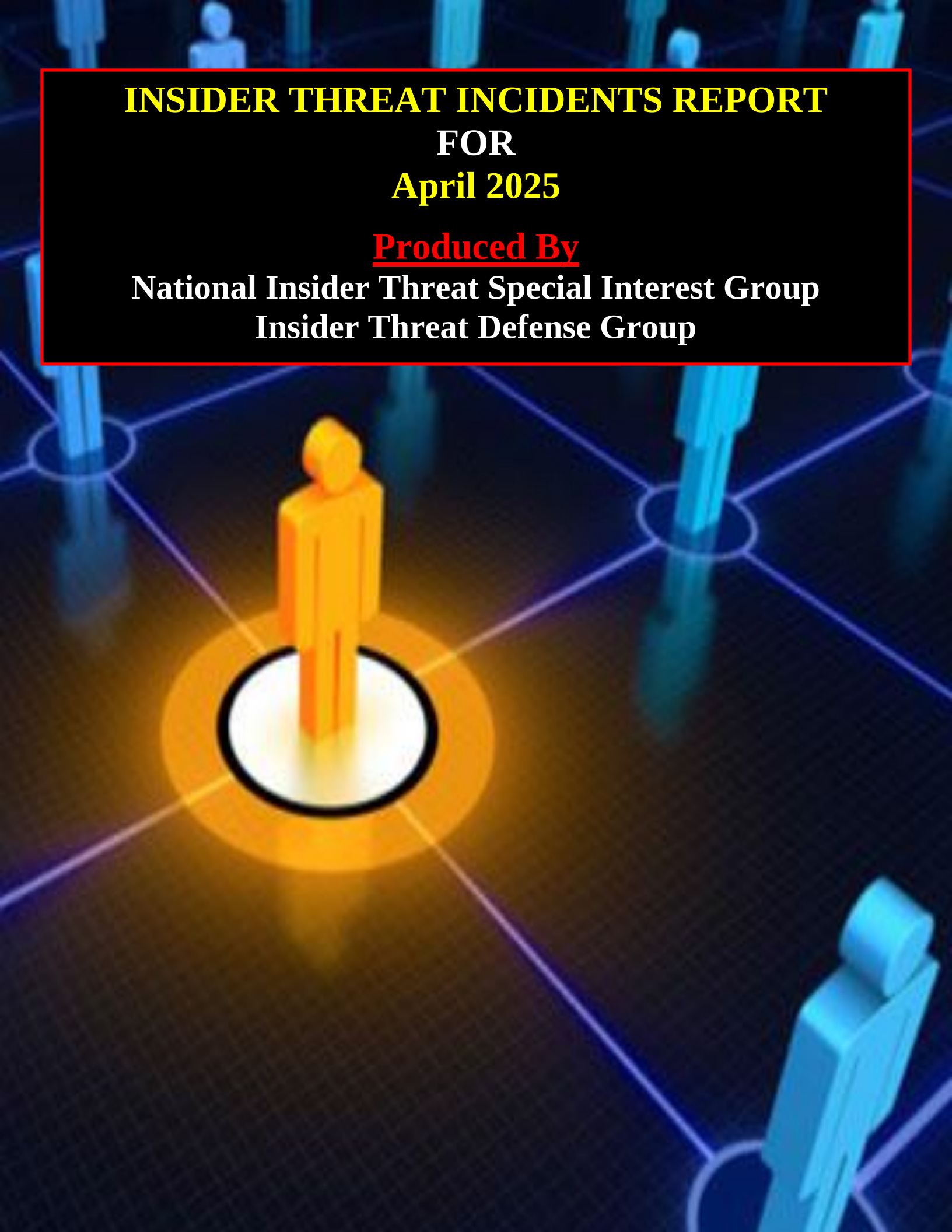


INSIDER THREAT INCIDENTS REPORT
FOR
April 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

TABLE OF CONTENTS

PAGE

Insider Threat Incidents Report Overview ……. 3

Insider Threat Incidents For April 2025 …… 4

Definitions of Insider Threats …… 23

Types Of Organizations Impacted …… 23

Insider Threat Damages / Impacts Overview ……... 24

Insider Threat Motivations Overview ……... 25

What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations …… 26

2024 Association Of Certified Fraud Examiners Report On Fraud …….. 27

Fraud Resources …….. 28

Severe Impacts From Insider Threat Incidents …… 29

Insider Threat Incidents Involving Chinese Talent Plans …… 52

Sources For Insider Threat Incidents Postings …… 54

National Insider Threat Special Interest Group Overview …….. 55

Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview …… 57

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 **6,200+** 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, embezzlement, contracting fraud, bribery and kickbacks. This is 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. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

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 Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 21** of this report provide the justification, return on investment and the funding that is needed for an IRM 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 APRIL 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

United Kingdom Intelligence Agency Employee Pleads Guilty To Stealing Classified Top Secret Information - March 31, 2025

Hasaan Arshad, 25, from Rochdale, Greater Manchester, pleaded guilty to an offence under the Computer Misuse Act on what would have been the first day of his trial. The charge related to doing an unauthorised act which risked damaging national security.

On August 24 2022 he took his work mobile phone into a top secret area of GCHQ and connected the device to a top secret work station, it was alleged. He then transferred sensitive data from a secure, top secret computer to the phone before taking it home, it was claimed. Arshad then transferred the data from the phone to a hard drive connected to his personal home computer. (Source)

U.S. GOVERNMENT

Former Congressman George Santos Sentenced To Prison For Wire Fraud and Aggravated Identity Theft - April 25, 2025

Former Congressman George Santos was sentenced to prison for committing wire fraud and aggravated identity theft. As part of the sentence, Santos was ordered to pay restitution to his victims in the amount of $373,749.97 and $205,002.97 in forfeiture. Santos pleaded guilty in August 2024.

Santos Filed Fraudulent FEC Reports, Embezzled Funds from Campaign Donors, Stole Identities, Charged Credit Cards Without Authorization, Obtained Unemployment Benefits Through Fraud, and Lied in Reports to the U.S. House of Representatives. (Source)

Former FAA Contractor Pleads Guilty To Illegally Acting As An Agent Of The Iranian Government - April 16, 2025

From at least December 2017 through June 2024, Abouzar Rahmati conspired with Iranian government officials and intelligence operatives to act on their behalf in the United States, including by meeting with Iranian intelligence officers in Iran, communicating with coconspirators using a cover story to hide his conduct, obtaining employment with an FAA contractor with access to sensitive non-public information, and obtaining open-source and non-public materials about the U.S. solar energy industry and providing it to Iranian intelligence.

From June 2009 to May 2010, Rahmati served as a First Lieutenant in the Islamic Revolutionary Guard Corps (IRGC), an Iranian military and counterintelligence organization under the authority of the Supreme Leader of Iran. After being discharged from the IRGC, Rahmati lied to the United States government regarding his military service with the IRGC in order to, among other things, gain employment as a U.S. government contractor. (Source)

Booz Allen Hamilton Agrees To Pay $422,000+ To Settle Allegations That A BAH Employee Billed General Services Administration For Work Not Performed - April 4, 2025

Booz Allen Hamilton Inc. (BAH), located in McLean, agreed to pay $422,557 to settle allegations that a BAH employee assigned to work on a General Services Administration (GSA) contract over reported his time resulting in BAH issuing invoices for services under the contract that were not performed.

Between 2018 and 2022, GSA paid invoices submitted by BAH that included services for a BAH employee under a GSA contract. Investigators from GSA and the Defense Intelligence Agency compared invoices and timesheets for the employee with the employee's badge swipe data for entering and exiting the secure facility where the contract was performed to determine the number of overcharged hours attributable to the employee. As a result, the government alleged that BAH billed for services that the employee did not provide. BAH agreed to settle allegations for common law claims of payment by mistake and unjust enrichment.

This investigation was initiated when BAH made a contractor disclosure. BAH received credit under the Department of Justice's guidelines for taking disclosure, cooperation, and remediation into account. (Source)

U.S. Forest Service Law Enforcement Officer Pleads Time & Attendance Fraud Of $18,000+ - April 21, 2025

The government alleged in court documents that the defendant (Nathan Snead) was required to work 40 hours of regular time per week, and he was compensated for administratively uncontrollable overtime, which is premium pay designed to compensate law enforcement officers (LEOs) for irregular and unscheduled overtime duty. In 2023, Snead's overtime rate was 15%, meaning he was required to justify an additional 5-7 hours per week to maintain that percentage at his next overtime review.

On May 2, 2023, based on informationSnead was not working his claimed hours, agents installed a GPS tracker on his government-issued patrol vehicle to monitor his movements. The tracker data showed Snead's patrol vehicle was stationary at his house during hours he claimed to be working.

On several occasions, Snead certified on his Time and Attendance Record he worked an 8-hour regular shift. However, his patrol vehicle remained stationary at his house for the entire 8 hours. Additionally, Snead claimed overtime hours when his patrol vehicle was stationary at his house for much of his regular shift and for the entire time of claimed overtime.

Agents also evaluated Snead's law enforcement statistics from 2021 through 2023. His productivity levels, measured via incident reports and the issuance of violation notices, were much lower than other similarly situated LEOs. Snead's false time claims resulted in him stealing approximately $18,645. (Source)

GSA Contracting Officer Representative Accepted $50,000 Worth Of Bribes From Company - April 21, 2025

Christopher Brackins, 51, conspired to bribe a former GSA contracting officer's representative (COR).

