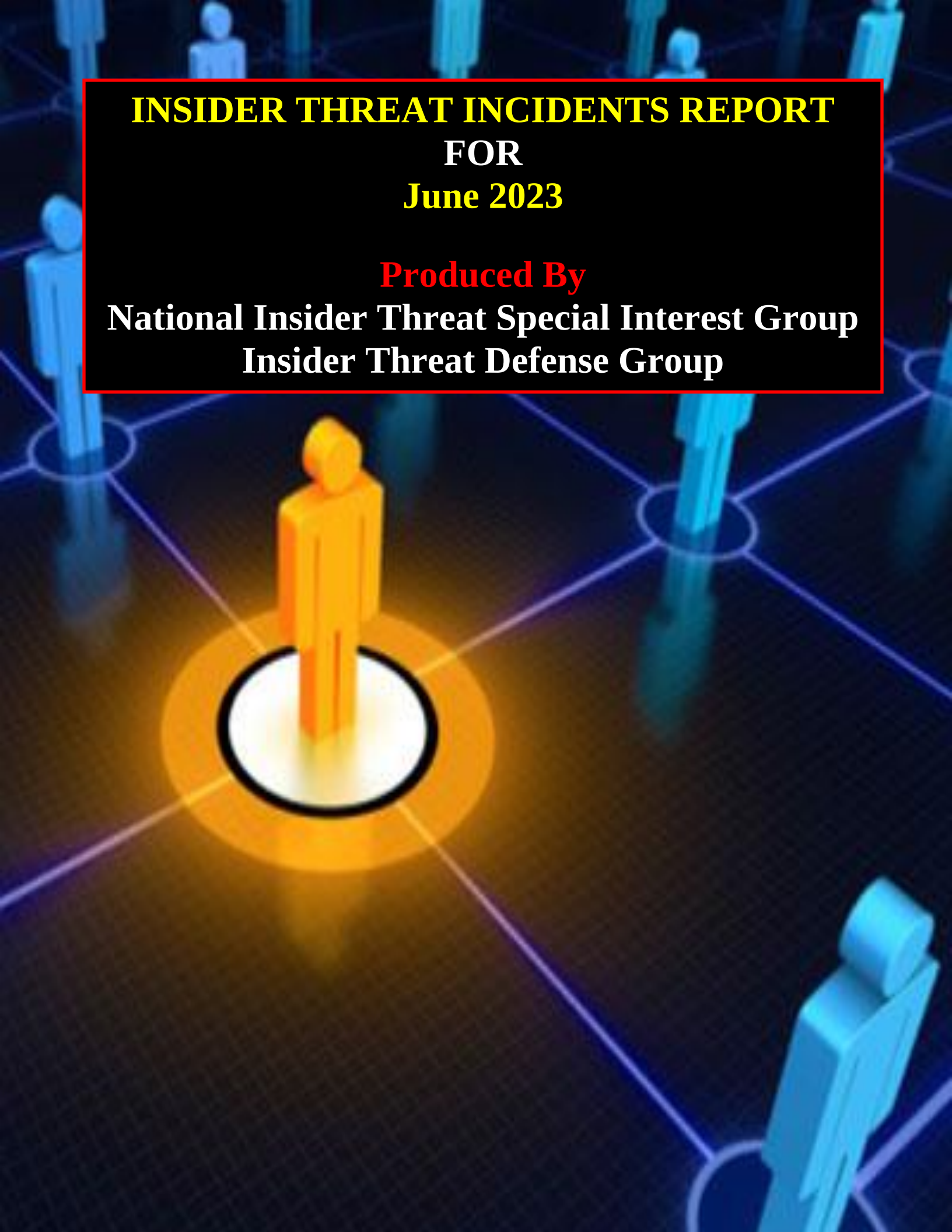

INSIDER THREAT INCIDENTS REPORT
FOR
June 2023

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

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 sit behind firewalls or telework through firewalls. 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 10+ years. This research has evaluated and analyzed over **4,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

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. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees'.

According to the Association of Certified Fraud Examiners 2022 Report to the Nations, organizations with less than 100 employees' suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most 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.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees' are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 6 to 24 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

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 CC2 & 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
- ☐ 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 / Airline Industry (Pilots, Flight Attendants)
  - 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)
- ☐ 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
- ☐ Employees' Loose Jobs / Company Goes Out Of Business

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, Buy 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, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

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

INSIDER THREAT INCIDENTS
FOR JUNE 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

2 Former Employees Of Collapsed Wirecard Asia Sentenced To Prison For Involvement In $2 BILLION Fraud Scheme - June 20, 2023

James Wardhana, who was the International Finance Process Manager of Wirecard Asia, and Chai Ai Lim, who was the Head Of Finance at Wirecard Asia, were sentenced to prison for conspiring to misappropriate funds.

These are the first criminal convictions handed down in charges related to accounting frauds at Wirecard, the German payments group that collapsed in June 2020 after revealing that half of the annual revenue it had claimed did not exist.

Wardhana's and Lim's superior at Wirecard Asia, Edo Kurniawan, is at large, with a warrant for his arrest having been issued.

In addition, James Henry O'Sullivan, who controlled companies that did business with Wirecard and is charged with abetting the falsification of documents, is scheduled to go on trial in Singapore next month.

In Germany, 3 Wirecard executives, including CEO Markus Braun, are on trial in a court battle that is expected to extend at least into 2024. Braun had resigned and was arrested on charges of misrepresenting Wirecard's accounts and market manipulation. Wirecard's former Chief Operating Officer, Jan Marsalek, is also at large, and has not been found.

The company filed for insolvency in June 2020, becoming the first member of Germany's Frankfurt Stock Exchange to go out of business less than a week after auditors disclosed $2.1 Billion of supposed deposits were missing from two Philippines banks. (Source)

Chinese Research Scientist Arrested For Suspicion Of Industrial Espionage / Confidential Data Leak - June 16. 2023

A Chinese scientist working for Japan's state-funded research body was arrested on suspicion of industrial espionage, according to the Metropolitan Police Department in Tokyo.

Quan Hengdao was Researcher at the National Institute of Advanced Industrial Science and Technology (AIST). He is alleged to have given a Chinese firm the institute's confidential data in a possible violation of the Unfair Competition Prevention Law.

The data, on technologies for synthesizing fluorine compounds, is believed to have been shared with the firm in an email sent on April 13, 2018, from an account that belonged to the AIST.
Hengda is believed to have been part of the team that was working on the data.

Investigators are searching locations related to the suspect and looking into ties between Hengda and the Chinese firm.

