orders. Hedges allegedly generated approximately 70 fraudulent no-fee money orders. 11 of those no-fee money orders were made out to her boyfriend or a family member. From on or about Aug. 1, 2023 to on or about Aug. 14, 2023, video surveillance from above Hedges' workstation allegedly showed Hedges on at least one occasion removing cash from her assigned drawer and putting it in her pocket. In all, Hedges allegedly embezzling over $19,707 in postal funds. (Source)

**U.S. Postal Service Employee Sentenced To Prison For Stealing Mail Over 4 Years - March 5, 2024**

Pamela Jo Rosas pleaded guilty to theft of mail by a postal employee and was sentenced to 37 months.

In April 2020, postal inspectors began receiving complaints that a series of parcels containing valuable coins were missing after being placed in the post office for delivery. Federal agents conducted surveillance and identified a postal employee, Pamela Jo Rosas, as a subject involved in the theft after viewing her handling packages in a suspicious manner. Rosas was also found in possession of several pieces of stolen mail packages after leaving work. Rosas admitted to stealing many items from the post office during the previous three to four years. Agents were able to recover hundreds of valuable coins from her apartment, along with other items Rosas had stolen from the mail during the course of her employment. (Source)

**4 U.S. Postal Service Employees Charged For Delay Of 40 Pieces Of Election Mail - March 14, 2024**

In September 2022, the Puerto Rico State Elections Commission (Commission) conducted a Special Election for the San Juan, Puerto Rico District 1 Senate vacancy. As part of the Commission's services provided for the Special Election, in August 2022, the Administrative Board of Absent Voting and Early Voting ("Junta Administrativa de Voto Ausente y Voto Adelantado" ("JAVAA")) mailed ballots to certain eligible voters in Puerto Rico, via USPS certified mail service.

Four individual mail carriers, employed by the USPS, delayed and did not deliver a total of forty pieces of election mail from the September 2022 Special Election to domiciled active voters in San Juan. (Source)

**FEMA Employees Brought Government Devices Abroad (China, Iraq) Without Authorization According To FEMA OIG Report - February 26, 2024**

The Federal Emergency Management Agency Office of the Chief Information Officer has tracked scores of employees bringing government mobile devices abroad, including to countries like China and Iraq, without authorization, according to a document obtained by FedScoop.

The issue was highlighted in a DHS inspector general's report published last July that pointed to concerns about how the emergency management agency handles the security of government-issued mobile devices. Among other issues, the report centered on concerns with international travel.

FEMA policies stipulate that employees cannot bring government devices abroad, while DHS policy requires the use of loaner devices and that any device detected internationally (without authorization) is turned off. The inspector general found that FEMA was not effectively tracking whether data on devices taken on international travel had been wiped.

FEMA is still working on fixes, originally expected in December of last year, to address the issue, which heightens security risks and violates broader Department of Homeland Security mobile device policy. (Source)

**DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY**

**Army Civilian Employee Pleads Guilty To $108 Million Fraud Fake Company Scheme / Used Funds For Jewelry, Clothing, Vehicles, 31 Real Estate Properties - March 2, 2024**

Jenet Mello worked for the Army as a civilian Financial Program Manager at Fort Sam Houston in San Antonio, Texas.

Mello allegedly stole more than $100 million in Army funds by regularly submitting fraudulent paperwork that indicated an entity she controlled, Child Health and Youth Lifelong Development (CHYLD), was entitled to receive funds from the Army. Mello claimed that CHYLD provided services to military members and their families, when, in reality, CHYLD did not provide any services. The indictment alleges that Mello instead used the funds to buy millions of dollars in jewelry, clothing, vehicles, and real estate. Additionally, Mello is alleged to have falsified the digital signature of one of her supervisors on multiple occasions.

The U.S. government is investigating the 31 properties under her name in Texas, New Mexico, Colorado and Washington, as well as about 80 motorcycles and $18 million discovered in six bank accounts.

Another new article stated that Mello was allowed to retire with full benefits, the San Antonio Express-News has confirmed. (Source)

**Former Navy Civilian Employee & Former Company Executive Charged In Bribery Scheme Involving $100 Million+ In Government Contracts - March 7, 2024**

A former civilian employee of San Diego-based Naval Information Warfare Center and a former executive with a South Carolina defense contractor were chargedwith participating in a bribery scheme to trade expensive meals, jobs and a ticket to a premiere sporting event for help obtaining more than $100 million in government contracts.

James Soriano worked for the Naval Information Warfare Center, which provided contract administration services for the Navy. From 2006 to 2019, Soriano was an engineer, project leader and certified "Contracting Officer Representative" with technological expertise to help manage Department of Defense contracts.

Soriano was supposed to act as liaison between the government and the contractor, including keeping contractor bid, proposal and selection information confidential, and protecting the integrity of the acquisition process by maintaining fairness in the government's treatment of all bidders.

Soriano instead used his considerable influence to steer lucrative contracts to Russell Thurston of Mt. Pleasant, South Carolina, who was an executive vice president of a company vying for defense contracts with locations in Arlington, Virginia, and Charleston, South Carolina. The company provided technical and consulting services in the information technology field.

Thurston and others working under him, gave Soriano various things of value including jobs for a family member and friends, free meals at various restaurants, as well as a ticket to the 2018 MLB All Star Game held at Nationals Park in Washington, D.C. One of the friends who was given a job at Soriano's request gave Soriano half her salary every month—approximately $2,000 per month—in cash. The indictment indicates the friend was not actually performing the duties for which she was being paid.

In return, Soriano took official action to benefit the company, including allowing Thurston and other employees to draft procurement documents for various contracting efforts, even where the company was competing for the contract against other bidders.

As a result of Soriano's efforts, the company won a task order with a more than $300 million ceiling. Soriano then approved numerous projects on this task order, ultimately causing the government to obligate more than $100 million to the company.

To conceal their activities, Thurston, Soriano, and other employees at the company would intentionally delete document properties on procurement documents drafted by employees. (Source)

**Army Reserve Officer Pleads Guilty To $488,000+ COVID Relief Fraud Scheme / Used Funds For Investment Ventures & To Pay Debts - March 6, 2024**

Russell Laraway, an Army Reserve officer, incorporated two business entities in Virginia that he purported to operate out of his home in Leesburg: Loudoun Innovation LLC ("LI LLC") and Commonwealth Commerce LLC ("CC LLC"). Beginning in April 2020, Laraway submitted loan applications through the Paycheck Protection Program (PPP), a COVID-19 relief program that was intended to provide loans backed by the Small Business Administration to certain businesses, nonprofit organizations, and other entities to help them retain their employees or stay afloat during the pandemic. In his applications, Laraway inflated the numbers of people his business entities employed and falsified payroll expenses and revenues for each company.

Laraway sought loan forgiveness for some of the PPP loans by falsely certifying that the PPP money had been used solely for payroll or other authorized purposes, while he actually intended to use the money to engage in spurious investment ventures and pay off personal debts.

Laraway fraudulently received two PPP loans for LI LLC and two PPP loans for CC LLC. The four PPP loans totaled approximately $488,952, some of which Laraway paid to foreign entities in scams of which he was a victim. (Source)

**U.S. Government Contractor Project Manager Pleads Guilty To $100,000+ Kickback Scheme To Defraud U.S. Army Facility - January 30, 2024**

Kevin Mahler was a project manager for a government contractor. He pleaded guilty for his role in a conspiracy to inflate project costs by over $200,000 and receive kickbacks related to contracts for commercial flooring services at a U.S. Army facility in Fairbanks, Alaska.

From March 2016 to March 2021, Mahler conspired to receive kickbacks from Benjamin McCulloch, the owner of a commercial flooring services company, related to construction contracts administered by the U.S. Army at Fort Wainwright.

Mahler pleaded guilty to conspiring with McCulloch to inflate the costs of flooring construction subcontracts and receiving half of the proceeds as kickback payments from McCulloch. During the five-year scheme, Mahler received over $100,000 in kickbacks. As a part of his plea, he has agreed to pay restitution. (Source)

**Air Force Employee Charged For Unlawful Disclosure Of Classified Information On Foreign Online Dating Website - March 4, 2024**

David Slater worked in a classified space at USSTRATCOM and held a Top Secret security clearance from in or around August 2021 until in or around April 2022, after retiring as a Lieutenant Colonel from the U.S. Army.

Slater attended USSTRATCOM briefings regarding Russia's war against Ukraine that were classified up to TOP SECRET SENSITIVE COMPARTMENTED INFORMATION (TS//SCI).

Slater then transmitted classified information that he learned from those briefings via the foreign online dating website's messaging platform to his co-conspirator, who claimed to be a female living in Ukraine on the foreign dating website. The co-conspirator regularly asked Slater to provide her with sensitive, non-public, closely held and classified information and called Slater in their messages her "secret informant love" and her "secret agent." In response to these requests, Slater indeed provided classified information to her, including regarding military targets and Russian military capabilities relating to Russia's invasion of Ukraine. (Source)

**U.S. Army Intelligence Analyst Charged With Conspiracy To Obtain / Disclose Classified Information, Export Control Violations & Bribery - March 7, 2024**

Korbein Schultz, a U.S. Army soldier and intelligence analyst, was arrested at Fort Campbell following an indictment by a federal grand jury charging him with conspiracy to obtain and disclose national defense information, exporting technical data related to defense articles without a license, conspiracy to export defense articles without a license, and bribery of a public official,.

From June 2022 until the time of his arrest today, Schultz conspired with an individual, identified as Conspirator A, to disclose documents, writings, plans, maps, notes, and photographs relating to national defense as well as information relating to national defense which Schultz had reason to believe could be used to injure the United States or used to the advantage of a foreign nation. Conspirator A recruited Schultz, who possessed a Top Secret security clearance, and frequently tasked him to gather documents and sensitive U.S. military information. Specifically, Conspirator A tasked Schultz with gathering information related to a variety of U.S. military weapons systems, including classified information, and information related to the United States' potential plans in the event that Taiwan came under military attack.

Some of the information that Schultz provided to Conspirator A included documents related to the High Mobility Artillery Rocket System (HIMARS), information on hypersonic equipment, studies on the future development of U.S. military forces, studies on major countries such as the People's Republic of China, and summaries of military drills and operations.

In exchange for the documents and information, Conspirator A made at least 14 payments to Schultz that totaled approximately $42,000. Throughout the entirety of the conspiracy, Conspirator A represented to Schultz that he lived in Hong Kong and worked for a geopolitical consulting firm based overseas.

During the course of the conspiracy, Schultz also sent Conspirator A three documents that violated the Arms Export Control Act (AECA). The three documents included an Air Force Tactics Techniques and Procedures manual for the HH-60W helicopter, an Air Force Tactics Techniques and Procedures manual for the F22-A fighter aircraft, and an Air Force Tactics Techniques and Procedures manual for intercontinental ballistic missiles. (Source)

**Air National Guardsman Agrees Pleads Guilty To Disclosing Classified Information - March 1, 2024**

JackTeixeira enlisted in the U.S. Air National Guard (USANG) in September 2019, and was stationed in Massachusetts.

Teixeira has held a Top-Secret security clearance since 2021. It is alleged that, beginning in or around January 2022, Teixeira unlawfully retained and transmitted National Defense Information classified as TOP SECRET or SECRET and / or Sensitive Compartmented Information (SCI), onto a social media platform to persons not authorized to receive such information.