Between 2018 and 2021, Brackins provided approximately $50,000 worth of money and other things of value to the COR in exchange for the COR to direct GSA projects to Brackins's company. For example, in late 2018, as part of the bribery scheme, Brackins paid a fraudulently inflated bonus to one of his employees. Brackins then directed the employee to the COR $8,000 in cash from the fraudulently inflated bonus check.
In early 2021, Brackins paid the COR $25,000, at direction of the COR, using an intermediary who accepted the payments through the intermediary's air-conditioning repair business. The defendant and his company earned an estimated $133,413 in profits from this scheme. (Source)

U.S. Postal Service Employee Sentenced To Probation For Embezzling $37,000+ - April 21, 2025

Jaterria Davis was employed as the Lead Sales and Service Associate at the United States Post Office in Mishawaka, Indiana. Her duties included gathering the daily deposits of cash and checks paid to the post office for postal goods and services that were to be forwarded on to the post office for deposit.

From on or about July 20, 2024, through August 14, 2024, Davis violated her position of trust by embezzling for her own use, $37,023 in cash deposits paid to the post office.

Davis was sentenced to probation and ordered to pay $37,023 in restitution to the United States Postal Service. (Source)

U.S. Postal Service Carrier Sentenced To Prison For Stealing $155,000+ Of Checks From Mail To Support Drug Habit - April 25, 2025

Kiesha Brown, 32, worked for the U.S. Postal Service as a city carrier assistant at the LC Page Post Office in Norfolk, Virginia.

Beginning in June 2023, the U.S. Postal Service, Office of Inspector General began receiving complaints regarding mail theft and check fraud from customers utilizing the LC Page Postal Station.

In June 2023, a victim whose business was on Brown's delivery route reported that 16 checks had been stolen from the mail. The victim reported that one check in the amount of $146.64 did not reach the intended recipient, but was altered and deposited in a bank account in the amount of $4,890.02. Numerous customers on Brown's postal route complained of similar frauds occurring with checks they had mailed through the LC Page Post Office.

Brown was observed in her postal vehicle using drugs and rummaging through and stealing mail. Brown provided mail to an accomplice in exchange for cash to support her daughter and her drug habit. Investigators identified 37 people victimized by Brown. Brown's theft caused an intended loss of approximately $245,000 and an actual loss of $155,297.91.

In addition to her term of imprisonment, the Court ordered that Brown is to pay restitution in the total amount of $155,297.91. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former CIA Contractor Pleads Guilty To Acting As A Foreign Agent, Mishandling Classified Materials And Accepting Bribes - April 23, 2025

Dale Bendler began working as a full-time contractor at the CIA with a Top Secret SCI security clearance. Before he was a CIA contractor, Bendler spent over 30 years working for the CIA as an intelligence officer and retired as a member of the Senior Intelligence Service in 2014.

Beginning in July 2017 and continuing through at least July 2020, while a full-time CIA contractor and TS/SCI clearance holder, Bendler worked with a U.S. lobbying firm and engaged in unauthorized and hidden lobbying and public relations activities on behalf of foreign national clients. Bendler's undisclosed lobbying activities included an attempt to use his position and access at the CIA to influence a foreign government's embezzlement investigation of one of Bendler's foreign national clients and a separate attempt to use his position and access at the CIA to influence the U.S. government's decision as to whether to grant a U.S. visa to another of Bendler's clients, who was alleged to be associated with terrorism financing. In exchange for his unauthorized outside activities, Bendler was paid hundreds of thousands of dollars.

During the course of Bendler's unauthorized lobbying and public relations activities, Bendler also abused his access to CIA resources and personnel by, among other things, searching classified CIA systems for any information related to his private lobbying clients, improperly storing and disclosing non-public, sensitive, and classified U.S. government information to people not authorized to receive such information, and lying to the CIA and the FBI about his status as a foreign agent and his unauthorized lobbying and public relations activities. The CIA terminated Bendler's contract and access in September 2020. (Source)

U.S. Army Intelligence Analyst Sentenced To Prison For Selling Sensitive Military Information To Individual In Chinese Government For $42,000 - April 23, 2025

Between May 2022 until his arrest in March 2024, Korbein Schultz engaged in an ongoing conspiracy to provide dozens of sensitive U.S. military documents, many containing export-controlled tactical and technical information, directly to a foreign national residing in the People's Republic of China.

Despite clear indications that this individual was likely connected to the Chinese government, the Schultz continued the relationship in exchange for financial compensation. In exchange for approximately $42,000, Schultz provided documents and data related to U.S. military capabilities. (Source)

Former Naval Undersea Warfare Center Employee Charged For Making Death Threats To Employees - April 15, 2025

Luis Pardella is a former employee of the Naval Undersea Warfare Center in Middletown, Rhode Island.

Between July 2022 and February 2023, Pardella, 38, made numerous menacing, and at times threatening, telephone calls to at least eight of his former colleagues at the Naval Undersea Warfare Center. In one such instance, it is alleged that Pardella left a voicemail stating, "I will kill you and your wife when I see you on the street."

It is further alleged that between December 2022 and February 2023, Pardella made multiple threatening telephone calls to the Portsmouth, RI, Police Department, stating that an officer and his wife "will be going to jail," that "the Portsmouth Police Department is corrupt," and "write down (name of officer's wife) is dead write down. The wife of one of your cops is dead. Do you know who (name redacted) is? Write down she is dead." (Source)

CRITICAL INFRASTRUCTURE

Board Members For Water Works & Sewer Board And Co-Conspirators Charged In $2.4 Million Fraud Scheme - April 3, 2025

Criminal charges were placed against 7 defendants for a multi-million dollar fraud scheme at the Water Works and Sewer Board of the City of Prichard. in Alabama.

The Grand Jury returned an indictment alleging the following scheme: starting as early as 2018 through 2022, the defendants bilked the Prichard Water Board of at least approximately $2.4 million dollars through a false and fraudulent contractor scheme involving outside contractors and employees and board members of the Prichard Water Board. Approximately $960,000 of the money was illegally laundered, including through a business owned and operated by Nia Bradley and Randy Burden.

Ayanna Payton and another uncharged co-conspirator served on the board of the Prichard Water Board where they are alleged to have falsified payment authorizations and received kick-back payments and other benefits for their roles. Several of the conspirators communicated through coded messages and destroyed evidence to attempt to avoid detection of the crimes, according to the indictment. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S. Customs & Border Protection (CBP) Officer Arrested For Obtaining $149,000+ Of COVID 19 Business Relief Funds For Fake Companies - April 24, 2025

Amer Aldarawsheh a U.S. CBP Officer has been arrested for fraudulently obtaining nearly $150,000 in COVID-19 pandemic business-relief loan funds for two of his sham businesses.

Aldarawsheh owned and purportedly operated two businesses: Nahar Enterprises Inc., a San Bernardino based business he described as a trucking and freight company, and Ameral, which he described as an automotive repair company.

From July 2020 to December 2021, Aldarawsheh made false statements to the Small Business Administration (SBA) to fraudulently obtain a loan under the Economic Injury Disaster Loan Program (EIDL), which provided low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters.

Aldarawsheh applied to the SBA for EIDL loans on behalf of his two companies, neither of which had substantial business or employees.

EIDL loans were supposed to be used by the recipient to only pay certain authorized business expenses. Instead, Aldarawsheh knowingly misappropriated and misused the EIDL funds he received from the SBA for his own personal benefit, including in December 2020, causing the transfer of $149,900 in SBA COVID-19 EIDL loan funds to be wired from the SBA to a bank account under his control. (Source)

DEA Task Force Officer Sentenced To Prison For Drug Distribution - April 8, 2024

While employed as a Florida Highway Patrol Trooper and designated Task Force Officer with the Drug Enforcement Administration,Joshua Earrey and a co-conspirator engaged in widespread and extensive corrupt activity from 2017 - 2023. These corrupt acts included the theft of money and illegal drugs that were seized as evidence during criminal investigations; providing the illegal drugs to others to distribute on his behalf; and extorting or accepting cash payments from drug dealers in exchange for protecting them from arrest by law enforcement.

Earrey and his co-conspirator stole more than 1,000 pounds of marijuana from evidence and covered up the theft by submitting falsified paperwork showing that the drugs had been destroyed.

Earrey, who had an addiction to prescription opiates, also used his corrupt activities to obtain illegal drugs for his own use. On one occasion, he traded cases of ammunition that he had diverted from the Florida Highway Patrol to a convicted murderer in exchange for oxycodone. Despite knowing that his drug addiction made it illegal for him to have firearms and ammunition, Earrey continued to possess these items in violation of federal law. (Source)

U.S. Customs & Border Protection Officer Sentenced To Prison For Accepting $12,000 In Bribes For Role In Alien Smuggling - March 31, 2025

In December 2022, investigating agents received information that Omar Moreno, 46, was smuggling illegal aliens into the United States as a CBP officer, receiving $4,000 per alien from a smuggling organization. On Feb. 1, 2024, a video recording captured Moreno escorting two illegal aliens, one being a foot guide, into the U.S. through the Ysleta Port of Entry without undergoing an inspection.

On Feb. 23, 2024, two undercover officers posed as illegal aliens and used a confidential human source as a foot guide to enter the U.S. from Mexico. Again, Moreno allowed the smuggling to occur through the port of entry. After his shift ended, Moreno was paid $8,000 and arrested. (Source)

New York City Fire Department (FDNY) Bureau of Fire Prevention Chief Sentenced To Prison For Accepting $190,000 In Bribes - March 31, 2025

From 2021 to 2023, Brian Cordasco repeatedly abused his position as a Chief of the Bureau of Fire Prevention (BFP), by participating in a scheme to solicit and receive $190,000 in total bribe payments from a former FDNY firefighter named Henry Santiago, Jr.

In exchange for those bribe payments, Cordasco used his authority within the BFP to improperly "expedite" BFP inspections and plan reviews for Santiago's customers.