Quan joined the AIST in 2002, which is one of the largest public research bodies in Japan with approximately 2,300 scientists and engineers working at 12 locations across the country. (Source)

U.S. GOVERNMENT

Former Department of Energy Employee Pleads Guilty To Accepting $18,000 In Bribes In Exchange For Nearly $1 Million In Federal Contracts - June 26, 2023

Jami Anthony, is the former Small Business Program Liaison and Procurement Officer for a Department of Energy (DOE) laboratory based in Virginia.

She pleaded guilty to receiving bribes as a federal official in connection with a scheme to pay her more than $18,000 in exchange for more than $900,000 in DOE contracts.

Between approximately December 2017 and December 2020, Michael Montenes, the owner of M.S. Hi-Tech, Incorporated (MSHT), a Hauppauge-based distributor of electronic components, paid Anthony approximately $18,800 in bribes to induce her to enter into contracts for electronic components that MSHT supplied to the DOE's Virginia laboratory. Montenes mailed these payments, which ranged from $500 to $7,200, from Long Island to Anthony in Virginia. In exchange for the bribes, Anthony awarded MSHT contracts worth more than $900,000, which represented 95% of all of MSHT's sales to the DOE's Virginia laboratory.

In July 2021, some of the electronic components that Anthony procured from MSHT for DOE based upon Montenes's bribes failed and caused a fire, resulting in approximately $1.8 million in repairs and other costs to DOE. (Source)

Former USDA Animal Inspector Sentenced To Prison For Accepting $40,000+ In Bribes - June 1, 2023

Roberto Adams was a employed at the U.S. Department of Agriculture (USDA) as a lead animal health technician for 10 years. In that role, he was responsible for inspecting and quarantining or excluding tick-infested or diseased cattle. He was only one of two technicians the USDA employed in Laredo and exercised high level decision-making authority.

Adams admitted he accepted over $40,000 in bribe payments from Mexican cattle brokers while acting in his official position as a USDA employee. In return, he allowed cattle to enter the United States without proper quarantine or inspection. (Source)

Former U.S. Postal Service Employee Pleads Guilty To Using Her Position To Obtain The Personal Information Of Victims As Part Of Conspiracy To Commit Bank Fraud / Wire Fraud - - June 6, 2023

Breanna Cartledge was a Clerk with the U.S. Postal Service (USPS).

Cartledge pleaded guilty to conspiracy to commit bank fraud and wire fraud, in connection with a scheme to defraud financial institutions by creating fake checks using information Cartledge collected.

Cartledge wrongfully accessed USPS money orders and individual mail to illegally obtain the personal information of victim individuals and businesses, which she and her co-conspirators used without the victims' authorization.

For example, after a co-conspirator texted Cartledge requesting pictures of checks, Cartledge sent the co-conspirator images of at least nine separate money orders or checks that contained personal identifying information with the intent that the information be used to create fake checks to steal from victim accounts.

Cartledge negotiated a counterfeit check fraudulently drawn for $4,900 from the account of a victim, but the transaction was reversed by the bank. Cartledge admitted that she abused her position as a USPS Clerk to facilitate the commission or concealment of the offense. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Air Force Base Director Sentenced To Prison For Role In Conspiring To Pay Lobbyists, Consultants & Contractors $8.4 Million With Funds Fraudulently Obtained From United States Government - June 27, 2023

Beginning in 2004, Milton Boutte, who was then the Director of the Big Crow Program Office at Kirtland Air Force Base, conspired with others to pay lobbyists, consultants and contractors with funds fraudulently obtained from the United States.

Boutte conspired with George Lowe, a lobbyist, and Joe Diaz and Arturo Vargas, owners of Miratek and Vartek, two minority-owned small businesses that had sole-source contracts with the Big Crow Program Office. The conspirators disguised the nature of the claims for lobbying services provided by Lowe as well as other unauthorized subcontracts and expenditures. The Big Crow Program Office was not authorized to lobby or to expend appropriated funds for lobbying activities under the contracts.

Over the course of the conspiracy, Miratek and Vartek received approximately $8.4 million from the government. Of that amount, Boutte required those small businesses to pay nearly $4.1 million to lobbyists, consultants and contractors that Boutte had retained. Of that sum, Miratek and Vartek diverted more than $900,000 to Lowe, and another government contractor paid Lowe an additional $300,000. (Source)

Former U.S. Air Force Intelligence Officer Sentenced To Prison For Retaining 300+ Classified Secret / Top Secret Documents - June 1, 2023

Robert Birchum pleaded guilty to unlawfully possessing and retaining classified documents relating to the national defense of the United States on February. 21, 2023. Birchum previously served as a Lieutenant Colonel in the U.S. Air Force. During his 29-year career, Birchum served in various positions in intelligence, including those requiring him to work with classified intelligence information for the Joint Special Operations Command, the Special Operations Command, and the Office of the Director of National Intelligence.

While on active duty, Birchum entered into several agreements with the United States regarding the protection and proper handling of classified information.

In 2017, however, law enforcement officers discovered that Birchum knowingly removed more than 300 classified files or documents, including more than 30 items marked Top Secret, from authorized locations.

Birchum kept these classified materials in his home, his overseas officer's quarters, and a storage pod in his driveway. None of these locations were authorized for storage of classified national defense information. In particular, the criminal information charges that Birchum possessed two documents on a thumb drive found in his home that contained information relating to the National Security Agency's capabilities and methods of collection and targets' vulnerabilities. Both of these documents were classified as Top Secret/SCI, and their unauthorized release could be expected to cause exceptionally grave damage to the national security of the United States. (Source)

Air National Guardsman Charged For Unlawful Disclosure Of Classified Information - June 15, 2023

Jack Teixeira was a member of the United States Air National Guard (USANG).

Teixeira transmitted the classified National Defense Information (NDI) on the social media platform in two ways. First, Teixeira allegedly accessed classified documents containing NDI from a classified workstation at the USANG Base and transcribed and transmitted the information in written paragraphs to other users on the social media platform.

Teixeira also allegedly posted images of classified documents to the social media platform, which bore standard classification markings SECRET, TOP SECRET, and SCI designations, indicating that they contained highly classified United States government information. At least one of the documents containing NDI was allegedly found in digital form in a particular account associated with Teixeira. (Source)

Former U.S. Air Force Serviceman Sentenced To Prison For Illegally Exporting Night Vision Goggles, Other Military Items to Russia - June 23, 2023

Igor Panchernikov who once served in the United States Air Force Reserves, was sentenced to prison for one count of conspiracy to violate the Arms Export Control Act. He has been in federal custody since July 2022 after Israel extradited him to the United States.

From December 2016 to May 2018, Panchernikov conspired with other individuals to knowingly export from the United States to Russia defense articles without obtaining from the State Department a valid license or other approval for such exports.

Panchernikov's accomplices purchased defense articles including thermal riflescopes, weapons sights, monoculars and night vision googles from various online sellers located in the United States and directed the sellers to mail those items to Panchernikov's residence.

