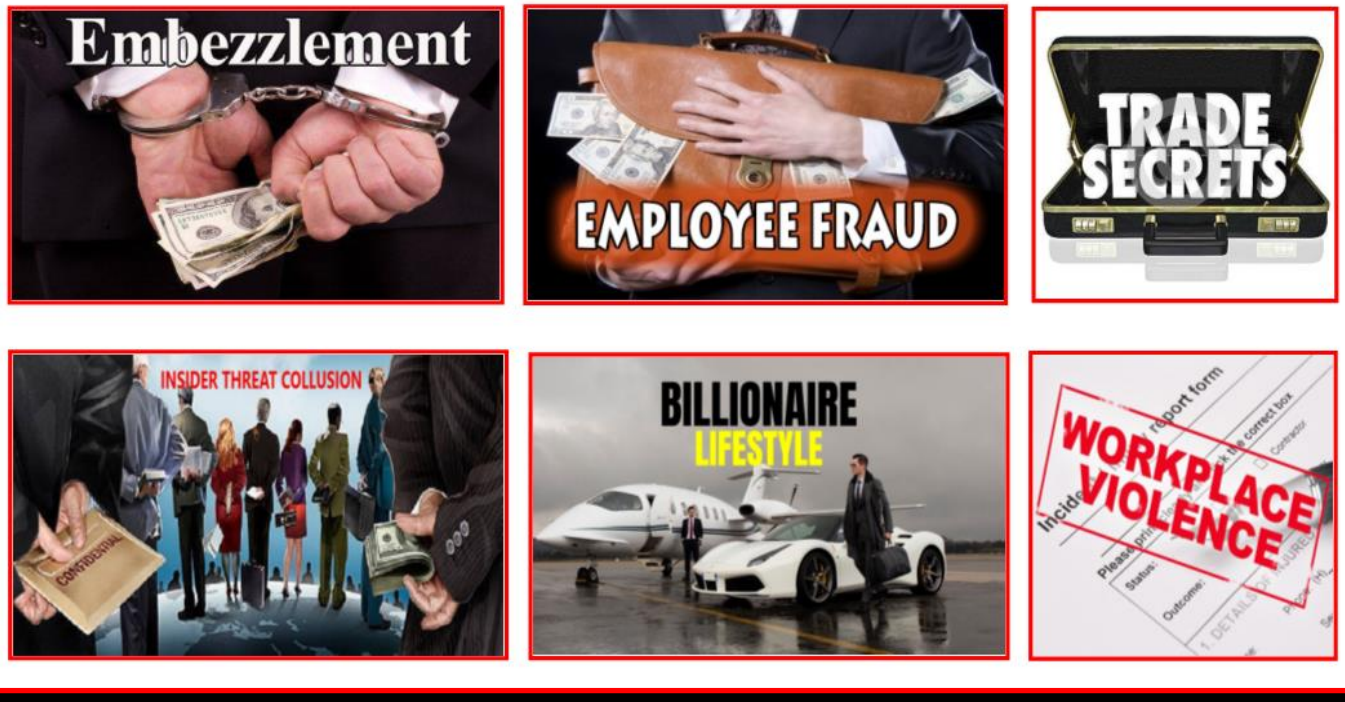
INSIDER THREAT INCIDENTS SPOTLIGHT REPORT

Providing A 360 View Of The Insider Threat Problem

Produced By

National Insider Threat Special Interest Group
U.S. Insider Risk Management Center Of Excellence
Insider Threat Defense Group



The Human Operating System (Brain) Is Very Sophisticated

Underestimating The Motivations & Capabilities Of A Negligent, Disgruntled, Malicious Or Opportunist Employee Can Have Severe Impacts For Organizations

October 29, 2023

www.insiderthreatincidents.com

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT

OVERVIEW

Since July 2021, the National Insider Threat Special Interest Group (NITSIG) / Insider Threat Defense Group have produced monthly Insider Threat Incidents Reports. These **EYE OPENING** reports provide clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)

These reports are recognized and used by Insider Risk Program Managers working for major corporations, as a **TRUSTED SOURCE** for education to gain support from CEO's, C-Suite, Key Stakeholders and Supervisors for detecting and mitigating Insider Threats. These reports provide the justification, return on investment and funding needed for developing, managing or optimizing an Insider Risk Management Program.

Inputs to this report were also provided by the U.S. Insider Risk Management Center Of Excellence (USIRMCOE) Advisory Board Members (ABM's). The USIRMCOE was established in 2023, by the Founder / Chairman of the NITSIG Jim Henderson. USIRMCOE ABM's are recognized industry Insider Risk Management Experts that have managed U.S. Government Insider Threat Programs, or who are currently managing or supporting Insider Risk Management Programs for private sector companies. Additional information on the USIRMCOE and its mission will be forthcoming.

This comprehensive report provides a **360 DEGREE VIEW** of the many different types of Malicious Actions employees' have taken against their employers. These **SEVERE IMPACTS** can be caused by **Just 1 Employee**, **Multiple Employees' In Collusion**, or **Employees' In Collusion With External Co-Conspirator(s).**

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

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

This report also serves as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization. As this report will reflect, not reporting employees' of concern can have catastrophic consequences, such as a company going out of business.