Teixeira allegedly accessed classified documents containing National Defense Information from a classified workstation at the Otis USANG Base and transcribed and transmitted the information in written paragraphs to other users on the social media platform. Teixeira also allegedly posted images of classified documents to the social media platform, which bore standard classification markings, including SECRET, TOP SECRET and SCI designations, indicating that they contained highly classified U.S. government information. (Source)

**Air Force Police Officer Convicted Of $150,000+ In COVID Unemployment Insurance Fraud - March 5, 2024**

Between April 2020 and June 2020, Treveon Miller submitted fraudulent claims in several states using his former name of Trevon Rodney. Miller told the state agencies that administer the unemployment insurance system that he was unemployed when he was an active-duty Air Force Police Officer the whole time. The claims were worth more than $150,000 and the money was put onto debit cards that were mailed to Miller. (Source)

**U.S. Marine Pleads Guilty To Gun Trafficking Charges - March 1, 2024**

Rylan Peterson while serving as a private first class in the Marine Corps at a base in North Carolina, admitted that he entered into an agreement with Oryn McLeod, for Peterson to acquire six semi-automatic handguns on behalf of McLeod and others.

Peterson then obtained the guns from North Carolina resident Mitchell Locke, who purchased them from a licensed dealer in North Carolina, falsely representing at the time of the purchase that he was acquiring the firearms for himself. McLeod paid Peterson for the guns, which Peterson transported to New York from North Carolina. McLeod was subsequently arrested for unlawful possession of two of the handguns. (Source)

## CRITICAL INFRASTRUCTURE

**Former Ontario Nuclear Power Plant Operator Charged With Making Online Posts About Security Vulnerabilities - February 20, 2024**

A former employee of the Crown corporation that operates Ontario nuclear plants has been charged with leaking "safeguarded information" that could harm Canada. James Mousaly faces a rare charge under the Security of Information Act.

A source familiar with the investigation stated a former employee was accused of making online posts about security vulnerabilities. The alleged offence occurred between Jan. 30 and Feb. 1, 2024. He faces a possible life sentence if convicted. (Source)

## LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

**Former FBI Agent Trainee Sentenced To Prison For $1.4 Million+ Insider Trading Scheme Using Information He Acquired From Girl Friends Law Firm - March 13, 2024**

In early 2021, Seth Markin and Brandon Wong together made more than $1.4 million dollars in illegal profits by trading in stock based on inside information that Markin stole from his then-girlfriend, who was at the time an attorney at a major law firm in Washington D.C.

At the time, Markin had been accepted into the Federal Bureau of Investigation (FBI) as a new agent trainee, and Wong was a systems analyst at an education company.

In February 2021, Markin secretly looked through the Law Firm Associate's confidential work documents, without her permission, and learned that, in a matter of weeks, Merck, a publicly traded pharmaceutical company, was going to acquire Pandion, a publicly traded biotechnology company. Markon immediately purchased Pandion stock on the basis of this material, non-public information and also told several family members and friends to purchase Pandion's stock.

In total, Markin and Wong together caused at least 20 people to trade in Pandion stock based on the material, non-public information that Markin misappropriated from his girlfriend, resulting in millions of dollars of illegally obtained trading profits. To conceal their illegal insider trading scheme, Markin and Wong used an encrypted messaging application and deleted many of their text messages with each other. They also agreed on a cover story that they could provide to law enforcement, namely, that if they were asked how they anticipated Pandion's stock price increase, they could say they read it on Stocktwit, in reference to a social media platform for sharing stock ideas, and falsely say that the news was publicly being announced there.

After Merck's acquisition of Pandion was announced publicly, and the Pandion stockholdings of Markin and Wong, and those whom they tipped, significantly increased in value, the defendants sold their shares of Pandion for significant profits. With their illegal profits, the defendants and their tippees purchased luxury items and bought gifts for each other. For example, Wong purchased for Markin a Rolex watch valued at approximately $40,000, a trip to Hawaii, and a meal at a three-Michelin-starred restaurant in New York that cost more than $1,000. Wong also purchased a home in Florida. (Source)

**Former Treasurer For State Police Foundation Pleads Guilty To Stealing $79,000 / Put Funds Into Cryptocurrency Account - March 8, 2024**

LeAnn Shirley admitted that in 2019 when she was the llinois State Police Heritage Foundation Treasurer, she devised a scheme to defraud the Illinois State Police Heritage Fund, by causing approximately $79,000 to be wired from a Foundation bank account in Illinois to an account in Vermont. After the money was transferred to the bank in Vermont, all but approximately $5,000 of it was then transferred into a cryptocurrency account by a third-party.

To facilitate the initial transfer, Shirley falsely claimed to bank employees that the payment was being used to ship items for the Foundation and that the Foundation would be reimbursed in the next couple of weeks. (Source)

**2 Former Miami Police Department Employees Plead Guilty To $30,000+ COVID-19 Relief Fraud Scheme - March, 12, 2024**

On March 6, 2024, Sheana Haslem, 38, who was formerly a MPD Police Staffing Specialist, pled guilty to wire fraud in connection with her fraudulent applications for a Paycheck Protection Program (PPP) loan and an Economic Injury Disaster Loan (EIDL) advance, before U.S. District Judge Kathleen M. Williams.

On July 6, 2020, Sheana Haslem, who at the time was employed full-time by the Miami Police Department, submitted with the assistance of an associate a fraudulent Economic Injury Disaster Loan (EIDL) application to the U.S. Small Business Administration (SBA).

That fraudulent application stated Haslem to be an independent contractor and the 100% owner of a hair and nail salon business operating under her own name. That EIDL application falsely certified that for the 12-month period prior to January 31, 2020, Haslem's business had gross revenues of approximately $89,993 and 15 employees. As a result of this fraudulent application, Haslem obtained from the SBA a $10,000 EIDL advance.

On February 27, 2021, Haslem submitted, and with the assistance of the same associate, caused to be submitted, a fraudulent PPP loan application claiming to be an independent contractor operating a business under her own name.

That application falsely represented the business' average monthly payroll as being $8,333, and as part of the application process, Haslem submitted a fraudulent IRS Form 1040, Schedule C, for tax year 2019, claiming she had a security officer business that had a gross income of $102,874, no expenses, and a net profit of $102,874. As a result of this fraudulent application, Haslem obtained a $20,832 PPP loan from an SBA approved lender. (Source)

**Sheriff's Office Deputy Convicted Of $31,000+ Of COVID-19 Relief Fraud While Employed - March 6, 2024**

In 2021, Stephanie Smith applied for and received two PPP loans for herself as a sole proprietor doing business as Children 1st Basketball Training and Agape Smith Vending, respectively. Smith presented materially false information about each business's total amount of gross income for the year 2019, including a falsified IRS tax form submitted with each application. Smith also sought and received forgiveness of both fraudulently obtained PPP loans, which totaled over $31,000 in principal and interest. During the period of the scheme, Smith was employed as a deputy sheriff in BSO's Department of Law Enforcement. (Source)

**Prisons Correctional Officer Sentenced To Prison For Accepting $5,000+ In Bribes To Smuggle Cigarettes And Love Letters Into Prison - March 20, 2024**

Beginning in 2019, Jordan Kelsheimer was employed with the United States Department of Justice, Federal Bureau of Prisons, as a Corrections Officer. At the time of the offense, Kelsheimer was employed at the Federal Correctional Complex in Terre Haute, Indiana.

For weeks, Kelsheimer had been smuggling tobacco into the facility, which is prohibited for inmate use in federal prisons.

On July 17, 2022, staff found eight packs of Newport cigarettes and a stack of love letters from the inmate Kelsheimer. Kelsheimer admitted in an interview on July 18, 2022, that she had been bringing in Newport cigarettes and getting paid $400 per carton by an inmate's relative via CashApp. Electronic records showed that she made $5,140 total in 15 separate payments.

Upon further investigation and interviewed, various inmates reported that they had repeatedly observed Kelsheimer in intimate contact with the inmate in and near her office within the housing unit where she was assigned and reported that the contact included kissing and, on occasion, more intimate contact. (Source)

**County Sheriff's Deputy Pleads Guilty To His Role In A Drug Trafficking & Procurement Fraud Conspiracies - March 27, 2024**

While Michael Cox was a sheriff's deputy, he helped various drug traffickers operating in Wayne County North Carolina, to evade charges. In one instance, he intercepted a drug trafficker who had made a purchase from the target of a Drug Enforcement Administration (DEA) investigation. Rather than arrest the trafficker, he seized the drugs and reimbursed him $2000 for the sale, claiming it had been a planned, controlled purchase. Even after his retirement, Cox continued his relationships with the drug traffickers, facilitating the purchase of drugs for other individuals. In addition, Cox was engaged in a scheme in which contracts for upfits of WCSO vehicles were steered to a business owned by Cox, and employing co-defendant Christopher Worth, regardless of whether Cox's company provided such work at the lowest price as required by the Wayne County procurement requirements. (Source)

**STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS**

**New Mexico State Representative And Friend Charged For $1.1 Million+ Fraud Scheme To Defraud U.S. Government - March 28, 2024**

A former State Representative (Sheryl Stapleton) and her longtime friend (Joseph Johnson) are facing federal charges for long-term scheme to defraud the U.S. government.

The indictment alleges that from about July 1, 2013, through June 30, 2020, Stapleton used her position at Albuquerque Public Schools (APS) as Director of the Perkins Project and Career and Technical Education (CTE) Coordinator to direct approximately 40% of APS's non-personnel CTE funding to Robotics Management Learning Systems (Robotics), a company owned and operated by her close personal friend, Johnson, for use of and support for the CyberQuest software in APS classrooms.

Stapleton used the blank checks to write approximately 233 checks from Robotics for her own benefit, totaling approximately $1,152,506.00, or 35% of the funds APS paid to Robotics. (Source)

**New York City Transit Worker & State Court Officer Sentenced To Prison For $770,000 Of COVID-19 Loan Fraud / Used Funds To Pay Credit Card Debt / Purchase Cryptocurrency - March 20, 2024**

Between May 2020 and July 2020, amid the COVID-19 pandemic, Arthur Cornwall and Sean Williams fraudulently applied for, and received, at least six PPP and EIDLP loans, totaling approximately $770,000, on behalf of purported corporate entities they controlled. As part of the scheme designed to mislead the SBA and a financial institution disbursing the funds, the defendants submitted supporting documentation that contained false information, including the identity of the individual applying for the loan, the number of employees, revenue, payroll costs, and the intended use of the loan proceeds. Instead of using the funds for disaster relief, Cornwall and Williams diverted them for their personal use, including the discharge of personal credit card debt and the purchase of cryptocurrency. Following their guilty pleas, the defendants resigned from their respective government jobs. (Source)

**Former Town Clerk Charged For Embezzling $195,000 From Town - March 22, 2024**

Luke Servas embezzled more than $195,000 while employed as the Town Clerk for the Town Of Cusick, Washington, between October 2022 and March 2023. During that time period, Servas was also an elected member of the town council.

In March of 2023, other town officials expressed concern that funds were missing from the town's account. The Indictment alleges that Servas then contacted the Pend Oreille County Sheriff's Office to report that between $150,000 and $200,000 had been stolen from the Town of Cusick's operating bank account, using the mayor's credit card account to which Servas stated only the mayor had access. The Indictment further alleges that, after making this report, Servas wrote a fraudulent $4,961 check from Cusick's account to himself, forged the mayor's signature as well as that of another town official, and cashed the check on or about March 20, 2023. (Source)

## SCHOOL SYSTEMS / UNIVERSITIES

**Former County Education Official Pleads Guilty To Embezzling Nearly $16 Million From School District - March 28, 2024**

Jorge Contreras is the former Snior Director of Fiscal Services at an Orange County Public School district in California. He pleaded guilty today to embezzling approximately $15.9 million from the district over several years.

Law enforcement so far has seized approximately $7.7 million in personal and real property traced to the scheme, including a home in Yorba Linda, a 2021 BMW automobile, 57 luxury designer bags (Mostly Louis Vuitton), various pieces of jewelry, designer clothes and shoes, and eight bottles of Clase Azul Ultra luxury tequila.

Contreras, whom the school district hired in 2006, managed the district's fiscal operations. The schools in this district educate children from preschool through sixth grade, 81% of whom are classified as socio-economically disadvantaged.