Panchernikov received at least 19 defense articles that his co-conspirators purchased from online sellers. After receiving these items, Panchernikov inspected the items to ensure that they were undamaged and operational. Pursuant to his co-conspirators' instructions, Panchernikov then mailed two of the items to accomplices in Russia and mailed 17 defense articles to Elena Shifrin, 61, of Mundelein, Illinois, who then mailed these items to Russia.

To conceal his unlawful activities, when Panchernikov exported the two defense articles to Russia, he listed fictitious sender names on the packages containing the items. He also falsely identified the items in the packages as non-export-controlled items, such as clothing. Finally, he concealed the defense articles in other items, including a drill press. (Source)

U.S. Marine Arrested On Charges Stemming From Role In Firebombing Of Planned Parenthood Clinic - June 14, 2023

Agents with the FBI and the Naval Criminal Investigative Service arrested two men on federal charges alleging they used a Molotov cocktail to firebomb a California Costa Mesa clinic operated by Planned Parenthood Federation of America.

Chance Brannonstrano was an active duty Marine stationed at Camp Pendleton, and the other individual invloved was Tibet Ergul.

Ergul and Brannon attacked the clinic during the early morning hours of March 13, 2022, by igniting and a throwing a Molotov cocktail at the clinic entrance. As a result of the fire, the Planned Parenthood Costa Mesa healthcare clinic was forced to close the following morning and cancel approximately 30 appointments.

Security videos described in the affidavit show that two men wearing hooded sweatshirts and face masks approached the Planned Parenthood facility at approximately 1 a.m. the day of the attack, ignited a device, and threw the flaming device at the front door of the building. The device landed against a southern wall next to the glass door and erupted into a fire, which spread up the wall and across the ceiling above the glass door. (Source)

U.S. Army Soldier Pleads Guilty To Terrorism Charges For Attempting To Assist ISIS To Conduct Deadly Ambush On U.S. Troops - June 14, 2023

Cole Bridges joined the U.S. Army in approximately September 2019 and was assigned as a cavalry scout in the Third Infantry Division based in Fort Stewart, Georgia.

Beginning in at least 2019, Bridges began researching and consuming online propaganda promoting jihadists and their violent ideology. Bridges also expressed his support for ISIS and jihad on social media. In or about October 2020, Bridges began communicating with a Federal Bureau of Investigation (FBI) online covert employee (The OCE), who was posing as an ISIS supporter in contact with ISIS fighters in the Middle East.

During these communications, Bridges expressed his frustration with the U.S. military and his desire to aid ISIS. Bridges then provided training and guidance to purported ISIS fighters who were planning attacks, including advice about potential targets in New York City. Bridges also provided the OCE with portions of a U.S. Army training manual and guidance about military combat tactics, for use by ISIS.

In or about December 2020, Bridges began to supply the OCE with instructions for the purported ISIS fighters on how to attack U.S. forces in the Middle East. Bridges diagrammed specific military maneuvers intended to help ISIS fighters maximize the lethality of attacks on U.S. troops.

Bridges further provided advice about the best way to fortify an ISIS encampment to repel an attack by U.S. Special Forces, including by wiring certain buildings with explosives to kill the U.S. troops. Then, in January 2021, Bridges provided the OCE with a video of himself in his U.S. Army body armor standing in front of a flag often used by ISIS fighters and making a gesture symbolic of support for ISIS. Approximately a week later, Bridges sent a second video in which Bridges using a voice manipulator, narrated a propaganda speech in support of the anticipated ambush by ISIS on U.S. troops. (Source)

Former Army Reservist Sentenced To Prison For Stealing $21,000+ Of Government Funds - June 16, 2023

Lynea Sanders is a former United States Army Reservist.

Sanders pled guilty to conspiracy to commit theft of government funds, having stolen $21,780.18 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

Former Army Reservist Sentenced To Prison For Stealing $8,300+ Of Government Funds - June 16, 2023

Chantelle Davis is a forrmer United States Army Reservist.

Davis pled guilty to conspiracy to commit theft of government funds, having stolen $8,399.65 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former FBI Analyst Sentenced To Prison For Retaining 386 Classified Documents And Keeping Them At Her Home - June 21, 2023

Kendra Kingsbury is a former Intelligence Analyst with the Kansas City Division of the FBI, from 2004 to 2017. Kingsbury was assigned to a sequence of different FBI squads, each of which had a particular focus, such as illegal drug trafficking, violent crime, violent gangs, and counterintelligence. Kingsbury held a TOP SECRET//SCI security clearance and had access to national defense and classified information.

Kingsbury admitted that, over the course of her FBI employment, she repeatedly removed from the FBI and retained in her personal residence an abundance of sensitive government materials, including classified documents related to the national defense. In total, Kingsbury improperly removed and unlawfully and willfully retained approximately 386 classified documents in her personal residence. (Source)

Sheriff Charged For Accepting $72,000 In Bribes / Campaign Contributions To Sell Law Enforcement Badges And Credentials - June 29, 2023

From at least April 2019, Culpeper County Virginia Sheriff Scott Jenkins accepted cash bribes and bribes in the form of campaign contributions totaling at least $72,500 from numerous individuals. In return, Jenkins appointed each of the bribe payors as auxiliary Deputy Sheriffs, a sworn law-enforcement position, and issued them Culpeper County Sheriff's Office badges and identification cards. Jenkins told or caused others to tell the bribe payors that those law-enforcement credentials authorized them to carry concealed firearms in all 50 states without obtaining a permit. (Source)

Former Federal Correctional Officer Sentenced To Prison For $46,000+ COVID Paycheck Protection Program Fraud / Used Funds For Travel New SUV, Etc. - June 16. 2023

Harrescia Hopkins, while a Federal Bureau of Prisons Correctional Officer, applied for two PPP loans for $19,100 each in August 2020 and January 2021. The PPP loan applications were purportedly to help a business named Hopkins Towing and Storage, which she claimed had a gross income of $100,525 in 2019. In reality, Hopkins Towing and Storage was not a real and functioning business. Hopkins also obtained a $4,000 loan from the United States Small Business Administration's COVID-19 Economic Injury Disaster Loan program.

Hopkins caused the loan proceeds to be deposited into her personal checking account. Hopkins then spent the money on personal expenses – including a Caribbean cruise and other travel, a new Chevrolet Blazer, landscaping for her house, restaurant meals, and retail goods.

Hopkins was ordered to repay all three loans in full in the amount of $46,004.04. (Source)

Former Sheriff's Office Employee Pleads Guilty To Theft Of $150,000+ - May 11, 2023

From July 2018 to September 2022, while employed at the West Baton Rouge Parish Sheriff's Office, Mandy Miller stole cash paid for traffic tickets and hid the thefts by recording fraudulent journal entries in the Sheriff's Office accounting system.