Cordasco personally profited $57,000 as part of this scheme. To carry out this conspiracy, Cordasco lied to his BFP subordinates to justify otherwise improper expediting requests. Cordasco also lied to law enforcement when interviewed about his involvement in the scheme. (Source)

Volunteer Fire Chief Sentenced To Prison For $50,000 COVID-19 Fraud Scheme / Used Funds For Personal Use - April 8, 2025

Christopher Chapman is the former Fire Chief of the Blackberry Volunteer Fire Department (BVFD) in Pike County, Kentucky.

In Spring 2022, Pike County local government authorized the distribution of $50,000 of these funds through grants that were allocated for the purchase of turnout gear for fire and rescue, along with equipment and building maintenance. Chapman applied for these grants on behalf of BVFD, and the local government awarded the full amount of the grants.

Chapman created a company named Rural Public Safety Equipment, LLC. (RPSE), as the sole organizer and member, and registered it with the West Virginia Secretary of State. Chapman then informed members of the BVFD that he could obtain fire safety equipment at cost from a safety equipment company, and he failed to disclose that he was the owner of the company. The fire department pre-paid and ordered $76,854.50 worth of fire and safety equipment from RPSE. Instead of using the prepayments from BVFD to fulfill the orders, Chapman never fulfilled any fire and safety equipment orders, spent all the money on his own personal use, and withdrew $61,500 in cash from the RPSE bank account. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Detroit Riverfront Conservancy Chief Financial Officer Sentenced To Prison For Embezzling $40 Million+ Over 12 Years / USed Funds To Live Extravagant Lifestyle - April 24, 2025

William Smith was employed as the Chief Financial Officer for the Detroit Riverfront Conservancy, Inc. (DRC) from 2011 through May 2024.

The DRC is a 501(c)(3) organization formed with the mission of developing access to the Detroit riverfront. In his position as Chief Financial Officer of the DRC, Smith enjoyed substantial discretion in overseeing and managing the Conservancy's financial affairs.

Beginning no later than November 2012 and continuing until May 2024, Smith orchestrated a scheme to embezzle millions of dollars in funds belonging to the DRC.

Court documents indicate Smith engaged in various practices to cover up and sustain this massive fraud scheme. In some instances, Smith falsified bank statements that he provided to the DRC bookkeeper, altering or deleting unauthorized transfers on the statements in order to keep them off of the DRC books. In at least one other instance, he took out a line of credit with a financial institution (Citizen's Bank) on behalf of the DRC.

Smith claimed to be acting with the authorization of the DRC Board of Directors in taking out this line of credit. In fact, Smith had no such authority, and the documents he provided Citizen's Bank purporting to show that he had such authorization were forgeries. Smith used the funds from this line of credit (which eventually totaled $5 million) to infuse monies into the Conservancy's bank accounts to help cover up his substantial embezzlement from those accounts.

Smith spent the money he appropriated from the DRC to live a lavish and extravagant lifestyle. Over the course of his scheme, Smith spent enormous sums of money on basketball tickets, cruises, private jet travel, designer clothing, jewelry, and the like. (Source)

Public Housing Authority Executive Director Sentenced To Prison For Embezzling $129,000+ / Used Funds For Airplane Tickets, Medical Expenses, Etc. - April 16, 2025

The American Falls Housing Authority (AFHA) is a federally funded public housing authority that manages public housing in American Falls, Idaho. Between 2019 and 2023, Bruce Hauber was employed as the Executive Director of AFHA and was tasked with paying bills, purchasing supplies, collecting rent, and managing bank accounts.

Beginning in spring 2019, Hauber began to make purchases on AFHA credit cards for unauthorized personal expenses, such as meals, airplane tickets, utilities for his home, medical expenses, and purchases at retailers. In total, between spring 2019 through 2023, Hauber made $129,022.38 in unauthorized personal expenses. Hauber used AFHA funds to make payments for those personal expenses. To conceal the embezzlement, Hauber wrote fictitious checks to venders and entered the checks into AFHA's internal accounting system. (Source)

City Employee Arrested For Altering Her Time Sheets Since 2022 And Receiving $6,200 Of Unauthorized Payroll - April 17, 2024

Kentucky State Police reported that a payroll employee for the City of Oak Grove was arrested and charged after an investigation found that she allegedly altered her time sheets and destroyed payroll records.

KSP detailed that 38-year-old Hailey Bamford was found to have allegedly "falsified her time entry and altered her time sheets since May 2022."

During the investigation, KSP noted that an audit revealed several instances of "false entries, altering, deletion, and destruction of records to business payroll" for the city.

Further, from May 2022 through October 2023, Bamford allegedly falsified business records "to obtain city taxpayer money via theft of time for a minimum of $6,208.75," according to KSP. (Source)

D.C. Department Of Human Services Employee Sentenced To Prison For Extorting Money From Low-Income Individuals To Process Assistance Applications - April 25, 2025

Ruth Nivar, 57, is a former D.C. Department of Human Services employee. She was sentenced to federal prison for extorting money from low-income individuals to process applications for public assistance programs, even though it was part of her job responsibilities to do that work free of charge.

Beginning at least since 2018 and continuing through at last May 2023, Nivar used the authority of her public office to obtain money from public assistance applicants to which she was not entitled. Nivar preyed on impoverished, largely non-English speaking individuals who lacked the resources to navigate what can be the complicated process of obtaining health care coverage from the government.

In 2022, after Nivar understood that law enforcement may have become aware of her scheme, she added an accomplice, a civilian who did not work for the D.C. government, to assist in the extortion scheme.

Because Nivar worked on public assistance programs for the D.C. government, Nivar was able to provide information to her accomplice about eligibility requirements for applicants – including certain documents that needed to be submitted with applications – as well as information about applicants from the internal DHS database, including historical benefits information, status of benefits, identity verification, and dependent information. The accomplice then created online accounts and submitted application materials for health care coverage on behalf of the individuals they extorted. Nivar told individuals to pay her accomplice, who would then split the monies evenly with Nivar, even though it was Nivar's duty to provide all these services for the community free of charge. (Source)

County Employee Arrest For Stealing Electronic Components - April 14, 2024

Shasta County employee Matthew Silveira, 39, has been arrested and charged with embezzlement following an investigation into missing components from county-owned electronics, the Shasta County Sheriff's Office (SCSO) announced.

In October 2024, the SCSO said county employees discovered inoperable electronics in storage, leading to an investigation that revealed crucial components had been removed. Further inquiries uncovered an online sales account actively selling Shasta County property.

The SCSO Major Crimes Unit took over the case, and detectives identified Silveira, a Redding resident, as the account's owner. A search warrant executed at Silveira's home resulted in the recovery of additional county property. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former County Schools Maintenance Supervisor Pleads Guilty To $3.4+ Million Invoicing Fraud Scheme - April 7, 2025

From about November 2019 through December 2023, Michael Barker ordered custodial and janitorial supplies for Boone County Schools from Jesse Marks and his company, Rush Enterprises. These supplies included hand soap, trash can liners, face masks, face shields, and hand sanitizer.

Barker admitted that he and Marks agreed that Rush Enterprises would overbill the Boone County Board of Education for these supplies. As part of this scheme, Barker approved invoices on behalf of Rush Enterprises that significantly inflated the number of products that were actually delivered to Boone County Schools. Barker submitted these fraudulent invoices to the Boone County Board of Education, which relied on them to mail checks to Rush Enterprises using the United States Mail.

Marks deposited the checks from Boone County Schools into the business bank account for Rush Enterprises, wrote himself checks on that account that he cashed at various banks, and personally delivered some of that cash to Barker in manila envelopes. Barker admitted that he spent the cash delivered by Marks to buy vehicles and equipment and make substantial improvements to his residence.

Marks deducted the cost of the products actually delivered to Boone County Schools from the proceeds of the overbilling scheme. Boone County Schools paid Rush Enterprises $4,310,714.82 from in or about November 2019 through in or about December 2023. Barker admitted that approximately 80 percent of the total payments received by Rush Enterprises, or $3,448,571.85, was based on fraudulent invoices. (Source)

Business Manager For School District Sentenced To Prison For Stealing $340,000 / Used Funds For Trips To Walt Disney World - April 25, 2025

Brandon Looney stole nearly $340,000 from Trinidad Independent School District (ISD) in Texas, between 2017 and 2023 while he served as Trinidad ISD's business manager. Federal law makes it a crime for someone to steal from an organization receiving more than $10,000 in federal funds annually.

Looney used the stolen funds to purchase personal trips to Walt Disney World and on spending sprees at the Disney Store. Trinidad ISD is one of the poorest school districts in Texas and suffered adverse financial consequences as a result of Looney's theft.

Looney worked with the Financial Litigation Unit of the U.S. Attorney's Office to liquidate his available assets, including his home, to pay $200,000 of the restitution before sentencing. The remaining balance of the restitution judgment will be collectible for 20 years after the termination of Looney's incarceration. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Contractor Admits To Role In $8.6 Million Debit Card Fraud Scheme - April 3, 2025

Jaysha Victorian worked for a bank contractor from late 2020 to early 2021. She used her access to the systems of a national banking institution to load prepaid debit cards with fraudulent funds. These included prepaid cards that were used to provide unemployment benefits, including for the state of California.

The cards were distributed to other recipients, who withdrew the funds at ATMs and other locations. In total, Victorian credited at least 187 cards with nearly $8.6 million in fraudulent funds. Over $7.6 million of that amount had been withdrawn or spent before the bank could freeze the cards.