Contreras managed and had access to various school district bank accounts as well as the student body bank account. Contreras caused checks from these accounts to be deposited into his personal bank account.

Contreras wrote checks in small dollar amounts written to "M S D," with the letters spaced out, and, after receiving the proper signatures from others, would include fictitious names and increase the amounts of the checks and deposit the checks into his personal bank account via ATMs. To conceal his fraud, Contreras provided bank reconciliation packets to others at the school district with falsified bank statements and records. In total, Contreras admitted to embezzling approximately $15,920,042 from the school district. (Source)

**Former College Coach Sentenced To Prison For Sextortion, Cyberstalking & Cyber Fraud Targeting 128 Women - March 6, 2024**

Steve Waithe is a former college track and field coach.

He was sentenced to prison in connection with a scheme to fraudulently obtain thousands of explicit photos from over 100 women across the country through the use of nearly two dozen sham social media and email accounts. Waithe cyberstalked one female student-athlete and orchestrated another scheme to gain unauthorized access to other victims' Snapchat accounts.

While a track coach at Northeastern University, Waithe requested the cell phones of female student-athletes under the pretense of "filming their form" at practices and meets and then covertly sending himself explicit photos of the victims that had previously been saved on their phones.

Approximately one year later in February 2020, and after he no longer worked at Northeastern University, Waithe began perpetrating an evolving series of schemes to deceive women into sending him nude or semi-nude photos of themselves.

In total, Waithe victimized at least 56 women and attempted to victimize 72 more. Waithe used anonymized social media accounts with usernames like "anon.4887" and variations of the phrase "Privacy Protector" to contact prospective victims, including some of the same student-athletes from the Northeastern University track and field team, claiming that he had "found" compromising photos of them online and offering to "help" get the photos removed from the internet.

Waithe also requested additional nude or semi-nude photos from victims that he could purportedly use for "reverse image searches." Notably, none of the Northeastern University student-athletes were tricked by this scheme, though Waithe continued to try it on new prospective victims.

Investigators identified 22 sham online accounts across at least seven different platforms used by Waithe and hundreds of photos sent by dozens of victims who thought they were emailing someone conducting a legitimate research study.

Waithe previously worked as a track and field coach at several academic institutions, including Northeastern University, Penn State University, Illinois Institute of Technology, University of Tennessee and Concordia University Chicago. (Source)

**School Bus Driver Charged For Setting Bus On Fire That Was Full of Children - March 2, 2024**

Michael Ford is a former Granite School District Bus Driver in Utah. He was ordered detained March 1, 2024, by a judge after he was accused of setting the school bus on fire on two occasions.

In February 2022, Michael Ford allegedly set a Granite School District school bus on fire that had 42 children inside and did so while driving in traffic. Ford used an ignition device to start a fire on the bus and was captured on video continuing to drive the bus, despite smoke billowing past his face towards the back of the bus where children were seated.

In April 2023, Ford was again driving a Granite School District bus in traffic, when he was captured on video igniting a fire on the bus. Again, Ford continued to drive the bus with smoke billowing past his face. Days later, in April 2023, Ford was arrested by Granite School Police and questioned about the fire but was released. (Source)

**CHURCHES / RELIGIOUS INSTITUTIONS**

**Church Administrator Convicted For Embezzling $360,000+ From Church / Used Funds For Hair Salon, Retail Shopping, VIP Concert Tickets - March 5, 2024**

From 2013 to 2018, Chanell Easton worked as the church administrator at a church in Yuba City, California.

During her employment, Easton stole over $360,000 from the church, including from its food pantry and youth ministry, during a years-long embezzlement scheme.

Easton used credit cards associated with the church to make personal purchases — at a hair salon, retail stores, online retailers, a vacation rental service, and to buy VIP concert tickets — and then paid off the resulting balance with the church's money.

One of the credit cards Easton used during her scheme belonged to the church's youth minister, and Easton used his identity to make thousands of dollars in unauthorized personal purchases on Zappos.com.

Easton's use of the youth minister's identity allowed her to obscure her embezzlement and to shift suspicion away from herself, thereby allowing her fraudulent scheme to continue.

Easton also transferred money directly from the church's bank accounts to her own personal account, paid down the balance of her own personal credit card, and paid her cellphone provider for her personal bills and for new phones. Easton also stole money from the church by writing checks to others for personal expenses and by writing checks to herself, on which she forged the signatures of the church's treasurer or the head volunteer of the church's food pantry. (Source)

## LABOR UNIONS

**No Incidents To Report**

## BANKING / FINANCIAL INSTITUTIONS

**Bank Director Sentenced To In Prison For $1.4 Million Of Bank Fraud Causing Bank To Collapse - March 19, 2024**

In or about 2009, Mendel Zilberberg (Bank Director) conspired with Aron Fried and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower (Straw Borrower) to make the loan application. The Straw Borrower applied for a $1.4 Million loan from the Bank on the basis of numerous lies directed by Zilberberg and his coconspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly. Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a $1.4 Million loan to the Straw Borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately $500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator. The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. In 2010, Park Avenue Bank was closed due to ineffective management and inadequate capital. (Source)

**Former Credit Union Employee Sentenced To Prison For Embezzling $136,000+ - March 22, 2024**

TracyThibodeau was sentenced to prison for defrauding her former employer, the Vermont VA Federal Credit Union (VVAFCU). The VVAFCU is a small credit union that has one office in White River Junction. Thibodeau began working at the credit union in 2015 and was promoted to branch manager some time in 2016. The credit union offered VVAFCU VISA credit cards to members and employees.

In April 2019, Thibodeau misused her authority at the bank to open a personal VVVAFCU credit card account without proper authorization from her superiors. Later in 2019, Thibodeau again misused her access to the credit union's credit card processing software to grant herself, without authorization, privileges on her card account.

Those privileges eliminated maximum account limits; excused her from paying late fees and penalties on overdue balances; and eliminated monthly minimum payments. Between April 2019 and February 2021, Thibodeau used her credit card to make purchases in excess of $140,000.

During that period, Thibodeau made only small monthly payments toward her large account balance. Thibodeau concealed her procurement and misuse of the credit card by manipulating internal credit card journal reports to hide from her superiors the existence of a large balance on her account. The credit union discovered the fraud in April 2022 and promptly fired Thibodeau. At that time, the outstanding balance on her account was about $137,000. That loss has been absorbed by the credit union and its insurer.

Thibodeau was orderd to pay $136,936.57 in restitution. (Source)

## TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

**Facebook / Meta Sues Former Executive Over Alleged Theft Of Proprietary Information That He Took To New Employer - March 2, 2024**

Meta is suing its former vice president of infrastructure over allegations that he stole proprietary human resources data about the company's top performers, and key information about its data center supply chain partners to bring to his new employer.

In a complaint filed in late February in a California State Court, the software giant alleged that Dipinder Singh Khurana breached contractual agreements, loyalty, and fiduciary duties by taking proprietary, information related to Meta's data centers, supply chain, as well as employee compensation to a Stealth AI startup where he holds a similar position to what he held at Meta.

Meta has alleged that during his last days as an employee, Khurana leaned on subordinates to give him confidential agreements with suppliers for its data centers.

Unaware of Khurana's plans, the employee provided Khurana with, among other things, Meta's pricing-form agreement with that supplier for the computing hardware and the supplier's Meta-specific preliminary pricing for a particular chip, the complaint read.

Taken together, the sensitive, confidential, and non-public information in these spreadsheets provides an inside view as to how Meta makes compensation decisions, and also provides key information regarding not just the names of Meta employees but their levels, performance, and skills at Meta," the complaint read. (Source)

**Johnson & Johnson Accuses Former Employee Of Taking Thousands Of Files To New Role At Pfizer Just Before Resignation - March 21, 2024**

Johnson & Johnson (J&J) has sued its former employee Andrew Brackbill, claiming he clandestinely and maliciously downloaded more than a thousand sensitive strategy-related files onto external hard drives three weeks prior to his resignation. To make matters worse, Brackbill then accessed the J&J information while on the clock in his new position at Pfizer, J&J alleged.

In addition to the company files, Brackbill transferred personal photos and documents in what J&J claims was an attempt to hide the theft. A company security program flagged the large file transfer, leading to an investigation that included an interview and a forensic examination.

Brackbill's most recent title during his 24-year career at J&J was Director of Trade Channel Strategy, a role which gave him access to extremely confidential information necessary to make important strategic decisions.

The position is within J&J's Strategic Customer Group (SCG) department, which is effectively responsible for creating and developing competitive strategies for the company's medicines. Brackbill had access to confidential sales data, customer and channel lists, pricing models, market research, contracting strategies, launch playbooks and other strategy plans.

Brackbill resigned from J&J in July of last year and finished his last day in August. His new role at Pfizer is as Director of Contract Strategy, U.S. market access, a position that J&J says is a directly competitive one.

Pfizer itself sued a "soon-to-be former employee in 2021, accusing the staffer of uploading more than 12,000 files to a personal Google Drive account, some of which could contain confidential information about the company's COVID-19 vaccine.

Recently, Pfizer took two ex-employees to court claiming they stole "the hard work of Pfizer scientists when setting up a new company. (Source)

**Basketball Sports Team Coaching Analyst Employee Charged For Stealing Thousand Of Files From Team Executive - March 20, 2024**

Somak Sarkar previously served as a coaching analyst for the Minnesota Timberwolves.

Sachin Gupta, a Timberwolves executive vice president who oversees the team's analytics department, left a hard drive connected to a laptop in his office at the Target Center in downtown Minneapolis.

That drive contained Gupta's personal financial information as well as private information for the team, including employment and player contracts.

When Gupta returned to work on Feb. 5, the hard drive was missing, and subsequent surveillance reviewed by security revealed that Sarkar had twice entered Gupta's office on Feb. 3 after looking to see if anyone could see him. He then left. Sarkar was fired immediately.

Another employee was able to recover the hard drive from Sarkar, and the team determined, after a forensic analysis, that he had accessed more than 5,000 files and downloaded them onto another device. (Source)

**CHINESE ESPIONAGE / THEFT OF TRADE SECRETS INVLOVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES**

**Owners Of China Based Company Charged With Conspiracy To Distribute $13 Million Of U.S. Trade Secrets Stolen By Former Employees - March 21, 2024**

Klaus Pflugbeil a resident of the People's Republic of China, and Canadian nationalYilong Shao, a Chinese national, were charged with conspiring to send trade secrets that belonged to a leading U.S.-based electric vehicle company.

Victim Company-1 is a U.S.-based leading manufacturer of battery-powered electric vehicles and battery energy systems. In 2019, Victim Company-1 acquired a Canada-based manufacturer of automated, precision dispensing pumps and battery assembly lines. Prior to its purchase by Victim Company-1, the Canadian Manufacturer sold battery assembly lines to customers who manufactured alkaline and lithium-ion batteries for consumer use. The battery assembly lines contained or utilized a proprietary technology now owned by Victim Company-1: continuous motion battery assembly. The proprietary technology provided a substantial competitive advantage to Victim Company-1 in the battery manufacturing process. Victim Company-1 spent at least $13 million developing the Battery Assembly Trade Secret.

Both Pflugbeil and Shao are former employees of the Canadian Manufacturer. The evidence reveals that, by no later than 2019, Pflugbeil and Shao planned to make use of Victim Company-1 trade secrets for their own business activities.

For example, between October and November 2019, Pflugbeil and Shao discussed setting up a company in Canada and China that would rely on the sensitive and confidential information needed to make and sell their own battery technology. Pflugbeil told Shao that he had a lot of original documents related to the technology, and sought out more original drawings from Victim Company-1 that they could copy for their planned business. Shao subsequently confirmed that "we have all of original assembly drawings by PDF."