In all, it is alleged that Miller embezzled, stole, and otherwise without authority, knowingly converted to her own use more than $150,000 in official funds. (Source)

Former Prison Correctional Officer Sentenced To Prison For Accepting Bribes To Smuggle Contraband - June 2, 2023

Ty Craig pleaded guilty to accepting thousands of dollars in cash bribes in exchange for smuggling contraband into the James Crabtree Correctional Center (JCCC) in Helena, Oklahoma.

The contraband included cell phones, marijuana, and methamphetamine. (Source)

Employee Of County Detention Center Charged With Taking Bribe Money / Sexual Favors To Smuggle Controlled Substance To Inmates - June 7, 2023

And employee of a county detention center, along with three associates of an inmate detained at the center, have been indicted by a federal grand jury for their roles in a conspiracy to smuggle papers laced with K2 to jail inmates.

Aaron Copes took bribe money and sexual favors in exchange for smuggling contraband into the detention center and delivering it to inmates. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former West Virginia Environmental Protection Official Pleads Guilty To Theft Of $94,000+ Of Federal Grant Funds - June 2, 2023

Jerry Elkins pleaded guilty to theft from programs receiving federal funds. Elkins admitted to fraudulently obtaining $94,197.93 of federal abandoned mine land (AML) remediation sub-grant funds while employed by the West Virginia Department of Environmental Protection (DEP).

From on or about April 2017 until on or about August 7, 2019, Elkins assisted an individual, A.K., and his company apply for and obtain an AML sub-grant. Thereafter, Elkins set up a shell limited liability company to receive a portion of the sub-grant award funds and created fraudulent invoices in an attempt to conceal the nature of the payments. (Source)

Former City Councilman Pleads Guilty To Accepting $15,000 Cash Bribe From Investors - June 7, 2023

Between June 2018 and January 2019, Jeffrey Pastor accepted and agreed to accept things of value in exchange for favorable official action by Pastor relating to two development projects in the city.

In September 2018 Pastor and his associate flew to Miami, Florida, on a private plane to meet with investors regarding a real estate development project. Pastor never paid for or disclosed the trip. During the trip, Pastor explained he would ensure favorable action on behalf of the city for the project and could receive money through his associate's non-profit entity (which had been incorporated two weeks prior). Pastor discussed compensation and agreed to accept $15,000 for helping with the project. He said the purpose of his associate's entity was to sanitize the money.

After flying back to Cincinnati, Pastor called the investor to negotiate a monthly retainer and said that $15,000 would be the retainer fee for providing official action. On Oct. 4, 2018, Pastor accepted $15,000 in cash. After receiving the money, Pastor continued to solicit additional payment from the investor and others. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

University Professor And Wife Sentenced To Prison For $2.1 Million Of Federal Grant Fraud - June 29, 2022

Shaorong Liu and Juan Lu were sentenced to prison and ordered to pay $2.1 Million in restitution for making false statements involving a Department of Energy grant.

Liu served since 2008 as a professor at the University of Oklahoma in its Department of Chemistry and Biochemistry. In approximately 2001, Liu and his wife Lu formed and controlled a company called MicroChem Solutions (MCS). Through MCS, they applied for and received federal grant monies from the Small Business Technology Transfer Program of the Department of Energy. The mission of the grant program was to support scientific excellence and technological innovation through the investment of federal research funds in critical American priorities to build a strong national economy. However, Liu and Lu spent this grant money on matters unrelated to the purpose of the grant funding, including on personal expenses. Liu and Lu also made false statements and submitted altered documents to the Department of Energy regarding how they spent grant money. (Source)

High School Employee Charged With Federal Explosive Offenses For Manufacturing & Selling Explosive Materials - June 8, 2023

Angelo Mendiver was an employee of the Kern High School District in California. He is charged with conspiring to commit offenses against the United States; engaging in manufacturing and dealing in explosive materials; two counts of mailing an explosive device; improper storage of explosives; and making false statements to agents of the Federal Bureau of Investigation.

Mendiver used an Instagram account to sell explosives and explosive materials and worked closely with a male juvenile Bakersfield high school student to fulfill transactions.

A federal search warrant executed at Mendiver's residence on June 1, 2023, resulted in the seizure of approximately 500 pounds of explosives and explosive materials. Agents seized another 500 pounds of explosives and explosive materials from the juvenile's residence. (Source)

Former New York City Department Of Education CEO Of School Support Services & 3 Company Executives Convicted Of Extortion Conspiracy And Bribery - June 28, 2023

A federal jury in Brooklyn, New York returned guilty verdicts on all counts of a superseding indictment against Eric Goldstein, the former Chief Executive Officer of the New York City Department of Education's (NYC DOE) Office of School Support Services, and Blaine Iler, Michael Turley and Brian Twomey, operators of a food services company, with conspiring to commit extortion and giving of bribes relating to programs receiving federal funds.

As proven at trial and contained in court filings, between 2008 and September 2018, Goldstein oversaw the management, budget, and operations of several NYC DOE departments, including the Office of Food and Nutrition Services (SchoolFood), which was responsible for managing the overall food service operation for all New York City public schools. In early 2015, Iler, Turley, and Twomey created a food services company called SOMMA Food Group (SOMMA), to provide food products to retail and food service markets, including to K-12 schools across the United States. SOMMA promoted and sold yogurt, hamburgers, and antibiotic-free chicken products marketed under the brand name Chickentopia.

At or about the same time SOMMA was founded, Goldstein, Iler, Turley, and Twomey co-founded Range Meats Supply Company (RMSCO), to purchase grass-fed beef products that SOMMA, in turn, would then promote and sell under the brand name Range Meats to retail markets and New York City schools. At the same time, Iler, Turley, and Twomey partnered with Goldstein in RMSCO, Iler, Turley and Twomey began to promote SOMMA's products to SchoolFood officials and employees, all of whom reported to Goldstein in his role as OSS Chief Executive. During a meeting with Iler in New York in July 2015, Goldstein told him, "I'm going to buy a lot of f---ing chicken from you guys, let's do the beef." (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Union Secretary Sentenced To Prison For Stealing $63,000 To Pay Gambling Debts - June 26, 2023

Wilbert Barnes held the position of Recording Secretary of United Steelworkers Local 1362.

Barnes confessed to the local sheriff's office that he took $12,500 of Local 1352's funds via two unauthorized checks in June 2021.