Victorian admitted she used some of the funds to conduct ATM transactions on her own, including a $1,000 withdrawal at a branch in Houston. She also received approximately $300,000 in cash proceeds from her role in the scheme. (Source)

Bank General Counsel Sentenced To Prison For Embezzling $7.4 Over 10 Years / Used Funds To Purchase Vacation Property, Luxury Vehicles, Etc. - April 24, 2025

From approximately 2013 to January 2022, James Blose was an attorney and held high-ranking positions, including General Counsel, at Hudson Valley Bank and Sterling National Bank in Connecticut.

From approximately January 2022, when Webster Bank acquired Sterling National Bank, until February 2023, Blose served as Executive Vice President and General Counsel and Corporate Secretary at Webster Bank.

From approximately 2013 until Webster Bank discovered his scheme and his employment was terminated in February 2023, Blose defrauded his employers (The Bank) in various ways.

In certain commercial loan transactions where The Bank was the lender, Blose fraudulently retained for himself portions of closing costs, including legal fees.

In certain real estate transactions in which The Bank was the seller, Blose retained portions of the sale proceeds for himself. For some of the real estate transactions, Blose created false documents in order to hide his theft from The Bank. Blose also stole from The Bank in other ways.

As part of the scheme, Blose used his attorney trust accounts to make personal expenditures, and to transfer funds to accounts in the names of business entities he created and controlled, and then used those funds for his personal benefit. Through this scheme, Blose stole approximately $7.4 million from his employers, and used the stolen funds to purchase a vacation property on Kiawah Island in South Carolina, for construction of his Connecticut home, and for luxury vehicles, jewelry, private jets charters, multiple country club memberships, and other expenses. (Source)

Bank Executive Pleads Guilty To $3.5 Million+ Wire Fraud Scheme - April 18, 2025

Russell Laffitte was an officer and executive at Palmetto State Bank in Hampton, South Carolina. His co-conspirator, Alex Murdaugh, was a personal injury attorney at a law firm in Hampton.

Laffitte admitted that he agreed to serve as conservator and personal representative for several of Murdaugh's clients, knowing that he would personally profit from doing so. Beginning in 2011, Laffitte began extending himself and Murdaugh loans from conservator accounts Laffitte was charged with managing. Laffitte did not disclose the loans to the conservatees, despite owing them a fiduciary duty.

Around that time, Murdaugh devised a scheme to obtain money belonging to his clients. In furtherance of the scheme, Murdaugh directed law firm employees to make clients' checks payable to Palmetto State Bank. The checks were drawn on the law firm's client trust account, identified the clients on the memo lines, and corresponded to amounts set forth in the clients' disbursement sheets.

As to two of Murdaugh's clients, Laffitte—their conservator—saw their disbursement sheets and knew that the bank was supposed to receive their settlement funds. Murdaugh presented the clients' checks to Laffitte and directed that they be used for Murdaugh's personal benefit, including to pay off loans Laffitte had extended from conservator accounts. Laffitte negotiated nine separate transactions for Murdaugh's benefit, knowing that the funds belonged to the clients.

Laffitte also aided and abetted the structuring of transactions from a second check belonging to one of the clients, disbursing the funds at Murdaugh's direction and for Murdaugh's personal benefit.

As to a third client of Murdaugh's, Laffitte negotiated 12 separate transactions, disbursing $1,325,000 in client settlement funds for Murdaugh's benefit.

Despite knowing they were client funds, Laffitte allowed Murdaugh to use the funds to repay Murdaugh's personal loans, repay loans Laffitte extended from a conservator account, purchase vehicles and equipment, and receive cash back. Laffitte also deposited some of the funds into Murdaugh's personal account.

In 2015, Laffitte misapplied bank funds by extending over $284,000 from a line of credit that was supposed to be for farming to repay Murdaugh's remaining loans from the conservatorship.

Laffitte also misapplied bank funds on two other occasions. In July 2021, he extended Murdaugh a $750,000 loan for the stated purpose of beach house renovations.

But Laffitte authorized a $350,000 wire transfer to an attorney and then transferred $400,000 of "loan proceeds" to Murdaugh's account to cover over $367,000 in overdraft, knowing that these funds had nothing to do with beach house renovations.

In October 2021, the law firm uncovered that Murdaugh had stolen from clients. Laffitte knew he had negotiated stolen checks at Murdaugh's direction despite knowing the funds did not belong to Murdaugh. Laffitte then paid the law firm $680,000 in bank funds without the knowledge or consent of the full bank Board of Directors or Executive Committee in an attempt to settle the matter with the law firm.

Under the terms of the plea agreement, Laffitte agrees to pay $3,555,884.80 in criminal restitution before sentencing. Laffitte also agrees that his guilty plea prohibits him from controlling or participating in the conduct of any federally insured bank or credit union, and he cannot serve as a director or officer of any such bank or credit union without permission. (Source)

Bank Vice President Charged In $1.9 Million+ Fraud Scheme - April 9, 2025

Andrew Blassie served as the Executive Vice President for the Bank of O'Fallon in Illinois. He is charged with defrauding the bank out of $1,972,887.67 in a check kite scheme from September 2023 through September 2024 during his employment.

Blassie is accused of falsely inflating the balance of his personal checking account at the Bank of O'Fallon by depositing checks he knew to be backed by non-sufficient funds.

He allegedly deposited checks with non-sufficient funds from four personal accounts at three other banks and one credit union into the Bank of O'Fallon account.

The indictment alleges Blassie paid nearly $2.7 million for personal expenses from the falsely inflated account thus using funds belonging to the Bank of O'Fallon.

As the former Executive Vice President, Blassie is accused of using his position to conceal his fraud from the Bank of O'Fallon by scrubbing his name and account number from the suspected kiting reports.

From August 2022 through September 2024, Blassie is also accused of persuading a couple from Lebanon, Illinois, to give him $429,000 of their retirement savings. In return for this investment, Blassie gave the couple two promissory notes. He agreed to pay the couple interest on the notes and used money he obtained through his check kite scheme to pay some of that interest. As security for his promissory notes, Blassie pledged 128 of his and his wife's shares of the holding company which owns the Bank of O'Fallon.

According to the indictment, Blassie later sold most of these shares and did not use those funds to repay the Lebanon couple. This left the couple with no means of recourse when Blassie later defaulted on the promissory notes. (Source)

Credit Union Employee Sentenced To Prison For Stealing $300,000+ From Elderly Customers - April 24, 2025

Tyra Brown was a customer service representative for a New Hampshire credit union. Because of her job, Brown could access customers' personal identifying information, security questions and answers, and account balances. She was only permitted to access customer account information for business purposes, such as to answer customer questions on calls.

Brown used that access to steal $301,674.89 from at least 10 elderly victims and attempted to steal $428,526.85 in total. Brown used wires, electronic debits, and Zelle to transfer victim funds to other accounts. (Source)

Former Bank Officer Pleads Guilty To Embezzling $122,000+ / Used Funds For Gambling, Paying Debt, Retail Purchases - April 10, 2025

Edward Jenkinson was employed as a bank officer at Bank 1, an FDIC insured institution that was a member bank of the Federal Home Loan Bank of Atlanta.

As a bank officer, Jenkinson was responsible for managing a Bank 1 financial center located in Tampa. One of Jenkinson's duties was to oversee the Automated Teller Machine (ATM) and teller cash drawers at the financial center.

Between March and November 2024, Jenkinson embezzled FDIC-insured funds. As part of his embezzlement scheme, Jenkinson redeemed certificates of deposit without the customers' knowledge or consent. He then prepared deposit tickets and deposited the redeemed funds in customer checking accounts.

Subsequently, Jenkinson embezzled the funds from the victim customers' accounts and drafted cashiers' checks payable to himself, which he deposited into his own bank accounts. Jenkinson depleted most of the embezzled funds through cash withdrawals. He also embezzled $52,000 from the ATM machine at the Bank 1 financial center he managed in Tampa, as well as $2,500 from a bank teller drawer. Jenkinson spent the embezzled funds on gambling, paying off debt, and retail purchases. (Source)

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

2 Laboratory Sales Executives Sentenced To Prison For Roles In $997,000+ Health Care Kickback Conspiracy - April 25, 2025

Stephen Kash was ordered to forfeit $779,773.70 in criminal proceeds.

Courtney Love was ordered to forfeit $217,268.75 in criminal proceeds.

Two rural Texas hospitals, Little River Healthcare (LRH) based in Rockdale, and Stamford Memorial Hospital based in Stamford, partnered with True Health Diagnostics (THD), a clinical laboratory based in Frisco, Texas, that specialized in advanced cardiovascular lipid testing. For a fee, THD processed the blood tests while the hospitals billed the tests to insurers as hospital outpatient services, with the hospitals charging insurers a much higher rate than THD could receive as a clinical laboratory. The hospitals utilized a network of marketers who in turn operated management services organizations (MSOs) that offered investment opportunities to physicians throughout the State of Texas. In reality, the MSOs were simply a means to facilitate payments to physicians in return for the physicians' laboratory referrals. Pursuant to the kickback scheme, the hospitals paid a portion of their laboratory revenues to marketers, who in turn kicked back a portion of those funds to the referring physicians who ordered THD tests. THD executives and sales force personnel leveraged the MSO kickbacks to gain and increase referrals and, in turn, to increase their revenues, bonuses, and commissions. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

CHINESE / NORTH KOREA FOREIGN GOVERNMENT ESPIONAGE / THEFT OF TRADE SECRETS INVOLVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

Company Bookkeeper Sentenced To Prison For Embezzling $865,000+ Over 6 Years - April 9, 2025

Jennifer Cormier was employed at a family-owned business offering plumbing, heating, and air conditioning services in Naugatuck, Connecticut where she performed bookkeeping and other office-related tasks.