In or about July 2020, Pflugbeil and Shao opened Business-1, which has since expanded to locations in China, Canada, Germany and Brazil. Business-1 makes the same precision dispensing pumps and battery assembly lines that Victim Company-1 manufactured using its proprietary technology. Business-1 is marketed by Pflugbeil as an alternative source for the sale of products that rely upon Victim Company-1 trade secrets, publishing online advertisements that state, for example, "Are you looking for Victim Company-1 Metering pumps and spare parts? Look no further." (Source)

**Google Engineer Arrested For Theft Of AI Trade Secrets While Secretly Working For 2 Chinese Companies - March 6, 2024**

Leon Ding, a national of the People's Republic of China and resident of Newark, California, transferred sensitive Google trade secrets and other confidential information from Google's network to his personal account while secretly affiliating himself with PRC-based companies in the AI industry.

Ding stole involves the building blocks of Google's advanced supercomputing data centers, which are designed to support machine learning workloads used to train and host large AI models.

Google hired Ding as a software engineer in 2019.

On May 21, 2022, Ding began secretly uploading trade secrets that were stored in Google's network by copying the information into a personal Google Cloud account. Ding continued periodic uploads until May 2, 2023, by which time Ding allegedly uploaded more than 500 unique files containing confidential information.

Ding secretly affiliated himself with two PRC-based technology companies.

On or about June 13, 2022, Ding received several emails from the CEO of an early-stage technology company based in the PRC indicating Ding had been offered the position of Chief Technology Officer for the company. Ding allegedly traveled to the PRC on Oct. 29, 2022, and remained there until March 25, 2023, during which time he participated in investor meetings to raise capital for the new company.

The indictment alleges potential investors were told Ding was the new company's Chief Technology Officer and that Ding owned 20% of the company's stock.

Unbeknownst to Google, by no later than May 30, 2023, Ding had founded his own technology company in the AI and machine learning industry and was acting as the company's CEO. (Source)

**PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES**

**Orthodontist Who Sold His Business, But Remained An Employee Charged With Embezzling $73,000 - March 5, 2024**

Dr. Kassman was the former owner of a Tucson orthodontics practice. After selling the practice, Dr. Kassman and his wife continued as employees for the new owner.

Dr. Kassman worked as an orthodontist, and Dr. Kassman's wife continued as the office manager. The indictment alleges that, after the sale, Dr. Kassman kept his business bank account open. The Kassmans then engaged in an embezzlement scheme in which they diverted funds that belonged to the practice without the new owner's knowledge or consent. To conceal the scheme, Laurie Kassman manipulated financial records in the practice's record keeping system. The Kassmans embezzled at least $73,000. (Source)

**Receptionist At Medical Care Facility Sentenced To Prison For Stealing $52,000 - February 14, 2024**

Del Busso was a receptionist at Integrated Specialist Medical Care in 2019m when bosses discovered she had pocketed $52,000.

Busso took over banking responsibilities for the company's two practices, in Kogarah and Randwick, when the manager was on holiday from late December 2019 until the beginning of February 2020.

Upon return, the manager realised the finances did not add up and ordered a full audit, revealing $35,785 was missing from the Kogarah accounts and $16,565 from Randwick.

It is not the first time Del Busso's actions have made for a controversial spotlight. She rose to fame during her high-profile relationship with former NRL player Josh Reynolds, during which she faked three miscarriages, and also appeared on reality show SAS Australia in 2020. (Source)

**EMBEZZLEMENT / FINANCIAL THEFT / FRAUD / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING / INSIDER TRADING / STOCK TRADING FRAUD**

**Senior Executives Of International Cargo Airline Plead Guilty To Role In Defrauding Their Employer & Receiving $23 Million In Kickbacks Over 12 Years - February 29, 2024**

From at least in or about 2009 through in or about July 2021, Lars Winkelbauer and Abilash Kurien, and at least 8 other individuals participated in a massive scheme to defraud Polar. Air Cargo. At all relevant times, Winkelbauer and Kurien, and two co-defendants who were senior executives of Polar, and six co-defendants (Vendor Defendants) owned and operated various Polar vendors and customers.

Winkelbauer was Polar's Chief Operating Officer and Executive Vice President and is the most senior of the Executive Defendants. Kurien was the Vice President of Marketing, Revenue Management, and Network Planning.

The Executive Defendants agreed to accept millions of dollars in kickbacks from the Vendor Defendants and also reaped substantial financial benefits as a result of their secret ownership interests in certain Polar vendors, in exchange for ensuring that those vendors received favorable business arrangements with Polar.

The fraud they perpetrated involved a substantial portion of Polar's senior management and at least 10 customers and vendors of Polar, and led to pervasive corruption of Polar's business, touching nearly every aspect of the company's operations for over a decade.

As a result of the scheme, the Executive Defendants, along with two co-conspirators who also worked as senior executives at Polar, received unlawful payments, either directly or through various limited liability companies they controlled, in excess of approximately $23 million in kickback payments or disbursements as a result of their ownership of conflicted companies. (Source)

**Former Employee Sentenced To Prison For Stealing $3.4 Million+ Over 5 Years - March 15, 2024**

James Dwyer was employed by Mobile Money, Inc. for over 20 years. Part of Mobile Money, Inc.'s business operations were servicing ATMs across eastern Iowa. Starting in January 2016, Dwyer defrauded and stole from Mobile Money, Inc. by stealing cash that was meant for ATMs or cash that was supposed to be deposited into a Mobile Money, Inc. bank account.

In January 2021, Dwyer told his superiors, which included someone Dwyer had been friends with for over 30 years, that there was approximately $1.1 million in cash locked in a vault in Waterloo that he could not access because the vault lock was broken. It was later discovered that Dwyer had intentionally tampered with the vault in order to prevent anyone else from accessing it. In February 2021, other employees got into the vault and discovered there was less than $100,000 in cash in it.

Also in January 2021, Mobile Money, Inc. executives discovered Dwyer had failed to deposit approximately $2.5 million in cash into bank accounts. On February 1, 2021, Dwyer sent ten bank deposit tickets to Mobile Money, Inc., purporting to show he had deposited that money. However, the bank deposit tickets were fraudulent and he had not deposited any such money.

Once Mobile Money, Inc. discovered Dwyer had been stealing from the company, the company determined his fraud had resulted in the company losing $3,407,000. (Source)

**Company Financial Controller Sentenced To Prison For Embezzling $2.37 Million Over 6 Years - March 27, 2024**

From 2014 through December 2020, Gerard Beauzile abused his position as a Financial Controller of a New York-based company, to embezzle funds by issuing fraudulent company checks to himself and then depositing those checks into his bank account for his own personal benefit. Beauzile issued approximately 140 company checks to himself with a total value of $2.37 million. Beauzile concealed the theft from the company by falsely entering the fraudulent checks into the company's accounting system under various company vendor names as the payees, causing the accounting system to falsely reflect that the checks were made payable to company vendors instead of to Beauzile. He also falsified vendor invoices to correspond to the entries made in the accounting system, and company bank statements by removing and altering opening, running, and closing balances, check payment entries, summary check listings, and inter-account transfers. (Source)

**Former Law Firm Office Manager Sentenced To Prison For Embezzling $1.1 Million+ From Law Firm For 7 Years - March 13, 2024**

Jairo Santos admitted he embezzled more than $1.1 million from a San Francisco-based law firm where he had been employed as the office manager.

Santos began his embezzlement scheme no later than March 2016 and continued it through February 2023. As part of the scheme, Santos obtained checks from the victim law firm, filled out the payee line of those checks, addressing them to Jairo Santos, and signed each check with the signature of the law firm's senior partner even though Santos was not authorized to do so.

Santos then deposited these checks into his personal checking accounts at Wells Fargo Bank. Santos admitted he deposited approximately 806 fraudulent and unauthorized checks from the victim law firm made payable to Santos into his personal checking accounts. The total value of these unauthorized deposits was approximately $1,191,683. (Source)

**Former Accounting Director Sentenced To Prison For Embezzling $930,000 Million+ - March 1, 2024**

Jenev Boyd was sentenced to prison for embezzling from her employer, which managed the financial affairs for homeowner associations.

Boyd was a long-time employee of and the Director Of Accounting for Encore Property Management, a company that provided property management services to its homeowner association clients.

From January 2012 to August 2020, Boyd reactivated retired or non-active client accounts in a software program Encore used to falsely reflect that these were still active clients. She then changed the selected vendor's information to reflect her own name and address.

Through manipulation of Encore's internal accounting software, Boyd was able to mask payments to herself from client accounts as vendor payments. Boyd kept the monthly amounts in line with other vendor payments therefore hiding the embezzlement.

Boyd also forged signatures, including that of Encore's president, on each check she fraudulently issued to herself. She also misled the company's clients about the checks she wrote to herself out of their accounts, including by describing the transactions as being for operating expenses rather than as a payment to her based on a bogus invoice. In total, Boyd defrauded her employer and its clients out of $931,077. (Source)

**Financial Services Manager At Education Institution Found Guilty For Role In Embezzling $835,000+ - March 4, 2024**

Andrea Mitchell served as a financial services manager at a higher education institution in the Middle District of Florida.

Mitchell, Lester Best, and their coconspirators used her position to embezzle hundreds of thousands of dollars from the institution. Mitchell stole the identities of current and former students at the higher education institution and then used their student identification numbers to access their student sponsorship accounts.

Mitchell identified refunds in these accounts made by the higher education institution to a tuition management business and/or a college savings program on behalf of the students and, thereby, located entries reflecting illusory balances in the students' sponsorship accounts. Mitchell used the illusory balances to create the appearance of funds to back fraudulent checks.

She then caused the higher education institution to issue the checks in the names of multiple coconspirators who had been recruited by Best to negotiate the bogus checks. None of these coconspirators were students at the higher education institution. The coconspirators cashed or deposited the fraudulent checks at various financial institutions and then shared the proceeds. As a result, the higher education institution lost more than $835,000. (Source)

**Former Chairman Of New York Housing Authority Sentenced To Prison For Role In $800,000+ Contract Fraud & For Accepting $100,000+ In Kickbacks - March 11, 2024**

The former Chairman of the Board of Commissioners (Board) at the Village of Hempstead Housing Authority (VHHA) In New York, was sentenced to 10 years in prison for conspiracy to commit honest services fraud and three counts of federal program bribery.

Cornell Bozier used his official position to orchestrate a bid-rigging and kickback scheme, by filling numerous positions in the Housing Authority with either co-conspirators who were actively participating in the scheme, or people he believed could be manipulated and would not interfere.

Bozier relied on bribes, threats and intimidation to pressure other Board members into supporting his fraudulent schemes. Bozier also fraudulently induced the Board to declare numerous projects as emergencies to sidestep the normal procedure process by which the VHHA obtained HUD funding. Bozier and his co-conspirators submitted grossly inflated bids to the Board for repair projects at properties throughout the VHHA and Bozier used his control over the Board to secure the acceptance of those bids.

The work related to those projects was then subcontracted out at a fraction of the amount paid by the VHHA for nominal and, in many cases, substandard repairs and work.

Bozier demanded and received numerous cash payments from his co-conspirators, who prepared and submitted the fraudulent bids as kickbacks for his role in the scheme, which totaled more than $100,000.

Bozier steered more than $800,000 of VHHA funds to co-conspirator companies as part of his fraudulent scheme and received more than $100,000 in kickback payments. (Source)

**Former Employee Charged For Embezzling $116,000+ From Employer - March 20, 2024**

Angela Mitchell is alleged to have diverted to herself approximately $116,998.70 from Company A by, among other things, fraudulently transferring funds from Company A's bank accounts via electronic transfers and by drafting unauthorized checks to herself. Mitchell committed the fraud during her employment, and continued illegally accessing Company A's accounts after she was terminated in June 2018. (Source)

**Former Telecommunications Company Manager Admits Role In Taking Kickbacks In Cell Phone SIM Swapping Scheme - March 13, 2024**

In May 2021, Jonathan Katz was employed as a manager at a telecommunications store and accessed several customer accounts by using managerial credentials. Katz swapped the SIM numbers associated with the customers' phone numbers into mobile devices controlled by another individual, enabling this other individual to control the customers' phones and access the customers' electronic accounts – including email, social media, and cryptocurrency accounts. In exchange for the swaps, Katz was paid in Bitcoin, which was traced back to Katz's cryptocurrency account. (Source)

**EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS**

**Chief Marketing Officer For Insurance Company Sentenced To Prison For Embezzling $10 Million+ / Used Funds To Purchase Yacht, Plane & Mercedes-Benz - March 20, 2024**

Brinson Silver is the former Chief Marketing Officer of Root Insurance.