Upon further investigation, it was determined that Barnes had misappropriated at least $25,000 of Local 1362's funds since 2017. In 2017, Barnes negotiated a Local 1362 check worth $9,000. In May of 2021, Barnes negotiated a check for $4,000 with a memo entry falsely stating that the check was for "school books, t-shirts." In June of 2021, Barnes forged a check for $7,500 and made a cash withdrawal from the union's account in the amount of $5,000. BARNES confessed that he used this money to pay his gambling debts. (Source)

Former Union President Admits Filing False Report To Hide His $36,000 Of Embezzlement / Used Funds For Shopping, Travel, Dining, Etc. - June 15, 2023

Felix Luciano is the former Union President of Local 2805 Chapter of the American Federation of Government Employees and a former Department of Homeland Security Officer.

From January of 2016 to December of 2018, Luciano used some of Local 2805's money for a variety of personal expenses, including shopping, travel reimbursements, groceries, dining, dry cleaning, and paying for non-union accounts. He did this by writing checks from Local 2805's checking account and using Local 2805's debit and credit cards to directly pay personal expenses. As a result of Luciano's actions, he caused a total loss of $36,000 to Local 2805.

As Local 2805's president, Luciano was required to file an annual Form LM-3 financial report with the United States Department of Labor, Office of Labor-Management Standards. A Form LM-3 is a report containing information about the organization over the prior year, including assets, liabilities, and disbursements to officers. A Form LM-3 is sworn under penalty of perjury. In the LM-3 report he filed in 2018, Luciano underreported the amount of money that he received from Local 2805 and Local 2805's cash balance. In doing so, Luciano attempted to hide his embezzlement from the Department of Labor, his fellow union officers, as well as the union membership whose dues were the source of the embezzled funds. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee Convicted Sentenced To Prison For Role In $2 Million Fraud Scheme - June 2, 2023

Diape Seck was convicted for his role in a bank fraud scheme in which he and his co-conspirators obtained or attempted to obtain almost $2 Million by fraud, including by stealing checks from the mail of churches and religious institutions.

From at least January 2019 to January 2020, Diape Seck, who was a Customer Service Representative with Bank A, conspired with Mateus Vaduva, Marius Vaduva, Vlad Baceanu, Nicolae Gindac, Florin Vaduva, Marian Unguru, Daniel Velcu, Vali Unguru and others to commit bank fraud.

Seck fraudulently opened bank accounts in fake identities in exchange for cash bribes. Co-conspirators engaged in fraud that included fraud involving rental cars and the deposit of checks stolen from the incoming and outgoing mail of churches and other religious institutions, into the fraudulently opened bank accounts. The co-conspirators then withdrew the funds and spent the fraudulently obtained proceeds

Seck violated numerous bank policies in opening approximately 412 checking accounts in a one-year period from approximately January 2, 2019 through January 3, 2020, relying predominantly on purported Romanian passports and driver's license information.

Checks payable to and written from churches and other religious institutions from around the country were deposited into many of the 412 checking accounts which were not opened in the names of the churches.

The co-conspirators fraudulently negotiated the stolen checks by depositing them into the victim bank accounts, including the fraudulent accounts opened by Seck at Bank A, often by way of automated teller machine (ATM) transactions. After depositing the stolen checks into the bank accounts, the conspirators made cash withdrawals from ATMs and purchases using debit cards associated with the bank accounts. (Source)

Former Bank Employee Sentenced To Prison For Embezzling $439,000 - June 6, 2023

Samantha Cherry was a Manager at a UMB Bank branch in St. Louis.

Between January 2021 and March 2022, Cherry took cash directly from the vault and moved currency from other cash supplies into her cash drawer totals. Cherry admitted to the theft after being questioned by bank personnel, that she embezzled about $439,000. (Source)

Former Bank Branch Manager Pleads Guilty To Stealing $120,000+ From Customer Bank Accounts For Personal Use - June 8, 2023

From June 2020 through November 2021, Nathan Wadsworth was employed as a Bank Branch Manager for PNC Bank in Boston.

Beginning in or around March 2021, Wadsworth used his position to identify dormant accounts of foreign account holders, transfer the funds in those dormant accounts to a new account he opened in the customers' names and then moved the funds to his own accounts for personal use. In total, Wadsworth stole approximately $121,000 in customer funds. All the funds have since been repaid to the affected customers. (Source)

Former Credit Union Assistant Branch Manager Arrested For Embezzling $60,000+ To Spend On TikTok - June 1, 2023

Andrade Olson began working at the credit union in 2005 and was promoted to assistant branch manager in 2019.

In July and August 2022, Olson made several unauthorized withdrawals from four members' accounts, including seven withdrawals totaling $35,000 from one member. When questioned by credit union officials, Olson abruptly resigned from her position. Court documents indicate that Olson was using some of the embezzled funds to promote herself on TikTok. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Engineer Sentenced To Prison For Stealing Employers Semiconductor Trade Secret To Start His Own Microchip Business - June 1, 2023

Between 2014 and 2017, Haoyang Yu worked at Analog Devices, Inc. (ADI), where he designed microchips used by the communications, defense, and aerospace industries. Through his employment, Yu had access to various kinds of ADI intellectual property, including present and future microchip designs, schematics, layouts, modeling files, customer lists, and ordering histories.

While employed at ADI, Yu used this information to start his own microchip business, Tricon MMIC, LLC. Forensic analysis later showed that Yu's personal, at-home computer held exact, bit-for-bit copies of hundreds of ADI intellectual property files.

Evidence showed that Yu had accessed these files on ADI's secure servers, copied them, changed their filenames – often to those of cartoon characters, and then saved them on his personal electronic accounts and devices.

Evidence showed that all of the chips Yu's business sold were built with ADI's stolen intellectual property. In particular, Yu used the stolen HMC1022A design to manufacture two knock-off versions of ADI's chip. Yu then began selling his versions of the HMC1022A to ADI's customers and others even before ADI went to market with its own completed design.

In all, before his arrest, Yu manufactured about 10,000 chips built with stolen ADI property and grossed about $235,000. ADI cooperated fully in the government's investigation. (Source)

Abbott Laboratories Accuses Former Scientist Of Trade Secrets Theft In U.S. Court - May 31, 2023

Healthcare company Abbott Laboratories sued one of its former scientists, accusing him in U.S. court of secretly downloading sensitive corporate files containing competitive information about nutrition products.

The lawsuit in Chicago federal court alleged Roger Tyre committed flagrant misconduct prior to leaving Illinois-based Abbott. Abbott said it learned of the alleged downloads of thousands of files in March.

Tyre, who worked at Abbott from 2012 to 2018, developed products and supported Abbott's existing products by troubleshooting and addressing any issues.

Abbott's lawyers argued the misappropriation will cause Abbott irreparable harm by undermining Abbott's competitive advantage in the nutrition market.

After leaving Abbott, Tyre worked at manufacturer Better Nutritionals LLC, whose website identified him as Chief Operating Officer. (Source)

Former Hospital Employees Inappropriately Accessed The Personal Information Of 280 Patients - Hospital Fined $988,000 - June 15, 2023

A proposed settlement of $988,550 has been reached in a class-action lawsuit relating to patient health records being wrongfully accessed by former employees at the Peterborough Regional Health Centre more than a decade ago.