Between approximately 2017 and July 2023, Cormier stole from her employer by fraudulently creating approximately 1,000 checks made payable to her and to cash. She forged the signature of the company's owner or used the owner's signature stamp on the checks, and then cashed them or deposited them into her personal bank account. After the checks were issued, she deleted the transaction in company's accounting system. Cormier embezzled a total of $865,106.17. (Source)

Automotive Dealership Senior Accountant Convicted Of Embezzling $535.000+ - April 1, 2025

From November of 2018 through May of 2023, Sehrelina Tardo was a senior accountant at a car dealership in New Orleans.

Tardo embezzled customer cash down payments and deposits, taking the funds for herself. Tardo hid her theft by creating fake journal entries of customer transactions on her employer's books and records. Tardo agreed to pay restitution of $535,750.77 to her former employer. (Source)

Company Accounting Specialist Sentenced To Prison For Embezzling $480,000+ - April 18, 2025

Between March 2021 and July 2022, Rhonda Canidate was employed as an accounting specialist at Henry Molded Products Company (Henry Molded) in Lebanon, Pennsylvania.

Between October 2021 and June 2022, Canidate entered false payment entries for former Henry Molded employees into Henry Molded's third-party payroll software, causing the software to issue direct deposit payments from Henry Molded's bank account to bank accounts controlled by Canidate in the name of the former employees. This fraud not only financially injured Henry Molded, but it also harmed the former employees by creating an overpayment for tax purposes. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMENT AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBT PROBLEMS

Information Technology Manager Charged For Stealing $950,000+ From Employer / Used Funds For Personal Expenses - April 11, 2025

Paul Welch worked for Algas-SDI, a energy manufacturing company, from 2011 to 2024. He was promoted to Information Technology Manager in 2018.

Welch used various schemes to steal more than $950,000 from the company.

In early 2017, Welch used the company's Amazon business account to make unauthorized personal purchases from Amazon. Between 2017 and 2023, those purchases totaled at least $43,000. Welch primarily purchased electronics such at televisions, laptops and more—all for personal use.

In 2019, Welch began using his company credit card for personal purchases through other online retailers such as Apple, Alaska Airlines, Instacart and BestBuy. Between 2019 and 2024, those unauthorized personal purchases totaled at least an additional $60,000.

The scheme really accelerated in January 2021 when Welch began making payments to himself disguised as payments to a computer services company. Welch allegedly created a series of email addresses and payment processor accounts using a business name that was very similar to a legitimate computer services company based in Washington State. Welch then used Algas-SDI company credit cards to pay the computer services company under the guise that the company was providing IT equipment and services to Algas-SDI. However, the legitimate computer services company had no relationship with Welch and never provided any services or equipment to Algas-SDI. The credit card payments Welch made from Algas-SDI's credit cards went directly to the payment processor accounts that Welch controlled. Between 2021 and 2024 Welch allegedly used this scheme to transfer approximately $879,175 from company accounts to his own accounts. (Source)

Director Of Finance For Charity Admits To Stealing $690,000+ For Over 10 Years / Used Funds For Rent Payments, Travel, Etc. - April 1, 2025

Joelle Fouse was the manager / director of finance and human resources for the charity and was responsible for payroll, expense reimbursement and maintaining the charity's books and records. She admitted stealing from the charity in multiple ways.

Fouse caused 181 unauthorized expense payments totaling $407,186 to be transferred into bank accounts she controlled by providing false expense reimbursement information to a third-party payroll processing company. She provided false payroll information that triggered 71 other unauthorized payments totaling $139,810. Her theft, and the unauthorized payments, caused the charity to overpay payroll taxes by approximately $10,694.

Fouse also used her company credit card to make 184 unauthorized purchases totaling $133,210. She attempted to cover up her crimes by falsifying financial and accounting records. Fouse admitted to embezzling about $690,000 over more than a decade.

Fouse admitted using the money to pay for personal expenses for herself and relatives including travel, clothing, entertainment, restaurants and rent payments. Fouse's fraud limited the charity's ability to provide services to the disabled adults it served. (Source)

Fouse worked for the charity from October 2012 through December 2023, when she was terminated and her employer contacted federal authorities. (Source)

Executive Director For Non-Profit Pleads Guilty To Embezzling $500,000+ / Used Fund For Vacations, Etc. - April 24, 2025

Howard Solomon, 38, served as the Executive Director of East Oakland Boxing Association (EOBA) from late 2016 until 2021. EOBA is a non-profit organization that serves low-income youths in neighborhoods and communities through a variety of programming, including after-school boxing lessons.

Solomon admitted to a multi-year mail fraud scheme in which he embezzled at least $549,000 from his former employer.

After being added in September 2016 as an authorized signatory on EOBA bank accounts at Wells Fargo Bank, Solomon transferred EOBA funds out of the Wells Fargo accounts into accounts he controlled at other banking institutions. He also deposited charitable contributions to EOBA into the accounts he controlled, some of which were business accounts and others of which were his personal accounts. Solomon acknowledged that he took these actions without informing or seeking authority from EOBA board members or any other person affiliated with EOBA.

Solomon used the embezzled funds and donations to pay for personal expenses that had no connection to his job, including vacation expenses, a Ford Explorer, and Amazon purchases for personal use. (Source)

Company Bookkeeper Sentenced To Prison For Embezzling $330,000+ By Depositing Funds Into Her Personal Bank Account - April 21, 2025

Erin Jones worked part-time at a small business in Baton Rouge, Louisiana, that provided truck and diesel engine repair services. Jones was trusted to assist with the company's book-keeping and accounting, among other tasks. Jones held bank accounts at JPMorgan Chase Bank and Hancock Whitney Bank and the company also maintained a business bank account at Hancock Bank.

Beginning in or about May of 2019 and continuing through April of 2024, Jones knowingly executed a scheme to defraud the company and to obtain money by means of materially false and fraudulent pretenses, representations, and promises.

One of Jones' job responsibilities was to retrieve the company's mail from a post office box that the company maintained in Baton Rouge. Using her access to the post office box, she would retrieve checks that had been issued to the company and mailed to the company by its customers. The checks were drawn on the customers' bank accounts at banks located across the country. After gaining control of each check, Jones would endorse the back of the check and deposit it into one of her own personal bank accounts, either by using an ATM or making a remote online deposit.

Jones concealed her scheme in several ways. On many occasions, she would use her access to the company's accounting program to delete the underlying invoices that caused the company's customers and vendors to make the payments.

Over the course of the scheme, Jones embezzled and fraudulently deposited approximately 431 checks payable to the company, totaling approximately $334,000. (Source)

Employee Pleads Guilty To Embezzling $305,000+ / Used Funds To Purchase New Car - April 15, 2025

Jennifer Cabral admitted that she stole approximately $306,034.28 from her employer's bank account and used those funds for her personal benefit and use.

Cabral accessed her employer's accounting software and directed payments to her own personal bank accounts through the employer's online account at a local financial institution. Cabral used those funds for various personal benefits including vehicle payments toward the purchase of her car, which was forfeited as part of the plea agreement. (Source)

Company Bookkeeper Sentenced To Prison For Using Company Funds To Pay His Personal Credit Card Bills - April 23, 2025

David Tetreault worked as a bookkeeper for a Massachusetts-based electrical contractor between 2015 and 2021.

During those years, Tetreault received wages in cash and used company funds to pay his personal credit card bills. Tetreault manipulated the company's accounting records and bank statements to disguise these payments as business expenses. As a result of this conduct, Tetreault underreported his personal income by at least $2.1 million, causing a loss to the IRS of over $600,000.

In addition, Tetreault did not report his work for the electrical contractor or his income to the Social Security Administration and submitted false information about his employment and income to the Employees' Retirement System of Rhode Island (ERSRI). As a result of this conduct, Tetreault collected over $320,000 in Social Security Disability Insurance benefits and ERSRI disability pension benefits to which he was not entitled between 2016 and 2024.

Tetreault has been ordered to pay $623,602 to the Internal Revenue Service, $159,816 to the Social Security Administration and $161,835 to the Employment Retirement System of Rhode Island in restitution. (Source)

Popeyes Chicken Employee Arrested For Stealing Customer's Credit Card Information And Sending Money To Prison Inmate - April 15, 2024

According to the Flagler County Sheriff's Office in Florida, a customer reported seeing an employee at Popeye's in Palm Coast tapping her credit card twice while in the drive-thru last month, once for her order and then again to a cell phone.

Detectives discovered that the Popeye's employee, identified as 48-year-old Chaniqua Richberg, used the victim's money to make a commissary payment to an inmate at a correctional institution. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL THEIR EMPLOYERS MONEY TO SUPPORT THEIR PERSONAL BUSINESS

Former Rail Systems Assistant Chief Engineer Pleads Guilty Defrauding Company Of $8.5 Million Through False Invoicing Scheme That Benefited His Business - April, 18, 2025

John Pigsley is the former Assistant Chief Engineer of Facilities for Keolis Commuter Services (Keolis).

Pigsley pleaded guilty to defrauding Keolis of over $8 million.

Keolis has operated the MBTA commuter rail system since 2014 under an annual contract of $291–$349 million.

Between 2014 and November 2021, Pigsley was employed as Keolis' Assistant Chief Engineer of Facilities and was responsible for the maintenance of MBTA Commuter Rail Facilities and their engineering operations, including corrective repair and project management for assets and maintenance and ordering and approving his subordinates' orders of electrical supplies from outside vendors for Keolis.

Pigsley also operated a separate construction company called Pigman Group. Rafferty was the general manager of LJ Electric, Inc., an electrical supply vendor to which Keolis paid over $17 million between 2014 through 2021.