Silver entered into multiple contracts with marketing vendors and instructed them to divert portions of their contract proceeds to the bank accounts of companies that Silver controlled. From November 2021 to November 2022, Silver embezzled $10.2 million from Root, using his companies Collateral Damage, LLC, Eclipse Home Design, LLC, and Grind 24.

Silver used the embezzled funds for a variety of personal purchases, including a $1.4 million yacht, a Mercedes-Benz and an amphibious plane. In February 2023, Root sued Silver for the embezzlement.

Court filings indicate that after he was sued, Silver disobeyed court orders by failing to appear in court and routinely making purchases larger than $5,000. He spent lavishly while traveling internationally, including by spending $20,000 on plastic surgery and $8,000 on a resort in Bali. He sent an additional $92,000 through PayPal.

Before he was sued, Silver paid $75,000 to a consulting firm specializing in international relocation, global citizenship and offshore tax planning. In recorded phone calls, Silver asked about gaining citizenship to a country that would not extradite him to the U.S. He also wanted to move up to $10 million to a foreign bank account that the U.S. could not freeze. (Source)

**Former Employee For On-line Used Car Retailer Pleads Guilty For $2 Million+ Embezzlement Scheme / Used Funds For Lavish Lifestyle (Cars, Travel, Etc.) - March 22, 2024**

John Whisenant worked in a variety of roles at an online used car sales company beginning in October 2018. About a year after he began with the company, Whisenant was promoted into a role where he had access to the company bank accounts and accounting software.

Beginning in about June 2019 and continuing until November 2021, Whisenant used his access to make 57 wire transfers totaling over $2 Million into accounts he controlled.

Whisenant disguised the transfers as legitimate business expenses in the company's accounting software with a variety of false entries. Whisenant defrauded the company of $2,084,799. Whisenant then transferred the money to others and mixed it with other funds making it difficult to trace.

Whisenant used the money for a lavish lifestyle. He bought luxury automobiles such Porches and Mercedes. He spent $123,096 for a 2022 Audi E-Tron and bought a $98,100 Tesla. He rented luxury homes in Southern California and purchased two airline tickets to Paris at a cost of nearly $23,000 each. (Source)

The fraud on the company accounts was discovered when a bookkeeper began a more comprehensive review of the company's financials in January 2022. Whisenant resigned abruptly in February 2022. (Source)

**Employee Sentenced To Prison For Embezzling $462,000+ By Creating Fake Employees And Having Salaries Deposited Into Her Personal Bank Account - March 19. 2024**

Julia Linck was sentenced to prison for embezzling almost a half of a million dollars from her former employer by creating false employees and having salaries for the fake persons deposited into her personal bank accounts.

Linck stole the funds from October 2014 through July 2020 from Memphis Barbecue Company in DeSoto County. Linck was also ordered to pay back the stolen funds, with the court ordering her to pay $462,874.05 in restitution. (Source)

**Executive Director For Non-Profit Foundation Sentenced To Prison For Embezzling $428,000+ / Used Funds To Pay Off Credit Cards - March 21, 2024**

On February 28, 2023, Melodie Haile entered a plea of guilty to bank fraud. According to investigators, from 2017 until mid-2021, while employed as Executive Director of The MORE Foundation, a nonprofit that funds continuing education scholarships for high school graduates, Haile embezzled over $428,271.26 from the foundation's bank accounts for personal use. During that time, Haile embezzled funds through multiple different means, including bank transfers to pay off her personal credit card, ATM withdrawals, and the issuance of fraudulent payroll checks to herself. (Source)

**Financial Controller Sentenced To Prison For Embezzling $413,000+ From Company / Used Funds For Spa Treatments, Jewelry, Clothes, Etc. - March 18, 2024**

Around November 29, 2017, Bethany Olmsted was hired as controller for a company A, a private business, and five other investment companies partially owned by company A's owner. As these companies' controller, Olmsted managed the bookkeeping, tax reporting, accounts payable, accounts receivable, and day-to-day finances for each business. Olmsted's duties included tracking and categorizing all the companies' receipts and spending using accounting software. She also had the authority to write company checks to pay legitimate business expenses.

Starting on November 29, 2018, Olmsted began writing checks from the investment companies' bank accounts to herself and depositing them into her personal bank account. To conceal her thefts, Olmsted falsely categorized these payments to herself as payments to legitimate businesses or vendors such as for Mowing & Landscaping.

Similarly, she categorized checks written to herself as payments to "Fortune Companies Inc." for Repairs & Maintenance. In addition, she transferred money from company A's bank account to the other companies' bank accounts to hide the thefts.

When confronted by company officials about the theft of company funds, Olmsted repeatedly lied about the extent of the thefts and her efforts to avoid detection by altering the companies' books.

Between November 2018 and September 2021, Olmsted fraudulently wrote approximately 520 checks from the companies to herself, stealing $413,531. Olmsted used the stolen funds to purchase spa treatments, jewelry, clothes, and dinners at high-end steakhouses. (Source)

**Company Account Associate Employee Sentenced To Prison For Embezzling $397,000+ / Used Funds For Gambling, Family / Friends, Jewelry, Travel, Car Payments - March 28, 2024**

Trixie Dela Cruz was employed by a company that administers employee benefits for employers nationwide. Within six months of her hiring and immediately after she had been promoted, Dela Cruz began her embezzlement scheme.

Dela Cruz was hired by the company in October 2020, and in March 2021 was promoted to Account Associate. In that role, she managed client accounts and approved claims for benefits. Using her access, she created a duplicate account for a deceased employee of one of the clients. She connected the profile to her own bank account and then submitted and approved 58 fraudulent claims totaling $397,942. Dela Cruz would activate the profile for the fraudulent claim and then deactivate it so no record would show up for her company.

In January 2022, the company discovered the fraud and dismissed Dela Cruz. The company reimbursed the client for the fraudulent claims. Forensic analysis indicated Dela Cruz spent the money on gambling, cash application transfers to family and friends, and to pay for jewelry, travel, car payments and other shopping. (Source)

**Substance Abuse Treatment Center Employee Sentenced To Prison For Embezzling $45,000+ / Used Funds To Pay Car Loan Payments, Utility Bills, Etc. - March 4, 2024**

Matthew Huffman admitted to stealing from the Southern Highlands Community Mental Health Center in West Virginian, while employed as its Chief Substance Use Disorder Officer.

Between October 2022 and January 2023, Huffman embezzled money from Southern Highlands including more than $5,000 it received from the Comprehensive Opioid, Stimulant, and Substance Use Program (COSSUP).

Southern Highlands is a non-profit medical treatment center that offers a variety of services including addiction treatment. COSSUP grants are distributed, in part, to treat and support those impacted by illicit substance use and misuse.

Huffman admitted that he forged signatures required to approve the use of COSSUP grants and other funds, and also used the names of patients and consumers no longer receiving services from Southern Highlands on the necessary forms. Huffman further admitted that he embezzled these funds for his personal gain, using the money to pay his utility bills, vehicle loan payments and to purchase gift cards and prepaid debit cards.

Huffman was sentenced today to three years of federal probation, including 90 days on home detention with location monitoring, and ordered to pay $45,258.51 in restitution for theft or embezzlement in connection to healthcare services. (Source)

**SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES**

**Former Football Team Employee Sentenced To Prison For Embezzling $22 Million+ / Used Funds For Gambling, Purchase Condo, Tesla, Etc. - March, 12, 2024**

Amit Patel worked for the Jacksonville Jaguars Football Team.

Patel operated a fraud scheme through which he embezzled approximately $22,221,454 from his employer from September 2019, and continued until he was fired by his employer in February 2023.

Patel used his role as the administrator for company's virtual credit card (VCC) program to make hundreds of purchases and transactions with no legitimate business purpose.

Then, to hide and continue to operate the scheme, rather than accurately report his VCC transactions, Patel created accounting files that contained numerous false and fraudulent entries and emailed them to the accounting department.

Patel used a variety of methods to hide his illicit transactions by omitting them from the files, while still having the total dollar amount of VCC expenditures match the balances paid by the VCC program line of credit.

Patel identified legitimate reoccurring VCC transactions, such as catering, airfare, and hotel charges, and then duplicated those transactions; he inflated the amounts of legitimate reoccurring VCC transactions; he entered completely fictitious transactions that might sound plausible, but that never actually occurred; and he moved legitimate VCC charges from upcoming months into the month of the accounting file that was immediately due to the accounting department.

Patel used the proceeds of this scheme, in whole or part, to place bets with online gambling websites, to purchase a condominium in Ponte Vedra Beach, Florida, to pay for personal travel for himself and friends (including chartering private jets and booking luxury hotels and private rental residences), to acquire a new Tesla Model 3 sedan and Nissan pickup truck, to pay a criminal defense law firm, and to purchase cryptocurrency, non-fungible tokens, electronics, sports memorabilia, a country club membership, spa treatments, concert and sporting event tickets, home furnishings, and luxury wrist watches. (Source)

**Former Auditor For Commercial Real Estate Agency Sentenced To Prison For Embezzling $2.7 Million+ Using Fake Invoice Scheme - March 7, 2024**

From 2008 to January 2022, Varun Aggarwal worked in the internal auditing department of the Newport Beach-based KBS Realty Advisors and rose to the level of the department's director. Beginning at least as early as January 2012 and continuing until January 2022, Aggarwal used his position at KBS to embezzle his employer's money.

As a member of the company's internal auditing group, Aggarwal was familiar with KBS's policies and procedures for payments to vendors. Aggarwal used his knowledge of KBS's policies and procedures to have his friends and family serve as approved vendors to do contracting work for KBS.

After several of these companies became approved vendors for KBS, Aggarwal used these approved vendors to submit fraudulent invoices for consulting services that were not performed for the company or were submitted for work at inflated prices. He then funneled the payments on the invoices from KBS to his own bank accounts – through the approved vendors – at times without informing the vendors that the invoices and the payments on the invoices were for his own benefit.

In carrying out this scheme, Aggarwal fraudulently obtained approximately $2.7 Million. (Source)

**Company Bookkeeper Sentenced To Prison For Embezzling $180,000+ Using Inflated Invoice Scheme - March 14, 2024**

Christina Iannelli was an independent contractor for an interior design firm based in Lexington, Massachusetts.

Beginning in or about October 2018, Iannelli prepared dozens of fraudulent invoices with inflated totals derived from inaccurate math, and then issued herself checks for the inflated amounts due from the firm's checking account. Additionally, beginning in or about July 2019, Iannelli issued herself dozens of additional unauthorized checks. In both instances, Iannelli used a signature stamp in the name of the firm's owner to issue the fraudulent checks.

To conceal the fraudulent payments, Iannelli made false entries in the firm's accounting records.

In total, Iannelli embezzled more than $30,000 through inflated compensation checks and more than $150,000 through additional unauthorized checks. (Source)

**Former Non-Profit Vice President Sentenced To Prison For Role In $246,000 Fake Invoice Scheme / Used Funds For Clothing, Massages, Travel, Etc. - March 6. 2024**

Teela Gilber served as the Vice President, Academic Affairs Advisor and Office Manager of Hope 4 Change, a nonprofit organization that provided housing and care for adults with developmental disabilities, drug addiction problems and mental disorders.