Between 2011 and early 2012, former hospital employees inappropriately accessed the personal information of approximately 280 patients.

At the time the hospital said seven employees were fired as a result of alleged patient record privacy breaches which were reported to the Information and Privacy Commissioner. (Source)

CHINESE ESPIONAGE TARGETING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

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)

Former Hospital Financial Director Of Sentenced To Prison Stealing $890,000+ For 7 Years - June 21, 2023

Edward Calloway served as the Financial Director for Ouachita Parish Hospital Service District's G.B. Cooley Hospital (Cooley Hospital) from 2016 until October 2019. Prior to serving as their Financial Director, Calloway was the First Staff Accountant from 2010 until 2016.

Beginning in 2012, Calloway began stealing from Cooley Hospital by transferring money from the hospital's general fund, sinking fund, and payroll accounts to his personal accounts at a banl and credit union. Calloway used a computer to initiate the Automated Clearing House (ACH) bank transfers.

Calloway did an ACH transfer of $1,945.34 to be transferred by an interstate wire from a Cooley Hospital account to his personal bank account. Calloway's theft continued until October 2019 and resulted in a total loss of $892,602.18. (Source)

Former Employee Of Medical Professional Staffing Company Sentenced To Prison For Role In $127,000 Wire Fraud / Identity Theft Scheme - June 2, 2023

Rebecca Russell conspired with her sister, Roseanna Taylor, to commit fraud using stolen identities. Taylor worked for a medical professional staffing company based from May 2017 through January 2019.

By virtue of Taylor's employment, she obtained personal pedigree information, including means of identification of certain medical professionals. Russell obtained these stolen identities from Taylor and made various consumer lending transactions through mid-2020. As part of the scheme, Russell used fake identification documents containing her photo along with victims' personal information to obtain fraudulent loans for cash, at least one automobile, and other items of monetary value.

Russell was ordered to pay restitution to the victims of the fraud scheme in the amount of $127,663.26. (Source)

Snooping Of Medical Records By Hospital Security Guards Leads To $240,000 HIPAA Fine - June 15, 2023

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement with Yakima Valley Memorial Hospital, a not-for-profit community hospital located in Yakima, Washington, relating to an investigation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

OCR investigated allegations that several security guards from Yakima Valley Memorial Hospital impermissibly accessed the medical records of 419 individuals. Yakima Valley Memorial Hospital agreed to pay $240,000 and implement a plan to update its policies and procedures to safeguard protected health information and train its workforce members to prevent this type of snooping behavior in the future. (Source)

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

2 Trucking Company Employees Arrested For Embezzling $1.4 Million - June 1, 2023

Dina Morales and Laura Ballesteros allegedly used their positions with MH Group (Texas Based Trucking Company) to divert the company's customer account receivable payments to their own bank accounts. The total amount of the embezzled, diverted and stolen funds between July 2017 and April 2019 is alleged to have been approximately $1.4 Million. (Source)

Former Southwest Airline Employee Charged For Role In $1.87 Million Scheme To Fraudulently Create And Sell Travel Vouchers - June 6, 2023

Dajuan Martin was a customer service representative for Southwest Airlines.

She fraudulently created and sold travel vouchers worth more than $1.87 Million. While working for Southwest at Midway Airport in Chicago, Martin used fictitious customer names to fraudulently generate the vouchers without the airline's knowledge or approval. Martin then sold the vouchers at below market value to co-defendant Ned Brooks and others in exchange for cash.

The vouchers, known as "Southwest Luv Vouchers," were supposed to be used to compensate customers who had unfavorable travel experiences on the airline. (Source)

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

Former Property Management Company Chief Financial Officer Peads Guilty To Embezzling $3 Million+ - June 29, 2023

David Katz was the former Chief Financial Officer (CFO) of Durand and Associates (D&A), a property management company that specialized in servicing homeowner associations (HOAs). Between 2012 and 2017, Katz embezzled over $3 million from D&A and its client HOAs.

Katz worked for D&A from approximately 1998 to 2017, starting as an accountant and eventually becoming CFO. As CFO, Katz had authorization to open credit cards in D&A's name and use those credit cards for business expenses. However, Katz was not authorized to charge personal expenses to the cards, take out loans on D&A's behalf without the owner's approval, or use funds belonging to D&A or its HOA clients to pay his personal expenses.

Beginning in at least 2012 and continuing into 2017, Katz embezzled over $3 million from D&A and its HOA clients. Katz, who as CFO of D&A was responsible for payroll, paid himself significantly more than his agreed upon salary. Between 2011 and 2017, Katz paid himself $6,500 every two weeks as a salary despite his base salary never being more than $47,500 annually.

Katz also reimbursed himself for personal expenses and business expenses he never actually incurred. Katz paid himself between approximately $6,000 and $10,000 in reimbursements every two weeks. He labeled these payments as miscellaneous earnings and reimbursements, "recovery loans," bonuses, and commissions. Katz never loaned or invested money in D&A that he was entitled to "recover." To the extent he earned bonuses and commissions, they were in amounts significantly less than what he paid himself. And although Katz incurred some legitimate business-related expenses, they were in amounts significantly less than what he reimbursed himself. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $1.35 Million+ From Employer To Pay Off Credit Cards Debits, Purchase Truck, Camper, Boat, Firearms, Etc. - June 15, 2023

According to court documents and court proceedings, from October 2013 to December 2021, Danny Tremble executed a scheme to embezzle and defraud his employer, Azalea Management and Leasing, Inc. (Azalea).

Tremble worked at Azalea as an Accountant, and in that capacity had access to the company's bank accounts and accounting records. Over the course of the scheme, Tremble routinely misused his access to Azalea's bank accounts to embezzle company funds, which he used to pay off personal credit cards and to cover personal expenditures including lavish hotel stays, dining, and shopping. Tremble also used stolen company funds to purchase a camper, a boat, a trailer, a pickup truck, and to buy multiple firearms. (Source)

Former Company CPA Sentenced To Prison For Money Laundering / Embezzling $1 Million+ For 4 Years / Used Funds For Child Support Payments - June 27, 2023

Michael Harman was a Certified Public Accountant and was employed as a controller with his employer (Geis Company). As a controller, some of Harman's responsibilities included processing payroll adjustments.