Between July 2014 and November 2021, Pigsley and Rafferty defrauded Keolis of over $4 million through a false LJ Electric invoicing scheme.

Specifically, Rafferty purchased vehicles, construction equipment, construction supplies and other items for Pigsley, Pigman Group and others, and Pigsley directed Rafferty to recover the cost of these items by submitting false and fraudulent LJ Electric invoices to Keolis.

Rafferty spent more than $3 million on items for Pigsley and others – including: at least nine trucks; construction equipment including at least seven Bobcat machines; at least $1 million in home building supplies and services; and a $54,000 camper– for which Keolis paid Rafferty more than $4 million based on false LJ Electric invoices.

In addition to the false invoicing scheme, Pigsley directed Keolis to purchase copper wire which he then stole and sold to scrap metal businesses, keeping the cash proceeds for himself. To conceal the theft, Pigsley personally picked up the copper wire orders from vendors or had the orders delivered to his Beverly home. Pigsley then personally transported the wire to scrap yards where he traded it for thousands of dollars in cash several times a month and sometimes more than once a day. Pigsley obtained more than $4.5 million in cash by stealing and scrapping the copper wire. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Employee Sentenced To Prison For $4 Million+ Fraudulent Invoices Scheme Over 5 Years - April 14, 2025

While Madelyn Hernandez was employed by a textile and apparel supply chain company, she made false and fraudulent representations to the company to obtain money. Hernandez submitted fraudulent invoices via email from purported fabric supply companies and directed payment be sent to bank accounts that she controlled. As part of her scheme, Hernandez created and submitted false invoices purporting money due and owing to a fictitious company and another that was a defunct company for goods purportedly ordered and received. As a result of her scheme, between 2018 and 2024, Hernandez received a total of $4,199,498.42 from her employer.

Hernandez's fraud came to light after the owner of the company found discrepancies in the company's financial records, including inventory discrepancies and falsified business records.

In June 2024, the company became aware that invoices, proof of delivery records, and inventory reports that Hernandez had submitted were fraudulent. As the company was investigating and unraveling the fraudulent records, Hernandez sent a message to her employer from a purported family member stating that she had died after an illness and complications with surgery. The company contacted law enforcement.

In October 2024, agents with the FBI and IRS Criminal Investigation executed a search warrant at Hernandez's residence.

Hernandez admitted to agents that she had emailed invoices to the company for payment and had used the money deposited into her account, held in a fictitious company name, for her own personal expenses and for gambling. Further, she admitted to sending the message to her employer stating that she had died. (Source)

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

Cybersecurity Firm CEO Charged With Installing Malware On Hospital Computer To Most Likely Get Business - April 18, 2025

The CEO of an Edmond, OK-based cybersecurity firm has been accused of intentionally installing malware at an Oklahoma City hospital. On August 6, 2024, a member of staff at SSM Health's St. Anthony Hospital observed a man using a hospital computer that had been designated for employee use only. The man was apprehended by staff and questioned, and explained that a family member was undergoing surgery at the hospital and he needed to use the computer.

The hospital launched an investigation to identify the nature of the unauthorized activity and reviewed security camera footage. The man was observed attempting to access multiple offices in the hospital and using two hospital computers, one of which was for employee use only. The forensic investigation confirmed that malware had been installed on the computer. The malware was programmed to take screenshots every 20 seconds and transmit the images to an external IP address.

Law enforcement was notified about the unauthorized computer access and malware infection. The identity of the man was established and determined to be Jeffrey Bowie, the CEO of a cybersecurity firm that offers cybersecurity services such as digital forensics and incident response. An arrest warrant was issued, and Bowie was arrested by Oklahoma City police. He has since been charged with two counts of violating the Oklahoma Computer Crimes Act." (Source)

Employee Sentenced To Prison For Conducting Cyber Intrusions Against His Former Employer Following His Termination - April 24, 2025

Michael Scheuer conducted a series of computer intrusions or attacks directed at his former employer following his termination. These intrusions included manipulating allergen information in restaurant menus to indicate that food items were safe for customers with certain allergies, when they were not. Scheuer also altered menu information related to wine regions to reflect locations of recent mass shootings. Additionally, Scheuer launched denial-of-service attacks designed to lock certain company employees out of their accounts.

The court ordered Scheuer to pay $687,776.50 in restitution to the victims of his crimes. (Source)

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Nurse Working For Outpatient Surgical Center Admits To Stealing Fentanyl - April 7, 2025

Kristen Carotenuto was employed as a nurse at an outpatient surgical center in Stamford, Connecticut. As part of her employment, she was granted access to a secure location used by the surgical center to store controlled substances, including hydromorphone and fentanyl.

In December 2024, Carotenuto removed several vials, each containing hydromorphone or fentanyl, from the secure storage area. She then took the vials home, removed the controlled substances using a syringe, and used the drugs. She then refilled the vials with either saline or water and returned the tampered vials to the storage area in a location where they could be distributed for patient use. (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

No Incidents To Report

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

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

No Incidents To Report

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.

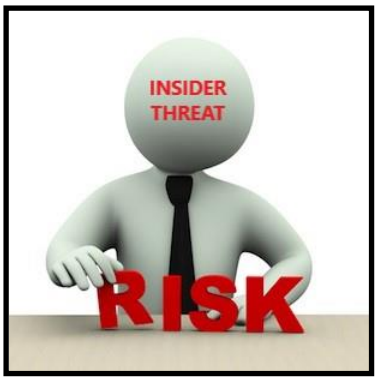
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

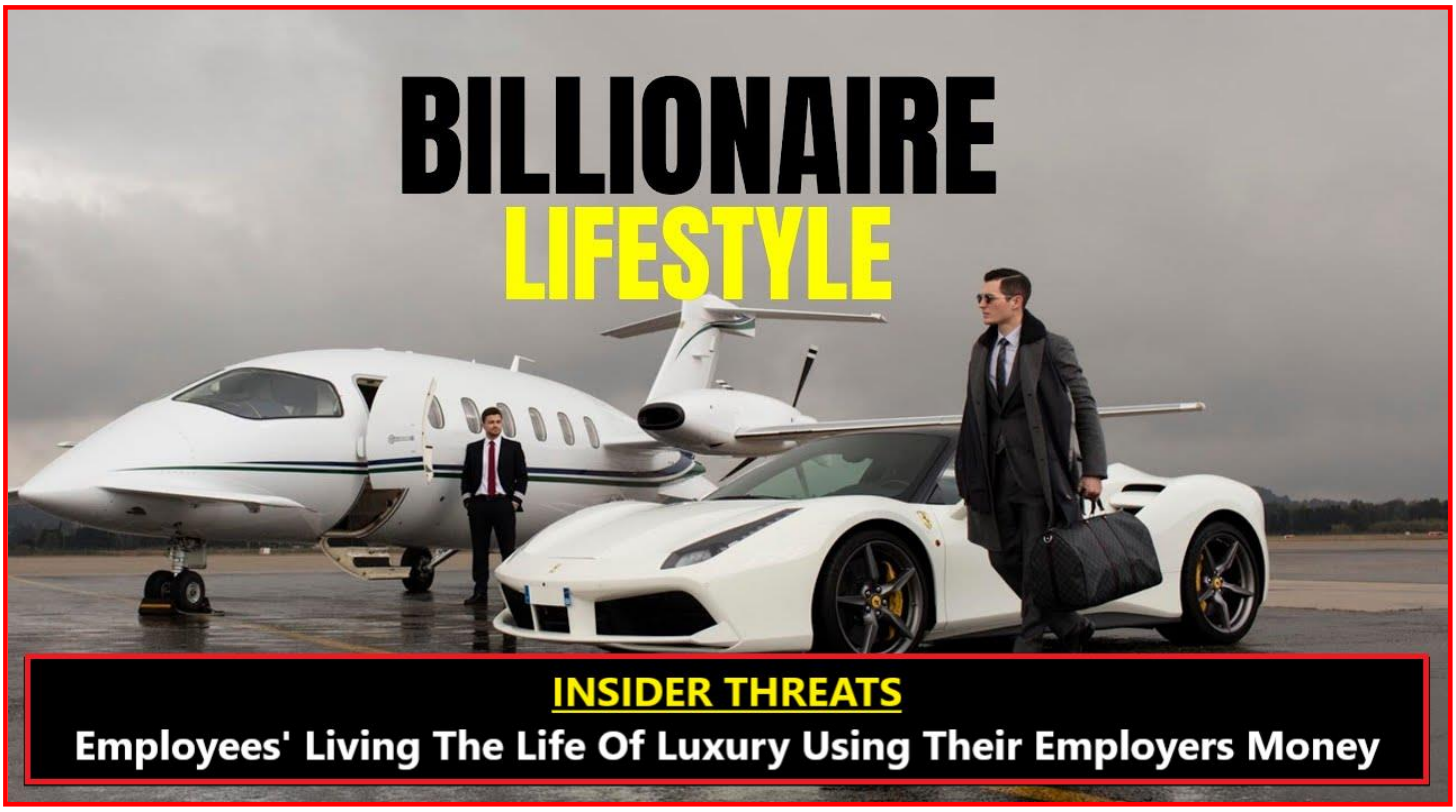
- ☐ Bribery, Extortion, Blackmail

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 WERE THE 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 FRAUD

2 Former Employees Of Mortgage Lending Business Charged For Roles In $3 BILLION Mortgage Fraud Scheme - November 13, 2024

Christopher Gallo and Mehmet Ali Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business.

Gallo was a senior loan officer and Elmas was a mortgage loan officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties. By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than approximately $3 billion in loans. (Source)

TD Bank Pleads Guilty To Money Laundering Conspiracy By Bribed Employees / FINED $1.8 BILLION - October 10, 2024

TD Bank failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than $670 million through TD Bank accounts between 2019 and 2023.