She also managed the operations of Black Wall Street Cooperative, a corporation registered with the State of Ohio that purported to create employment and business opportunities for low-income individuals.

Gilbert and co-defendant Barry Rene Isaacs, the founder, owner, CEO and president of Hope 4 Change and founder of Black Wall Street Cooperative, induced payments for false invoices to a company.

Gilbert submitted more than 30 fraudulent invoices totaling approximately $246,000 for services not actually performed by Black Wall Street Cooperative. Her fraudulent invoices named individuals who did not work for the corporation, including the identity of one woman who had died in 2019.

Hope 4 Change withheld FICA taxes from its 120 to 180 employees' paychecks, but did not pay over the employment taxes to the IRS for five quarters in late 2013 and 2014. Isaacs also fraudulently applied for an auto loan and credit card using someone else's social security account number.

Isaacs caused Hope 4 Change to spend thousands of dollars for clothing, massages, beauty care, travel and personal vehicles for Isaacs and Gilbert and their family. He was sentenced in November 2021 to 48 months in prison. (Source)

## NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE / UN-AUTHORIZED ACCESS TO COMPUTER SYSTEMS & NETWORKS

**No Incidents To Report**

## THEFT OF ORGANIZATIONS ASSESTS

**Former Employee Admits Stealing Hundreds Of Company Laptops & Putting On eBay For Sale - February 29, 2024**

Police say an employee admitted to stealing hundreds and possibly thousands of a company's out-of-service laptops while working for the company, and put them up for sale online.

The employe worked for Cargill for more than 30 years at various locations, lastly as a dock supervisor until he was fired.

An online check found laptops of various brands listed under the man's eBay account, at prices as high as $280.

An external party alerted Cargill that an Apple laptop purchased on eBay was locked by the company and rendered inaccessible, and was directed to the seller's eBay account and address in Shakopee. Cargill traced the address to one of its employees.

Police checked the man's eBay account and found more than 3,000 prior listings and sales. Photos and descriptions confirmed to police that the listings included laptops from Cargill.

The affidavit explained that Cargill stores laptops it is no longer using at the dock. A recycling company picks them up and sells them for a profit. Cargill also gets a large portion of the sales.

Cargill investigators interviewed the employee and he admitted taking 'hundreds' of laptops and selling them on eBay. (Source)

**Luxury Jewelry Company Supervisor Arrested For Stealing & Selling Millions Of Dollars Worth Of Precious Metals - March 15, 2024**

Since 2018, Benjamin Preacher worked fulltime in a supervisory position at a Rhode Island manufacturing facility operated by the company, which manufactures and sells luxury items, including jewelry made from gold, silver and platinum. It is alleged that Preacher used his position to steal precious metals from the company's facility in Rhode Island and then sell the metals to various businesses in Massachusetts.

From in or about March 2020 to March 2023, Preacher allegedly sold precious metals to a Canton-based metals dealer roughly one to two times per month, with sales to that dealer alone totaling more than $1 million. It is alleged that Preacher's sales of stolen metals included $50,521 in 18-carat gold in March 2020, $21,821 in 18-carat gold, platinum scrap and "sterling" in April 2021 and $30,939 in platinum in January 2022.

It is further alleged that Preacher also sold more than $177,000 in stolen precious metals to a separate metals deales between on or about May 16, 2023 and Nov. 16, 2023. This included gold sheets used by Preacher's employer in a particular machine, which Preacher allegedly stole and sold, along with other gold scrap, for nearly $21,000.

Most recently, it is alleged that, approximately 30 minutes into his shift on March 1, 2024, Preacher was captured on company security cameras stealing a piece of white gold "flat stock," measuring approximately an inch in diameter and approximately as thick as a quarter, valued at roughly $2,200.

Precious metal in scrap form were located and seized during a search of Preacher's home on March 14, 2024. (Source)

**EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)**

**No Incidents To Report**

**EMPLOYEE DRUG RELATED INCIDENTS**

**Employee Pleads Guilty To Selling His Co-Worker Fentanyl Pills That Resulted In The Co-Worker's Death - March 7, 2024**

On May 17, 2022, Tanner Goforth met his friend and co-worker, the victim, at a local gas station where Goforth sold the victim 10 fentanyl pills. The victim went home, ingested the fentanyl intravenously, and died almost immediately. Nearly a half hour later, his girlfriend found him in their bathroom, called 911, and began performing CPR. Police department officers arrived on scene and attempted life-saving measures. Unfortunately, the victim was unable to be resuscitated. (Source)

## OTHER FORMS OF INSIDER THREATS

**No Incidents To Report**

## MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

**No Incidents To Report**

## EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

**Individual Charged In Convincing Casino Employee To Take $700,000 From From Casino For Fraudulent Scam - March 7, 2024**

Jesus Gaytan-Garcia has been charged in a criminal complaint with theft from the Hartford, Michigan Four Winds Casino, which is owned and operated by the Pokagon Band of Potawatomi Indians.

The complaint alleges that on July 30, 2023, a call came into the Hartford Four Winds Casino. The caller falsely claimed that he was the tribal chairperson and needed funds to make an urgent payment.

A Casino supervisory employee, apparently duped by the caller's fraudulent claims, gathered up $700,000 in cash and walked out of the Casino. At the direction of the caller, the employee transported the cash to a gas station in Gary, Indiana, where the employee then handed the cash over two unknown individuals.

After a months-long investigation, the FBI and Pokagon Tribal Police were able to identify Jesus Gaytan-Garcia as one of the individuals the Casino employee met at the gas station and gave the $700,000.

Investigators conducted a search of Mr. Gaytan-Garcia's home, where they located a bundle of cash still wrapped in a paper band which was stamped with the word "Hartford," the location of the victimized Four Winds Casino, and the exact date of the theft, July 30, 2023. (Source)

## EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

**No Incidents To Report**

## WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

**Walgreens Employee Pursues And Shoots Alleged Shoplifter Who Was Pregnant 7 Times / Lawsuit Against Walgreens - March 27, 2024**

Travonsha Ferguson was 24 years old and 7 months pregnant in April 2023, when a Walgreens team leader who thought she was shoplifting followed her to her car and shot her several times.

In the civil lawsuit that the Tennessee mother filed against the pharmacy chain, she claims that she and a friend were followed from a Nashville drugstore by Mitarius Boyd, 21, an employee team leader who suspected them of shoplifting.

Lawyers for Ferguson claim that Walgreen Co. and an anonymous manager were negligent in failing to properly train and supervise Boyd. Boyd, however, is not named as a defendant in the lawsuit.

According to a statement by the Metropolitan Nashville Police following the incident, Boyd was notified by another employee that two women were stealing items from the store.

Boyd told detectives that he began to follow and record the women after he allegedly saw them place items into a cart and then into a bag, according to the statement.

Ferguson's attorneys are claiming that Boyd had never identified himself as a Walgreens employee before aggressively confronting Ferguson and her friend about alleged stolen items.

Once Ferguson and her friend got to their car, she sprayed Mace in Boyd's direction out of fear, that prompted Boyd to shoot Ferguson about seven times.

Boyd told detectives that he didn't know if the women were armed and that he, too, was in fear, according to a news release. Ferguson's friend drove away, and Boyd went back into the store to call

No criminal charges were filed against Boyd, who no longer works the store.

Ferguson's friend took her to a hospital, where Ferguson was initially listed in critical but stable condition. Ferguson's baby was delivered prematurely by C-section and had a heart defect. The infant fought for his life for weeks in the neonatal intensive care unit, according to the lawsuit. The baby is now reportedly at increased risk of long-term intellectual and developmental disabilities.

The attorneys also alleged that as a result of the shooting, Ferguson sustained permanent injuries that require her to wear colostomy bag to survive.

Ferguson's attorney's are asking the company to pay for damages based on her physical pain, mental anguish and emotional distress. Following someone to the parking lot and shooting them seven times for allegedly shoplifting is outrageous conduct that cannot be tolerated, her attorney says. (Source)

**Hospital Nurse Kills Patient By Replacing Pain Medication With Non-Sterile Tap Water / Family Suing For $11.5 Million - March 1, 2024**

The patient, Horace Wilson, was admitted to Asante Rogue Regional Medical Center in Medford Oregon, with a lacerated spleen and broken ribs, after he fell off a ladder in January 2022. As he recovered from multiple operations in the intensive care unit, Wilson's treatment team noticed unexplained high fevers, very high white blood cell counts, and a precipitous decline. He died in the hospital on Feb. 25, 2022.

The suit, filed on behalf of Wilson's estate and his wife, Patti Wilson, names both Asante Hospital and Dani Schofield, the nurse who allegedly swapped out the medication, accusing them of negligence. Schofield did not respond to multiple requests for comment. Records from the Oregon State Board of Nursing show that she voluntarily agreed in November to a nursing license suspension, pending "completion of an investigation."

The civil lawsuit seeks nearly $11.5 million and appears to be the first legal action taken since Medford, Oregon, police confirmed in January that they were investigating reports of drug theft at Asante Hospital.

As of March 2024, the police department said that it is actively investigating allegations of theft and misuse of controlled substances by an employee of Asante Hospital. Police did not identify who was being investigated and added that "no one has been charged with a crime as a result of this investigation."

"Since December 2023, investigators have been diligently working on this case," the statement said. "Numerous interviews have been conducted, with many more yet to be completed. We are meticulously reviewing thousands of documents, including medical records, which require thorough examination and consultation with experts in the medical field."

The wrongful death lawsuit alleges that Asante began notifying patients or their families in December that a nurse had replaced fentanyl with tap water, causing bacterial infections.

Wilson's family was not among those contacted, but once his relatives heard the reports of drug diversion, they suspected Wilson had also been a victim.

Horace Wilson was weaned from sedation and recovered enough mental function to communicate to the ICU staff that he no longer wished to live this way," the lawsuit says. (Source)

## EMPLOYEES' INVOLVED IN TERRORISM

**No Incidents To Report**

## PREVIOUS INSIDER THREAT INCIDENTS REPORTS

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

# DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

**TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH**

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

# ORGANIZATIONS IMPACTED

**TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS**

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports / Aviation (Pilots, Flight Attendants, Etc.)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others

# INSIDER THREAT DAMAGES / IMPACTS

**The Damages From An Insider Threat Incident Can Many:**

**Financial Loss**

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

**Operational Impact / Ability Of The Business To Execute Its Mission**

- ☐ IT / Network Sabotage, Data Destruction & Downtime
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead


**Reputation Impact**

- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

**Workplace Culture - Impact On Employees'**

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees'

**Legal & Liability Impacts (External Costs)**

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business


**DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)**

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

**MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST**

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

**IDEOLOGY**

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

**COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS**

- ☐ Bribery, Extortion, Blackmail

**COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS**

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

**OTHER**

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them


NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

**What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?**

**They Have Purchased:**
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

**They Have Used Company Funds / Credit Cards To Pay For:**
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Grow Marijuana, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

**They Have Issued Company Checks To:**
Themselves, Family Members, Friends, Boyfriends / Girlfriends

# ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

**Key Findings From Report / Infographic**
Fraud Scheme Types, How Fraud IS Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

**Behavioral Red Flags / Infographic**
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

**Profile Of Fraudsters / Infographic**
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERETHE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

**How Are Organization Responding To Employee Fraud / Infographic**
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

**Providing Fraud Awareness Training To The Workforce / Info Graphic**
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

# FRAUD RESOURCES

**ASSOCIATION OF CERTIFIED FRAUD EXAMINERS**

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

**DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES**

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

# SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

## EMPLOYEE EXTORTION

**Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / He Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - February 2, 2023**

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through April 1, 2021. Sharp was a Senior Developer who had administrative to credentials for company's Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from his technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

## DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

**Information Technology Professional Pleads Guilty To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022**

Casey Umetsu worked as an Information Technology Professional for a prominent Hawaii-based financial company between 2017 and 2019. In that role, Umetsu was responsible for administering the company's computer network and assisting other employees' with computer and technology problems.