From 2016 to August 2020, Harman devised a scheme to embezzle more than $1 Million from his employer and used the funds for personal use, including child support payments in the State of New York and moving expenses. Harman executed the scheme by using a series of unauthorized wire transfers, fictitious checks, and fraudulent charges on his employer's credit cards. (Source)

Former Office Manager / Bookkeeper For Construction Company Sentenced To Prison For Embezzling $765,000+ / Used Funds To Renovate House / Purchase Vehicle - June 6, 2023

Over a 5 year period Melissa Bittler embezzled over $765,000 from the construction company in where she was employed as the Office Manager and Bookkeeper. Among numerous and consistent personal expenditures with stolen money, Bittler bought and renovated her house and purchased a Honda Pilot with the embezzled company money. (Source)

Former Health Company Employee Who Resigned Is Accused Of Hacking Customer Accounts, Stealing $50,000+ - June 23, 2023

The Allegheny County District Attorney's Office charged Zakayah Scott who worked remotely from South Carolina for Highmark Health. Authorities said Scott had access to customers' personal information including birthdays, addresses and phone numbers.

They said she called Highmark's customer service department, claiming to be one of the victims, change their password to their health savings account, log in, then withdrew and transferred money. The amount stolen totals more than $50,000

According to the criminal complaint, Scott used the stolen money to buy things at Lululemon and the Apple store. Her coconspirators spent money at fast food restaurants and gas stations.

Highmark Health made the follwing statement saying: "We are aware that a former employee, who resigned earlier this year, is facing a criminal complaint related to allegations of theft and fraud.

We are thoroughly reviewing this ongoing investigation and have a number of systems in place to protect our members from fraudulent activity." (Source)

Former Town Official Pleads Guilty To $50,0000 Of Wire Fraud / Used Funds For Gambling 176 Times At Casino - June 26,2023

Cheryl Sullivan is the former Chairperson Of The Board of Tax Assessors for the Town of Dedham, MA.

She pleaded guilty to a charge of wire fraud, admitting that, while serving as a own official, real estate broker, tax preparer, and property manager for the River Island Condominium Association in Woonsocket, RI, she devised a scheme to access nearly $50,000 in Association funds for her own personal use.

Sullivan admitted that she used an Association debit card 58 times to withdraw cash between January and November 2019, when she visited the Plainfield Park Casino in Plainfield, MA.

Casino records reflect that from January 4, 2019, to November 19, 2019, Sullivan gambled at the casino 176 times, almost every day. Bank records associated with the Condominium Association's account reflect that there were 60 ATM withdrawals made from the account during the relevant time frame, of which 58 of those occurred at the casino. The withdrawals occurred on multiple dates that Sullivan's personal debit card had been used at the casino to attempt to withdraw cash from her own account but was declined. The condo association debit card was then immediately used to withdraw cash. (Source)

Former Housing Authority Executive Director Sentenced To Prison For Using $20,000+ Agency Funds For Personal Expenses - June 30, 2022

Thomas Upchurch is the former Executive Director of the Jefferson County Housing Authority.

Upchurch linked the housing authority's credit card to his personal Amazon account and made nearly 300 inappropriate charges for personal items. Over a three-year period, the charges totaled more than $20,000. To conceal his fraud, Upchurch blocked the members of JCHA's Board of Commissioners from reviewing his spending records. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Company Procurement Manager Pleads Guilty To Defrauding Employer Of $4.4 Million In Fake Invoice Scheme - June 7, 2023

From at least in or about July 2018, up to and including at least August 2022, Bhaskarray Barot engaged in a scheme to defraud his former employer of approximately $4.4 million through fake invoices designed to resemble those received from legitimate vendors of the company. Barot used his position as a procurement manager at the company to process the fraudulent invoices for payment.

When doing so, he often affixed the fake invoices to email messages that he, in some cases, sent in the names of employees of the company's real vendors so that it would appear as though the real vendors were seeking payment on the fake invoices.

The fake invoices, however, stated that payment should be made to entities with names that often differed slightly from those of the real vendor companies. Barot then incorporated companies and opened bank accounts in the names of some of the entities listed for payment on the fake invoices so that he could collect the payments that the company made on the fake invoices.

Baro repeated these fraudulent tactics with more than a dozen fictitious entities and caused payment from the company on approximately 40 fake invoices, totaling approximately $4.4 million.
(Source)

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

New York Lawyer Censured For Using TeamViewer Remote Access To Snoop On Former Firm's Business Activity - June 6, 2023

The New Jersey Supreme Court censured Lawyer Justin Scott in a May 31, 2023 order. The New Jersey Supreme Court's disciplinary review board had recommended a censure in an October 2022 decision.

Scott and Charles Bratton practiced elder law in a Haddonfield, New Jersey, firm that came to be known as Bratton Scott. Scott and Bratton disagree on whether Scott was fired, as was permitted by their partnership agreement, or whether he left on his accord.

A new attorney at Bratton's firm noticed that something was amiss when he was working on the laptop once used by Scott, according to the disciplinary review board. The new lawyer said he saw an incoming connection to a remote access program called TeamViewer, and his "computer screen started moving" without his input.

The new lawyer took control of his mouse, and the connection ended. When the new lawyer searched for TeamViewer on his computer, he saw that it had a connection named "Justin Scott." The new lawyer reported the incident to Bratton.

A forensics computer company investigated and reported that Scott had accessed the computer system six times in 2019, all after Scott left the firm. The remote access would allow Scott to see any application on the laptop, including the Time Matters program. The investigation found that Scott had not copied or transferred files using TeamViewer.

Bratton and Scott differed on whether TeamViewer was installed by the firm's technology company or by Scott. Scott said the company installed the program, so that he could work remotely. Bratton said his office didn't use TeamViewer, and he wouldn't have authorized its installation. A technology company representative also said it had not installed TeamViewer.

Scott initially said the TeamViewer access was accidental. But five months later, Scott admitted that access was intentional, and he logged in to see calendars. (Source)

2 Employees Of Mental Health Treatment Provider Charged With Sabotaging Network While Patients Were Receiving Treatments - June 27, 2023
Nathan Howe and Patrick Morin were employed by the non-profit until April 2021 and October 2020.

Between September and December of 2021, Howe and Morin conspired to access records of the non-profit's employees, listen to and view conversations between the employees, and create and deploy a computer program designed to impede a Vice President of the non-profit's use of the network.

In November 2021, Howe allegedly accessed the computer network and transmitted a command that shut down the network for the non-profit's Westborough campus where individuals were receiving in-patient treatment. By allegedly shutting down the network,

Howe made the non-profit's electronic medical records system inaccessible at its sites across Massachusetts, impairing or potentially impairing the medical examination, diagnosis, treatment and care of patients.

It is further alleged that, between July 2018 and November 2020, Howe and Edmonds-Morin conspired to commit wire fraud by obtaining cell phones from a cell phone provider which were intended for the non-profit's staff and, instead, selling the cell phones to third parties for personal profit, typically in the amounts of hundreds of dollars per phone. (Source)

Former CEO Charged For Fraudulently Entering Competitor Laboratory And Destroying / Stealing Equipment – June 2, 2023
Eric Leykin was the CEO of a clinical reference laboratory based in New Jersey.