Between January 2018 and February 2021, one money laundering network processed more than $470 million through the bank through large cash deposits into nominee accounts. The operators of this scheme provided employees gift cards worth more than $57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over $10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports.

In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million through shell accounts before TD Bank reported the activity.

In a third scheme, money laundering networks deposited funds in the United States and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately $39 million. The Justice Department has charged over two dozen individuals across these schemes, including two bank insiders. (Source)

Former Wells Fargo Executive Pleads Guilty To Opening Millions Of Accounts Without Customer Authorization - Wells Fargo Agrees To Pay $3 BILLION Penalty - March 15, 2023

The former head of Wells Fargo Bank's retail banking division (Carrie Tolstedt) has agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 BILLION penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding." (Source)

Former Company Chief Investment Officer Pleads Guilty To Role In $3 BILLION Of Securities Fraud / Company Pays $2.4 BILLION Fine - June 7, 2024

Gregorie Tournant is the former Chief Investment Officer and Co-Lead Portfolio Manager for a series of private investment funds managed by Allianz Global Investors (AGI).

Between 2014 and 2020, Tournant the Chief Investment Officer of a set of private funds at AGI known as the Structured Alpha Funds.

These funds were marketed largely to institutional investors, including pension funds for workers all across America. Tournant and his co-defendants misled these investors about the risk associated with their investments. To conceal the risk associated with how the Structured Alpha Funds were being managed, Tournant and his co-defendants provided investors with altered documents to hide the true riskiness of the funds' investments, including that investments were not sufficiently hedged against risks associated with a market crash.

In March 2020, following the onset of market declines brought on by the COVID-19 pandemic, the Structured Alpha Funds lost in excess of $7 Billion in market value, including over $3.2 billion in principal, faced margin calls and redemption requests, and ultimately were shut down.

On May 17, 2022, AGI pled guilty to securities fraud in connection with this fraudulent scheme and later was sentenced to a pay a criminal fine of approximately $2.3 billion, forfeit approximately $463 million, and pay more than $3 billion in restitution to the investor victims. (Source)

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Paying $1.6 BILLION In Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

Ng Chong Hwa, also known as "Roger Ng," a citizen of Malaysia and a former Managing Director of The Goldman Sachs Group, Inc., was was sentenced to 10 years in prisont for conspiring to launder BILLIONS of dollars embezzled from 1Malaysia Development Berhad (1MDB), conspiring to violate the Foreign Corrupt Practices Act (FCPA) by paying more than $1.6 BILLION in bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

1MDB is a Malaysian state-owned and controlled fund created to pursue investment and development projects for the economic benefit of Malaysia and its people.

Between approximately 2009 and 2014, Ng conspired with others to launder billions of dollars misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions it executed with Goldman Sachs, known as "Project Magnolia," "Project Maximus," and "Project Catalyze." As part of the scheme, Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite also known as "Jho Low," conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

They also conspired to launder the proceeds of their criminal conduct through the U.S. financial system by funding major Hollywood films such as "The Wolf of Wall Street," and purchasing, among other things, artwork from New York-based Christie's auction house including a $51 million Jean-Michael Basquiat painting, a $23 million diamond necklace, millions of dollars in Hermes handbags from a dealer based on Long Island, and luxury real estate in Manhattan.

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

Boeing Charged With 737 Max Fraud Conspiracy Agrees To Pay Over $2.5 BILLION In Penalties Because Of Employees Fraudulent And Deceptive Conduct - January 11, 2021

Aircraft manufacturer Boeing has agreed to pay over $2.5 billion in penalties as a result of "fraudulent and deceptive conduct by employees" in connection with the firm's B737 Max aircraft crashes.

"The misleading statements, half-truths, and omissions communicated by Boeing employees to the FAA impeded the government's ability to ensure the safety of the flying public," said U.S. Attorney Erin Nealy Cox for the Northern District of Texas.

As Boeing admitted in court documents, Boeing through two of its 737 MAX Flight Technical Pilots deceived the FAA about an important aircraft part called the Maneuvering Characteristics Augmentation System (MCAS) that impacted the flight control system of the Boeing 737 MAX. Because of their deception, a key document published by the FAA lacked information about MCAS, and in turn, airplane manuals and pilot-training materials for U.S.-based airlines lacked information about MCAS.

On Oct. 29, 2018, Lion Air Flight 610, a Boeing 737 MAX, crashed shortly after takeoff into the Java Sea near Indonesia. All 189 passengers and crew on board died.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 MAX, crashed shortly after takeoff near Ejere, Ethiopia. All 157 passengers and crew on board died. (Source)

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than $1.4 billion in loans. (Source)

Member Of Supervisory Board Of State Employees Federal Credit Union Pleads Guilty To $1 BILLION Scheme Involving High Risk Cash Transactions - January 31, 2024

A New York man pleaded guilty today to failure to maintain an anti-money laundering program in violation of the Bank Secrecy Act as part of a scheme to bring lucrative and high-risk international financial business to a small, unsophisticated credit union.

From 2014 to 2016, Gyanendra Asre of New York, was a member of the supervisory board of the New York State Employees Federal Credit Union (NYSEFCU), a financial institution that was required to have an anti-money laundering program. Through the NYSEFCU and other entities, Asre participated in a scheme that brought over $1 billion in high-risk transactions, including millions of dollars of bulk cash transactions from a foreign bank, to the NYSEFCU.

In addition, Asre was a certified anti-money laundering specialist who was experienced in international banking and trained in anti-money laundering compliance and procedures, and represented to the NYSEFCU that he and his businesses would conduct appropriate anti-money laundering oversight as required by the Bank Secrecy Act. Based on Asre's representations, the NYSEFCU, a small credit union with a volunteer board that primarily served New York state public employees, allowed Asre and his entities to conduct high-risk transactions through the NYSEFCU. Contrary to his representations, Asre willfully failed to implement and maintain an anti-money laundering program at the NYSEFCU. This failure caused the NYSEFCU to process the high-risk transactions without appropriate oversight and without ever filing a single Suspicious Activity Report, as required by law. (Source)

Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024

3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the world. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Pearce concealed the fraud scheme for many years by using these privileges to alter information about the accounts, which helped hide his creation of unauthorized license keys. Dusti Pearce handled accounting for the illegal business.

Hines operated Direct Business Services International (DBSI), a New Jersey-based business communications systems provider and a de-authorized Avaya reseller. He bought ADI software license keys from Brad and Dusti Pearce and then sold them to resellers and end users around the world for significantly below the wholesale price. Hines was by far the Pearces' largest customer and significantly influenced how the scheme operated. Hines was one of the biggest users of the ADI license system in the world.

To hide the nature and source of the money, the Pearces funneled their illegal gains through a PayPal account created under a false name to multiple bank accounts, and then transferred the money to investment and bank accounts. They also purchased large quantities of gold bullion and other valuable items. (Source)

COLLUSION – HOW MANY EMPLOYEES' OR INDIVIDUALS CAN BE INVLOVED?

193 Individuals Charged (Doctors, Nurses, Medical Professionals) For Participation In $2.75 BILLION Health Care Fraud Schemes - June 27, 2024

The Justice Department today announced the 2024 National Health Care Fraud Enforcement Action, which resulted in criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

In connection with the coordinated nationwide law enforcement action, and together with federal and state law enforcement partners, the government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication; over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

2 Executives Who Worked For a Geneva Oil Production Firm Involved In Misappropriating $1.8 BILLION - April 25, 2023

The former Petrosaudi employees are suspected of having worked with Jho Low, the alleged mastermind behind the scheme, to set up a fraudulent deal purported between the governments of Saudi Arabia and Malaysia, according to a statement from the Swiss Attorney General.

1MDB was the Malaysian sovereign wealth fund designed to finance economic development projects across the southeastern Asian nation but become a byword for scandal and corruption that triggered investigations in the US, UK, Singapore, Malaysia, Switzerland and Canada.

Low, currently a fugitive whose whereabouts are unknown, has previously denied wrongdoing. His playboy lifestyle was financed with money stolen from 1MDB, according to US prosecutors.

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 billion in financing from 1MDB, according to Swiss prosecutors. The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

The allegations cover a period at least from 2009 to 2015 and the duo have been indicted for commercial fraud, aggravated criminal mismanagement and aggravated money laundering. (Source)

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION in Health Care Fraud Scheme - June 28, 2023

The Justice Department, together with federal and state law enforcement partners, announced today a strategically coordinated, two-week nationwide law enforcement action that resulted in criminal charges against 78 defendants for their alleged participation in health care fraud and opioid abuse schemes that included over $2.5 Billion in alleged fraud. The enforcement action included charges against 11 defendants in connection with the submission of over $2 Billion in fraudulent claims resulting from telemedicine schemes.

In a case involving the alleged organizers of one of the largest health care fraud schemes ever prosecuted, an indictment in the Southern District of Florida alleges that the Chief Executive Officer (CEO), former CEO, and Vice President of Business Development of purported software and services companies conspired to generate and sell templated doctors' orders for orthotic braces and pain creams in exchange for kickbacks and bribes. The conspiracy allegedly resulted in the submission of $1.9 Billion in false and fraudulent claims to Medicare and other government insurers for orthotic braces, prescription skin creams, and other items that were medically unnecessary and ineligible for Medicare reimbursement. (Source)

10 Individuals (Hospital Managers And Others) Charged In $1.4 BILLION Hospital Pass - Through Billing Scheme - June 29, 2020

10 individuals, including hospital managers, laboratory owners, billers and recruiters, were charged for their participation in an elaborate pass-through billing scheme using rural hospitals in several states as billing shells to submit fraudulent claims for laboratory testing.