Umetsu admitted that, shortly after severing all ties with the company, he accessed a website the company used to manage its internet domain. After using his former employer's credentials to access the company's configuration settings on that website, Umetsu made numerous changes, including purposefully misdirecting web and email traffic to computers unaffiliated with the company, thereby incapacitating the company's web presence and email. Umetsu then prolonged the outage for several days by taking a variety of steps to keep the company locked out of the website. Umetsu admitted he caused the damage as part of a scheme to convince the company it should hire him back at a higher salary. (Source)

**IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)**

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

**Former Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)**

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

**Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)**

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data.

The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

**Fired IT System Administrator Sabotages Railway Network - February 14, 2018**

Christopher Grupe was suspended for 12 days back in December 2015 for insubordination while working for the Canadian Pacific Railway (CPR). When he returned the CPR had already decided they no longer wanted to work with Grupe and fired him. Grupe argued and got them to agree to let him resign. Little did CPR know, Grupe had no intention of going quietly.

As an IT System Administrator, Grupe had in his possession a work laptop, remote access authentication token, and access badge. Before returning these, he decided to sabotage the railway's computer network. Logging into the system using his still-active credentials, Grupe removed admin-level access from other accounts, deleted important files from the network, and changed passwords so other employees' could no longer gain access. He also deleted any logs showing what he had done.

The laptop was then returned, Grupe left, and all hell broke loose. Other CPR employees' couldn't log into the computer network and the system quickly stopped working. The fix involved rebooting the network and performing the equivalent of a factory reset to regain access.

Grupe may have been smirking to himself knowing what was going on, but CPR's management decided to find out exactly what happened. They called in computer forensic experts who found the evidence needed to prosecute Grupe. Grupe was found guilty of carrying out the network sabotage and handed a 366 day prison term. (Source)

**Former IT Systems Administrator Sentenced To Prison For Hacking Computer Systems Of His Former Employer - Causing Company To Go Out Of Business (2010)**

Dariusz Prugar worked as a IT Systems Administrator for an Internet Service Provider (Pa Online) until June 2010. But after a series of personal issues, he was let go.

Prugar logged into PA Online's network, using his old username and password. With his network privileges he was able to install backdoors and retrieve code that he had been working on while employed at the ISP.

Prugar tried to cover his tracks, running a script that deleted logs, but this caused the ISP's systems to crash, impacting 500 businesses and over 5,000 residential customers of PA Online, causing them to lose access to the internet and their email accounts.

According to court documents, that could have had some pretty serious consequences: "Some of the customers were involved in the transportation of hazardous materials as well as the online distribution of pharmaceuticals."

Unaware that Prugar was responsible for the damage, PA Online contacted their former employee requesting his help. However, when Prugar requested the rights to software and scripts he had created while working at the firm in lieu of payment. Pa Online got suspicious and called in the FBI.

A third-party contractor was hired to fix the problem, but the damage to PA Online's reputation was done and the ISP lost multiple clients.

Prugar ultimately pleaded guilty to computer hacking and wire fraud charges, and received a two year prison sentence alongside a $26,000 fine.

**And PA Online? Well, they went out of business in October 2015**. (Source)

**Former IT Administrator Sentenced To Prison For Attempting Computer Sabotage On 70 Company Servers / Feared He Was Going To Be Laid Off (2005)**

Yung-Hsun Lin was a former Unix System Administrator at Medco Health Solutions Inc.'s Fair Lawn, N.J. He pleaded guilty in federal court to attempting to sabotage critical data, including individual prescription drug data, on more than 70 servers.

Lin was one of several systems administrators at Medco who feared they would get laid off when their company was being spun off from drug maker Merck & Co. in 2003, according to a statement released by federal law enforcement authorities. Apparently angered by the prospect of losing his job, Lin on Oct. 2, 2003, created a "logic bomb" by modifying existing computer code and inserting new code into Medco's servers.

The bomb was originally set to go off on April 23, 2004, on Lin's birthday. When it failed to deploy because of a programming error, Lin reset the logic bomb to deploy on April 23, 2005, despite the fact that he had not been laid off as feared. The bomb was discovered and neutralized in early January 2005, after it was discovered by a Medco computer systems administrator investigating a system error.

Had it gone off as scheduled, the malicious code would have wiped out data stored on 70 servers. Among the databases that would have been affected was a critical one that maintained patient-specific drug interaction information that pharmacists use to determine whether conflicts exist among an individual's prescribed drugs. Also affected would have been information on clinical analyses, rebate applications, billing, new prescription call-ins from doctors, coverage determination applications and employee payroll data. (Source)

**Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System - September 26, 2014**

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared ATC Zero after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

Over the course of 17 days, FAA technical teams worked 24 hours a day alongside the Harris Corporation to completely rebuild and replace the destroyed communications equipment. They restored, installed and tested more than 20 racks of equipment, 835 telecommunications circuits and more than 10 miles of cables. (Source)

**Lottery Official Tried To Rig $14 Million+ Jackpot By Inserting Software Code Into Computer That Picked Numbers - Largest Lottery Fraud In U.S. History - 2010**

This incident happened in 2010, but the articles on the links below are worth reading, and are great examples of all the indicators that were ignored.

Eddie Tipton was a Lottery Official in Iowa. Tipton had been working for the Des Moines based Multi-State Lottery Association (MSLA) since 2003, and was promoted to the Information Security Director in 2013.

Tipton was first convicted in October 2015 of rigging a $14.3 Million drawing of the MSLA lottery game Hot Lotto. Tipton never got his hands on the winning total, but was sentenced to prison. Tipton was released on parole in July 2022.

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005.

Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

That software code was replicated on as many as 17 state lottery systems, as the MSLA random-number software was designed by Tipton. For nearly a decade, it allowed Tipton to rig the drawings for games played on three dates each year: May 27, Nov. 23 and Dec. 29.

Tipton ultimately confessed to rigging other lottery drawings in Colorado, Wisconsin, Kansas and Oklahoma.

**UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT**

Eddie Tipton was making almost $100,000 a year. But he felt underappreciated and overworked at the time he wrote the code to hack into the national lottery system.

He was working 50- to 60-hour weeks and often was in the office until 11 p.m. His managers expected him to take on far more roles than were practical, he complained.

Tipton Stated: "I wrote software. I worked on Web pages. I did network security. I did firewalls," he said in his confession. "And then I did my regular auditing job on top of all that. They just found no limits to what they wanted to make me do. It even got to the point where the word ‘slave’ was used."

Nobody at the MSLA oversaw his complete body of work, and few people truly cared about security, he said. That lack of oversight allowed Tipton to write, install and use his secret code without discovery.
Video Complete Story Indicators Overlooked / Ignored

**DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES**

**Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021**

On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank’s boardroom however the entire bank suffered smoke damage.

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day. The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

She also admitted to using the fraudulently obtained money to fund her boyfriend’s business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million dollars. (Source)

**Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023**

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

Cook was fired for being intoxicated at work. She returned shortly after being escorted out of the hotel by police and set multiple fires in the hotel, displacing the occupants of more than 400 rooms. (Source)

**EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS**

**Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023**

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners. As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

**3 Bank Board Members Of Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged / Bank Collapsed - August 8. 2023**

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

**Bank Director Convicted For $1.4 Million Of Bank Fraud Causing Bank To Collapse - July 12, 2023**

In 2009, Mendel Zilberberg (Bank Director) conspired with Aron Fried and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower (Straw Borrower) to make the loan application. The Straw Borrower applied for a $1.4 Million loan from the Bank on the basis of numerous lies directed by Zilberberg and his coconspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly. Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a $1.4 Million loan to the Straw Borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately $500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator.

The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. (Source)

**Former Vice President Of Discovery Tours Pleads Guilty To Embezzling $600,000 Causing Company To Cease Operations & File For Bankruptcy - June 15, 2022**

Joseph Cipolletti was employed as Vice President of Discovery Tours, Inc., a business that offered educational trips for students. Cipolletti managed the organization's finances, general ledger entries, accounts payable and accounts receivable. Cipolletti also had signature authority on Discovery Tours' business bank accounts.

From June 2014 to May 2018, Cipolletti devised a scheme to defraud parents and other student trip purchasers by diverting payments intended for these trips to his own personal use on items such as home renovations and vehicles.

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy.

Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

**Former Credit Union CEO Sentenced To Prison For Involvement In Fraud Scheme That Resulted In $10 Million In Losses, Forcing Credit Union To Close - April 5, 2022**

Helen Godfrey-Smith's was employed by the Shreveport Federal Credit Union (SFCU) from 1983 to 2017, and during much of that time was employed as the Chief Executive Officer (CEO) of the SFCU.

In October 2016, the SFCU, through Godfrey-Smith, entered into an agreement with the United States Department of the Treasury to buy back certain securities that were part of the Department's Troubled Asset Relief Program (TARP). Godfrey-Smith signed and submitted to the United States Department of the Treasury an Officer's Certificate which certified that all conditions precedent to the closing had been satisfied.

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union. Godfrey-Smith investigated and discovered that there were millions of dollars of fictitious entries on SFCU's general ledger, and the credit union's books were not balanced. But she failed to disclose this information to the United States Department of the Treasury and signed the false Officer's Statement.

In the Spring of 2017, the credit union failed. An investigation by revealed that SFCU had amassed in excess of $10 million in losses by December 2016. (Source)

**Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business (2021)**

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA.

From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

**Former Controller Of Oil & Gas Company Sentenced To Prison For $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)**

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

**Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)**

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

## WORKPLACE VIOLENCE

**Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022**

A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

A jury initially awarded more than $7 billion in damages in July, but the judge lowered that number to roughly $1.1 Billion.

Roy Holden, the former employee who murdered Thomas, performed a service call at her home in December 2019. The next day, while off-duty, he went back to her house and stole her credit cards as he was fixing her fax machine, then stabbed her to death before going on a spending spree with the stolen cards.

The attorneys also argued that Charter Spectrum hired Holden without reviewing his work history and ignored red flags during his employment. (Source)

**Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022**

Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

On or around June 21, 2022 a 55 year old female coworker of Ortiz, experienced a medical emergency and died immediately after treating herself for dehydration using an IV bag of saline taken from the surgical center. An autopsy report revealed that she died from a lethal dose of bupivacaine, a nerve blocking agent.

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU. Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupicavaine, and lidocaine.

Surgical center personnel concluded that the incidents listed above suggested a pattern of intentional adulteration of IV bags used at the surgical center. They identified about 10 additional unexpected cardiac emergencies that occurred during otherwise unremarkable surgeries between May and August 2022 .

The complaint alleges that none of the cardiac incidents occurred during Dr. Ortiz's surgeries, and that they began just two days after Dr. Oritz was notified of a disciplinary inquiry stemming from an incident during which he allegedly "deviated from the standard of care" during an anesthesia procedure when a patient experienced a medical emergency. The complaint alleges that all of the incidents occurred around the time Dr. Ortiz performed services at the facility, and no incidents occurred while Dr. Ortiz was on vacation.

The complaint further alleges that Dr. Ortiz had a history of disciplinary actions against him, and he had expressed his concern to other physicians over disciplinary action at the facility, and complained the center was trying to "crucify" him.

A nurse who worked on one of Dr. Ortiz's surgeries told law enforcement that Dr. Ortiz refused to use an IV bag she retrieved from the warmer, physically waving the bag off. A surveillance video from the center's operating room hallway showed Dr. Ortiz placing IV bags into the stainless-steel bag warmer shortly before other doctors' patients experienced cardiac emergencies.