Leykin's laboratory competed against the victim business, another clinical reference laboratory also based in New Jersey.

On June 30, 2022, Leykin bought a prepaid mobile phone and called an employee of the victim business, claiming to be a technician with a vendor that the victim business used to service its laboratory equipment.

On that false pretense, Leykin scheduled an appointment with the victim business' employee to supposedly service some of the victim business' laboratory equipment.

On July 1, 2022, the date of the supposed service appointment, Leykin went to the victim business and proceeded to destroy a significant amount of the victim business' laboratory and computer equipment, in at least one instance doing so with a USB kill stick device. Leykin also stole multiple hard drives housed within the victim business' equipment. (Source)

NOTE OF IMPORTANCE:
The employee let the CEO from competitor company into the facility. Did the company not have any procedures for verifying outside service calls were legit?

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.

The indictment says that on Dec. 22, 2022, Cook maliciously damaged by means of fire at 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)

THEFT OF ORGANIZATIONS ASSESTS

UPS Employee Conspired With 2 Individuals To Steal Cell Phone Shipments Valued At $142,000+ Over 3 Year Period - June 27, 2023
From 2018 to 2021, Parmod Kumar and Reecha Saini enlisted at least one employee at a UPS facility in Harrisburg, PA to steal packages that they believed contained smartphones. Kumar and Saini then paid the employee for the phones and arranged for their sale at a convenience store in Harrisburg. The conspiracy involved the theft of phones with a total value of over $142,000. (Source)

Former FedEx Driver Pleads Guilty To Selling Firearms He Stole From Packages On His Truck - June 16, 2023
Frank O'Toole previously worked as a FedEx delivery truck driver out of a FedEx facility in Middleborough, Boston.

Between October 2021 and June 2022, O'Toole stole three packages he was responsible for delivering, each containing a firearm intended for a Federal Firearms Licensee. On Aug. 9, 2022 and Aug. 12, 2022, O'Toole sold the three firearms to an undercover agent during two separate controlled purchases. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

CFO, Controller, Corporate Officers Charged In For Role In $53 Million Fraud Scheme Involving Pandemic Relief - June 28, 2023
14 people who allegedly bilked the Paycheck Protection Program, a COVID-era financial program, and numerous financial institutions out of more than $53 million in loan proceeds have been federally charged. This case is the largest investigated by the Pandemic Response Accountability Committee (PRAC) Fraud Task Force to date.

According to a series of indictments unsealed Wednesday, several of the charged defendants purportedly operated a group of affiliated recycling companies, including Mammoth Metal Recycling, Elephant Recycling, Gulf Coast Scrap, 4G Metals, 4G Plastics, 5G Metals, Level Eight, Sunshine Recycling, L.K. Industries, , NTC Industries, West Texas Equipment, and West Texas Scrap.

They allegedly submitted at least 29 Paycheck Protection Program (PPP) loan applications that fraudulently inflated payroll expenses, doctoring bank statements and Internal Revenue Service tax forms to falsely reflect business income. They then routed PPP loan funds through a series of bank accounts to create a false paper trail of payroll expenses. (Source)

Former Executive Director Sentenced To Prison For Role In $3 Million Of Health Care Fraud Scheme Involving 21 Individuals - June 14, 2023

Alfonzo Bailey founded Eye for Change Youth and Family Services in 2016 and provided a wide range of services to clients such as mental health counseling, case management, job training, and supportive housing.

Beginning in 2017, Bailey and his defendants conspired together to execute a scheme to defraud The Ohio Department of Medicaid by obtaining payments on false claims.

To execute the scheme, Bailey encouraged his staff to create false progress notes for counseling services not actually rendered to patients in order to bill the Ohio Department of Medicaid. Search warrants were executed at Eye for Change Youth and Family Services in 2020 which led to the indictments of 21 defendants including Bailey. Bailey must pay restitution of $3,465,643.33. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Hospital Emergency Medical Technician Sentenced To Prison For Drug & Gun Crimes, Including Selling Fentanyl That Resulted In Coworker's Death - June 14, 2023

Cruz Noel Quintero was employed as an Emergency Medical Technician at a Long Beach hospital, He shipped cocaine, methamphetamine, and other drugs across the country, and he distributed them locally out of a Long Beach residence.

In May 2019, in the parking lot outside the hospital's emergency room, Quintero sold a white powder he claimed was cocaine for $100 to a hospital coworker who was planning to go on a weekend trip to Las Vegas with her partner, a former Nurse at the Long Beach hospital and volunteer firefighter. The following morning, the couple sampled the white powder, not knowing that it in fact was fentanyl. Both of them passed out. One of the victims was later pronounced dead.

After learning that Quintero sold the fatal dose, law enforcement searched two residences in Long Beach and discovered Quintero's illicit drug-trafficking operation. Across both residences, they found 13 firearms that included two machine guns, two short-barreled assault rifles, and nine other guns, some of which were loaded.

One of the residences, which Quintero used as his base of operations, was littered with drug-trafficking paraphernalia, including over ten pounds of cutting agents used to dilute the quality of the drugs he sold and a hydraulic press used to manufacture kilogram bricks of cocaine. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS 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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE EXTORTION

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Found Guilty Of $1 BILLION Of Fraud Resulting In Failure Of Bank - February 10, 2023

A federal jury has returned a verdict of guilty on all 46 counts against former First NBC Bank President and CEO Ashton J. Ryan, Jr. and not guilty on all 7 counts against former First NBC Bank Senior Vice President Fred V. Beebe.

From 2006 through April 2017, Ryan and others conspired to defraud First NBC Bank through a variety of schemes. Ryan was the President and CEO of the Bank for most of its existence. Ryan and others, conspired to defraud First NBC Bank by disguising the true financial status of certain borrowers and their troubled loans, concealing the true financial condition of the Bank from the Board of Directors, auditors, and examiners.

When members of the Board or the Bank's outside auditors or examiners asked about loans to these borrowers, Ryan and others made false statements about the borrowers and their loans, omitting the truth about the borrowers' inability to pay their debts without getting new loans. As a result, the balance on these borrowers' loans continued to grow resulting, ultimately, in the failure of First NBC. The Bank's failure cost the Federal Deposit Insurance Corporation's deposit insurance fund slightly under $1 billion. (Source)

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

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

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

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy. Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports. This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guility 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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern. The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,600+ 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 POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The NITSIG Provides Guidance And Training The Membership And Others On;

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

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

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

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

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

The NITSIG had to suspend meetings and the ITS&E in 2020 to 2022 due to the COVID outbreak. We are working on resuming meetings in the later part of 2023, and looking at holding the ITS&E in 2024.

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

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the: White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines,) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

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

With over **10+** years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

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

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org