The indictment alleges that from approximately November 2015 through February 2018, the conspirators billed private insurance companies approximately $1.4 billion for laboratory testing claims as part of this fraudulent scheme, and were paid approximately $400 million. (Source)

Former University Financial Advisor Sentenced To Prison For $5.6 Million+ Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee.

As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied.

Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

3 Bank Board Members Of Failed Bank Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged - 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)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman.

Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

TRADE SECRET THEFT

Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION - May 2, 2022

Gongda Xue worked as a scientist at the Friedrich Miescher Institute for Biomedical Research (FMI) in Switzerland, which is affiliated with Novartis. His sister, Yu Xue, worked as a scientist at GlaxoSmithKline (GSK) in Pennsylvania. Both Gongda Xue and Yu Xue conducted cancer research as part of their employment at these companies.

While working for their respective entities, Gongda Xue and Yu Xue shared confidential information for their own personal benefit.

Gongda Xue created Abba Therapeutics AG in Switzerland, and Yu Xue and her associates formed Renopharma, Ltd., in China. Both companies intended to develop their own biopharmaceutical anti-cancer products.

Gongda Xue stole FMI research into anti-cancer products and sent that research to Yu Xue. Yu Xue, in turn, stole GSK research into anti-cancer products and sent that to Gongda Xue. Yu Xue also provided hundreds of GSK documents to her associates at Renopharma. Renopharma then attempted to re-brand GSK products under development as Renopharma products and attempted to sell them for billions of dollars. Renopharma's own internal projections showed that the company could be worth as much as $10 billion based upon the stolen GSK data. (Source)

U.S. Brokerage Firm Accuses Rival Firm Of Stealing Trade Secrets Valued At Over $1 BILLION - November 14, 2023

U.S. brokerage firm BTIG sued rival StoneX Group, accusing it of stealing trade secrets and seeking at least $200 million in damages.

StoneX recruited a team of BTIG traders and software engineers to exfiltrate BTIG software code and proprietary information and take it to StoneX, according to lawyers for BTIG.

StoneX used the software code and proprietary information to build competing products and business lines that generate tens of millions of dollars annually, they alleged in the lawsuit.

BTIG said in the lawsuit that StoneX had committed one of the greatest financial industry trade secret frauds in recent history, and that the scope of its misconduct is not presently known, and may easily exceed a billion dollars."

The complaint said StoneX hired several BTIG employees to steal confidential information that it used to develop its competing trading platform.

The complaint said that StoneX's stock price has increased 60% since it started misusing BTIG's trade secrets. (Source)

U.S. Petroleum Company Scientist Sentenced To Prison For $1 BILLION Theft Of Trade Secrets - Was Starting New Job In China - May 27, 2020

When scientist Hongjin Tan resigned from the petroleum company he had worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.

But Tan told a colleague a different story over dinner. He revealed to his colleague that he actually did have a job waiting for him in China. Tan's dinner companion reported the conversation to his supervisor. That conversation prompted Tan's employer to ask him to leave the firm immediately, and his employer made a call to the FBI tip line to report a possible crime.

Tan called his supervisor to tell them he had a thumb drive with company documents on it. The company told him to return the thumb drive. When he brought back the thumb drive, the company looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about. (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)

CEO Of Bank Sentenced To Prison For $47 Million Fraud Scheme That Caused Bank To Collapse - August 19, 2024

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering."

The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (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)

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (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 Role in $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)

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)

WORKPLACE VIOLENCE
Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024
Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

Between May and August 2022, numerous patients at Surgicare North Dallas suffered cardiac emergencies during routine medical procedures performed by various doctors. About one month after the unexplained emergencies began, an anesthesiologist who had worked at the facility earlier that day died while treating herself for dehydration using an IV bag. In August 2022, doctors at the surgical care center began to suspect tainted IV bags had caused the repeated crises after an 18-year-old patient had to be rushed to the intensive care unit in critical condition during a routine sinus surgery.

A local lab analyzed fluid from the bag used during the teenager's surgery and found bupivacaine (a nerve-blocking agent), epinephrine (a stimulant) and lidocaine (an anesthetic) — a drug cocktail that could have caused the boy's symptoms, which included very high blood pressure, cardiac dysfunction and pulmonary edema. The lab also observed a puncture in the bag.

Ortiz surreptitiously injected IV bags of saline with epinephrine, bupivacaine and other drugs, placed them into a warming bin at the facility, and waited for them to be used in colleagues' surgeries, knowing their patients would experience dangerous complications. Surveillance video introduced into evidence showed Ortiz repeatedly retrieving IV bags from the warming bin and replacing them shortly thereafter, not long before the bags were carried into operating rooms where patients experienced complications. Video also showed Ortiz mixing vials of medication and watching as victims were wheeled out by emergency responders.

Evidence presented at trial showed that Ortiz was facing disciplinary action at the time for an alleged medical mistake made in his one of his own surgeries, and that he potentially faced losing his medical license. (Source)

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) (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

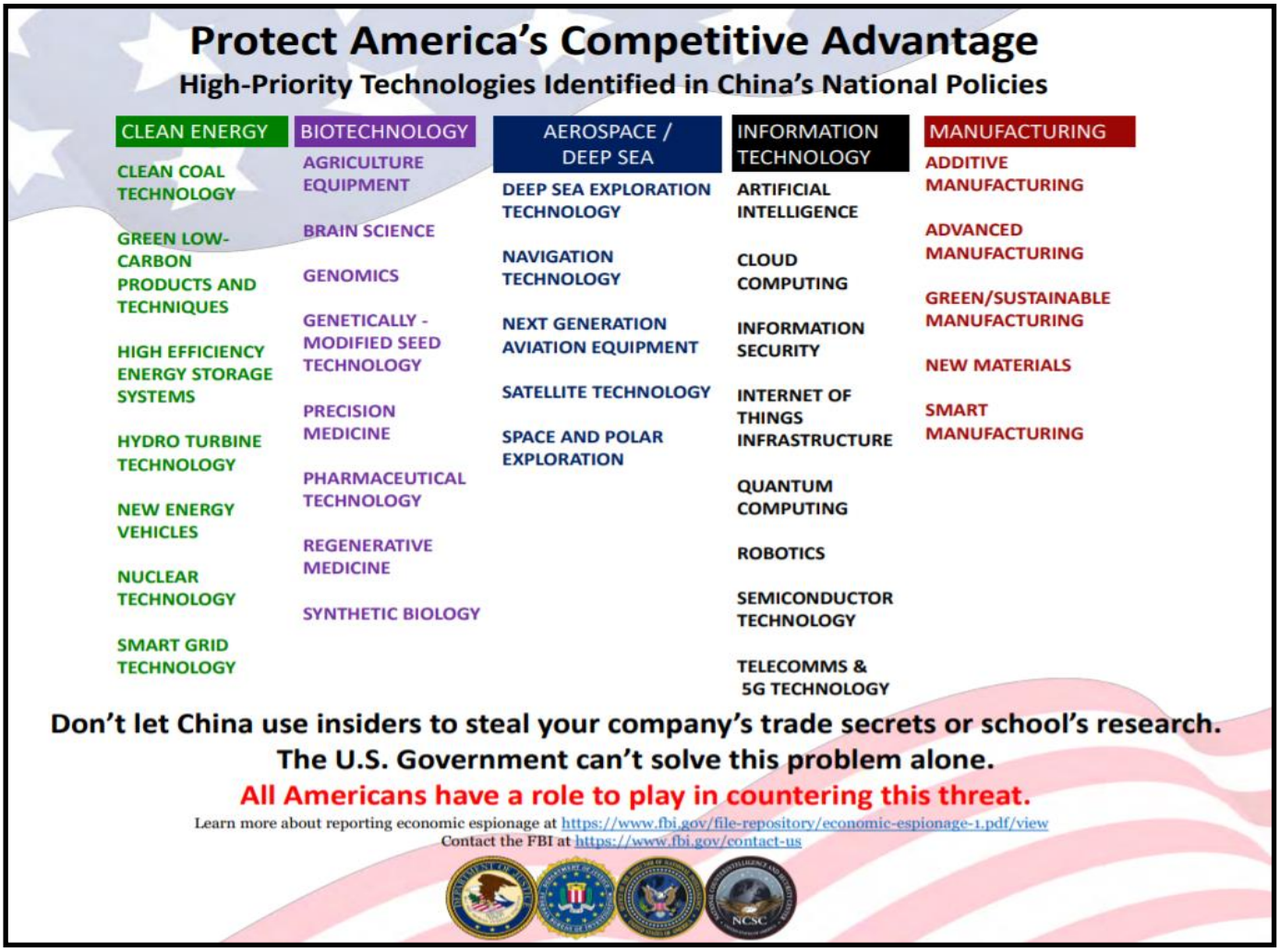
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 (**6,200+ 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 / X

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)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

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

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. 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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.

https://www.nationalinsiderthreatsig.org/aboutnitsig.html

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage, evaluate and optimize an Insider Risk Management (IRM) Program.

Over **1000+** 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, as well as attended our Insider Threat Investigations - Analysis Training Course and other training courses.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and IRM Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive IRM.

ITDG training and consulting services will empower individuals that manage or support IRM Programs, with the comprehensive knowledge, tools and a unified and holistic approach to identify, prevent and mitigate Insider Risks / Threats.

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Development, Management & Optimization Training Course
- ✓ IRM Program Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of 675 Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(Client Listing)

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 / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** 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

Please contact the ITDG with any questions regarding our training and consulting services.

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 Expert
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
FBI InfraGard Members
LinkedIn NITSIG Group

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