The complaint alleges that in one instance captured in the surveillance video, Dr. Ortiz was observed walking quickly from an operating room to the bag warmer, placing a single IV bag inside, visually scanning the empty hallway, and quickly walking away. Just over an hour later, according to the complaint, a 56-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. The complaint alleges that in another instance, agents observed Dr. Ortiz exit his operating room carrying an IV bag concealed in what appeared to be a paper folder, swap the bag with another bag from the warmer, and walk away. Roughly half an hour later, a 54-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. (Source)

**Former Nurse Charged With Murder Of 2 Patients At Hospital, Nearly Killing 3rd By Administering Lethal Doses Of Insulin - October 26, 2022**

Jonathan Hayes, a 47-year-old former Nurse at Atrium Health Wake Forest Baptist Medical Center in Winston-Salem, North Carolina, has been charged with 2 counts of murder and 1 count of attempted murder.

O'Neill said that on March 21, a team of investigators at the hospital presented him with information that Hayes may have administered a lethal dose of insulin to one patient and indicated there may be other victims.

The 1 count of murder against Hayes is related to the death of 61 year old Jen Crawford. Hayes administered a lethal dose of insulin to Crawford on Jan. 5. She died three days later.

The 2 count of murder is in connection with the death of 62-year-old Vickie Lingerfelt, who was administered a lethal dose of insulin on Jan. 22. She died on Jan. 27.

Hayes is also charged with administering a near-lethal dose of insulin to 62-year-old Pamela Little on Dec. 1, 2021. Little survived and Hayes faces one count of attempted murder.

Hayes was terminated from the hospital in March 2022, and he was arrested In October 2022. (Source)

**Hospital Nurse Alleged Killer Of 7 Babies / 15 Attempted Murders - October 13, 2022**

A neonatal nurse in the U.K. who allegedly murdered 7 babies and attempted to kill 10 more wrote notes reading, "I don't deserve to live," "I killed them on purpose because I'm not good enough to care for them. I am a horrible evil person."

Lucy Letby, 32, who worked in the Neonatal Unit of the Countess of Chester Hospital, left handwritten notes in her home that police found when they searched it in 2018, prosecutor Nick Johnson stated during her trial in October 2022.

Johnson argued that Letby was a constant, malevolent presence in the neonatal unit. Of the babies Letby allegedly murdered or attempted to murder between 2015 and 2016, the prosecution said she injected some with insulin or milk, while another she injected with air. She allegedly attempted to kill one baby three times.

Johnson told jurors the hospital had been marked by a significant rise in the number of babies who were dying and in the number of serious catastrophic collapses" after January 2015, before which he said its rates of infant mortality were comparable to other busy hospitals.

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours.

Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

**Former Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans - May 11, 2021**

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VAMC) in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

**Indianapolis FedEx Shooter That Killed 8 People Was Former FedEx Employee With Mental Health Problems - April 20, 2021**

Police say the 19 year old Indianapolis man who fatally shot 8 people at a southwest side FedEx Ground facility in April had planned the attack for at least nine months.

In a press conference, local and federal officials said the shooting was "an act of suicidal murder" in which Bandon Scott Hole decided to kill himself "in a way he believed would demonstrate his masculinity and capability while fulfilling a final desire to experience killing people."

Hole worked at the FedEx facility between August and October 2020. Police believe he targeted his former workplace not because he was trying to right a perceived injustice, but because he was familiar with the "pattern of activity" at the site.

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house. Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check. Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

**Former Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder - September 22, 2020**

On August 12, 2003, Richard Wilbern walked into Xerox Federal Credit Union, located on the Xerox Corporation campus, and committed robbery and murder. Wilbern was not caught until 2016 for robbery and murder, and was sentenced this week to life in prison.

Richard Wilbern walked into Xerox Federal Credit Union (XFCU) and was wearing a dark blue nylon jacket with the letters FBI written in yellow on the back of the jacket, sunglasses and a poorly fitting wig. Wilbern was also carrying a large briefcase, a green and gray-colored umbrella and had what appeared to be a United States Marshals badge hanging on a chain around his neck.

Wilbern was employed by Xerox between September 1996 and February 23, 2001 as which time he was terminated for repeated employment related infractions. In 2001, Wilbern filed a lawsuit against Xerox alleging that the company unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. Wilbern also maintained a checking and savings accounts at the Xerox Federal Credit Union. Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy.

In March 2016, a press conference was held to seek new leads in the investigation. Details of the crime were released as well as photographs of Wilbern committing the robbery. Anyone with information was asked to call a dedicated hotline.

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

In July 20016, FBI agents met with Wilbern regarding a complaint he had made to the FBI regarding an alleged real estate scam. During one of their meetings, agents obtained a DNA sample from Wilbern after he licked and sealed an envelope. That envelope was sent to OCME, and after comparing the DNA profile from the envelope to the DNA profile previously developed from the umbrella, determined there was a positive match. (Source)

**Florida Best Buy Driver Murders 75 Year Old Woman While Delivering Her Appliances - Lawyers Said The Murder Was Preventable If Best Buy Had Better Screened Employees' - September 30, 2019**

A Boca Raton family has filed a wrongful death lawsuit against Best Buy. This comes after allegations a delivery man for the company killed a 75-year-old woman while delivering appliances.

The family of 75 year old Evelyn Udell has filed a wrongful death lawsuit to hold Best Buy, two delivery contractors and the two deliverymen, accountable for her death.

Lawyers say the fatal attack was preventable if the companies had further screened their employees'.

On August 19th, police say Jorge Lachazo and another man were delivering a washer and dryer the Udells had bought from Best Buy.

Police say Lachazo beat Udell with a mallet, poured acetone on her body and set her on fire. She died the next day. Lachazo was arrested and is charged with murder.

According to the lawsuit, Best buy stores did nothing to investigate, supervise, or oversee the personnel used to perform these services on their behalf. Worse, it did nothing to advise, inform, or warn Mrs. Udell that the delivery and installation services had been delegated to a third-party.

Lawyers are also calling for sweeping changes to how businesses screen workers who have to go inside a customers' home. (Source)

**WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE**
This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

**View On The Link Below Or Download The Flipboard App To View On Your Mobile Device**
https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

**WORKPLACE VIOLENCE TODAY E-MAGAZINE**
https://www.workplaceviolence911.com/node/994

# INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

**CTTP =** China Thousand Talents Plan

- NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers
- U.S. Petroleum Company Scientist STP For $1 Billion Theft Of Trade Secrets - Was Starting New Job In China
- Cleveland Clinic Doctor Arrested For $3.6 Million Grant Funding Fraud Scheme Involving CTTP
- Hospital Researcher STP For Conspiring To Steal Trade Secrets And Sell Them in China With Help Of Husband
- Employee Of Research Institute Pleads Guilty To Steal Trade Secrets To Sell Them In China
- Raytheon Engineer STP For Exporting Sensitive Military Technology To China
- GE Power & Water Employee Charged With Stealing Turbine Technologies Trade Secrets Using Steganography For Data Exfiltration To Benefit People's Republic of China
- CIA Officer Charged With Espionage Over 10 Years Involving People's Republic of China
- Massachusetts Institute of Technology (MIT) Professor Charged With Grant Fraud Involving CTTP
- Employee At Los Alamos National Laboratory Receives Probation For Making False Statements About Being Employed By CTTP
- Texas A&M University Professor Arrested For Concealing His Association With CTTP
- West Virginia University Professor STP For Fraud And Participation In CTTP
- Harvard University Professor Charged With Receiving Financial Support From CTTP
- Visiting Chinese Professor At University of Texas Pleads Guilty To Lying To FBI About Stealing American Technology
- Researcher Who Worked At Nationwide Children's Hospital's Research Institute For 10 Years, Pleads Guilty To Stealing Scientific Trade Secrets To Sell To China
- U.S. University Researcher Charged With Illegally Using $4.1 Million In U.S. Grant Funds To Develop Scientific Expertise For China
- U.S. University Researcher Charged With VISA Fraud And Concealed Her Membership In Chinese Military
- Chinese Citizen Who Worked For U.S. Company Convicted Of Economic Espionage, Theft Of Trade Secrets To Start New Business In China
- Tennessee University Researcher Who Was Receiving Funding From NASA Arrested For Hiding Affiliation With A Chinese University
- Engineers Found Guilty Of Stealing Micron Secrets For China
- Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China
- Husband And Wife Scientists Working For American Pharmaceutical Company, Plead Guilty To Illegally Importing Potentially Toxic Lab Chemicals And Illegally Forwarding Confidential Vaccine Research to China
- Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Setup New Business In China
- Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION To Setup Business In China
- University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government
- Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company
- Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees' To Steal Technology

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy
- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company

# SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

**Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group**

The websites listed below are updated monthly with the latest incidents.

## INSIDER THREAT INCIDENTS E-MAGAZINE

**2014 To Present / Updated Daily**

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,000+ Incidents**).

**View On This Link. Or Download The Flipboard App To View On Your Mobile Device**

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

## INSIDER THREAT INCIDENTS MONTHLY REPORTS

**July 2021 To Present**

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

## INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

## INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

https://www.insiderthreatdefense.us/category/insider-threat-incidents/

**Incident Posting Notifications**

Enter your e-mail address in the Subscriptions box on the right of this page.
https://www.insiderthreatdefense.us/news/

## INSIDER THREAT INCIDENTS COSTING $1 MILLION TO $1 BILLION +

https://www.linkedin.com/post/edit/6696456113925230592/

## INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

**Updated Daily**

https://twitter.com/InsiderThreatDG
**Follow Us On Twitter**: @InsiderThreatDG

## CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

# National Insider Threat Special Interest Group (NITSIG)

## NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The NITSIG has been successful in bringing together Insider Risk Management (IRM) professionals and other security professionals from the U.S. Government, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

**The NITSIG Provides IRM Guidance And Training To The Membership And Others On;**

- ✓ Insider Threat Program (ITP) Development, Management & Optimization
- ✓ ITP Working Group / Hub Operations
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Insider Threat Awareness and Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

The NITSIG has created a LinkedIn Group for individuals that interested in sharing and gaining in-depth knowledge regarding IRM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for IRM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in IRM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for IRM.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to cancel ITS&E events for a few years due to COVID. We are in the process of planning our next ITS&E.

**NITSIG Insider Threat Mitigation Resources**

Posted on the NITSIG website are various documents, resources and training that will assist organizations with ITP Development, Management, Optimization and IRM.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

***Employee Risk / Threat Mitigations Is Our Business***

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Risk Mitigation (IRM) training and consulting services.

**The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:**
White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines, ) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **900+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over **14+** years of experience providing IRM training and consulting services, we approach the Insider Threat problem and IRM from a realistic, operational and holistic perspective. A primary centerpiece of providing our clients with a comprehensive IRM Framework, is that we incorporate lessons learned based on our analysis of ITP's and Insider Threat related incidents encountered from working with our clients.

Our IRM training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

**ITDG IRM Training / Consulting Services Offered**
**Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)**

- ✓ IRM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development, Management & Optimization Training Course & Related Training Courses
- ✓ IRM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Risk - Threat Vulnerability Assessments That Go Beyond Compliance Regulations For IRM
- ✓ ITP Gap Analysis Assessments
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized IRM Consulting Services For Our Clients

**Additional Background Information On ITDG**
Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG Meetings, ITS&E Events and ITDG Training Courses / Consulting Services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,300+** individuals. The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to 100 NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

**Jim Henderson, CISSP, CCISO**
**CEO Insider Threat Defense Group, Inc.**
**Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor**
**Insider Risk / Threat Vulnerability Assessment Specialist**
**ITP Gap Analysis / Evaluation & Optimization Specialist**
LinkedIn ITDG Company Profile
**Follow Us On Twitter / X: @InsiderThreatDG**

**Founder / Chairman Of The National Insider Threat Special Interest Group**
**Founder / Director Of Insider Threat Symposium & Expo**
**Insider Threat Researcher / Speaker**
LinkedIn NITSIG Group

**Contact Information**
**561-809-6800**
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org