The many examples listed below clearly substantiate the need to enhance security controls (Non-Technical, Technical) to detect and mitigate Insider Risks / Threats, or the importance of implementing an Insider Risk Management Program for your organization.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting your organization from employee risks / threats.

TABLE OF CONTENTS

U.S. GOVERNMENT / STATE GOVERNMENTS

U.S. State Department Government Contractor Arrested On Espionage Charges To Aid Foreign Government - September 21, 2023

Abraham Lemma worked as an IT administrator for the Department of State, and as a Management Analyst for the Department of Justice. In those positions, Lemma was granted a TOP SECRET security clearance and granted access to classified systems.

Between Dec. 19, 2022, and Aug. 7, 2023, Abraham Lemma copied classified information from intelligence reports and deleted the classification markings from them. Lemma then removed the information, which was classified as SECRET and TOP SECRET, from secure facilities at the Department of State.

Lemma used an encrypted application to transmit classified national defense information to a foreign government official associated with a foreign country's intelligence service. In these communications, Lemma expressed an interest and willingness to assist the foreign government official by providing information. In one communication, the foreign official stated, "It's time to continue your support." Lemma responded, "Roger that!" In other chats, the foreign official tasked Lemma to focus on information related to particular subjects, and Lemma responded "absolutely, I have been focusing on that all this week." The classified information Lemma transferred to the foreign official included satellite imagery and other information regarding military activities in the foreign country and region. (Source)

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)

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)

U.S. Government Contractor Sentenced To Probation / Home Confinement For Stealing $55,000+ Worth Of Government Property And Selling On eBay - January 4, 2023

Dennis Gamarra was employed as a contractor working at the United States Department of Commerce (DOC) within the International Trade Administration (ITA), at an office in Washington, D.C.

Gamarra largely worked to provide information technology (IT) support to the ITA and through his employment had access to certain government furnished equipment, including Microsoft Surface tablet devices belonging to DOC and issued to DOC employees

Gamarra stole at least one Microsoft Surface Tablet, worth $1,370, removing it from ITA's offices, advertising it for sale online through his eBay account, and ultimately re-selling it to another individual through eBay.

Starting in November 2019, Defendant Gamarra began working as a contractor for the Library of Congress (LOC), at an office in Washington, D.C. While at LOC, providing IT support services. While at LOC, Gamarra removed at least 29 separate Dell laptops from LOC that he knew to belong to LOC, cumulatively worth a total of approximately USD $55,590, advertised them on eBay, and ultimately resold them to different customers through that account. (Source)

State Of California Social Services Administration Employee Sentenced To Prison For Role In $973,000 Fraud Scheme By Using Clients' Stolen Identities - September 18, 2023

From August 2010 to June 2019, John Tran and his co-conspirators used the stolen information to fraudulently obtain money from the federal government, the State of California, the County of Orange and financial institutions.

The Orange County Social Services Administration employed Tran from July 1994 until October 2018. Tran abused his position of public trust to steal PII belonging to agency clients as well as other individuals, many of whom were recent immigrants to the United States.

Tran and his co-conspirators used the stolen PII to file false federal and state tax returns in the names of identity theft victims, fraudulently obtaining welfare benefits, underreporting income, and falsely claiming deductions on their personal tax returns, and opening credit cards and other lines of credit in the names of the identity theft victims. Proceeds from the schemes were laundered and structured to avoid detection by law enforcement and banks.

Tran also used the stolen identities of two victims to open fraudulent bank accounts, open credit cards, and open social services cases. For example, in September 2014, Tran opened a credit card account in another person's name and used that card for personal expenses, including for items such as skin care products, Costco purchases, and sports gambling.

Tran in 2007 charged approximately $14,000 to a credit card in the name of one victim after he convinced the victim to allow him to use the victim's credit card. The victim, who was a recent immigrant to the United States and one of Tran's SSA clients, believed that he had to let Tran use the credit card because Tran was a powerful government official who had control over the victim's families' SSA benefits.

In addition to opening at least 12 fraudulent bank and credit card accounts, Tran fraudulently created and managed SSA benefits cases for family, friends, and for himself, obtaining state benefits for which he and others were not entitled.

In total, along with the $973,153 in fraudulently obtained tax refunds, Tran defrauded two victims out of approximately $44,604, and defrauded the Orange County Social Services Administration out of approximately $92,531. (Source)

And Many More.....

DEPARTMENT OF DEFENSE

$35 Million Navy Bribery, Fraud And Corruption Scandal – 2018 To 2022

Leonard Glenn Francis, a Malaysian defense contractor, pleaded guilty to bribing scores of Navy officials with cash, prostitutes and other gifts, such as hotel stays, airfare and electronics. so they would provide him classified or inside information, which he used to defraud the Navy, and to win lucrative contracts for his Glenn Defense Marine Asia company.

This incident is considered the worst corruption scandal in Navy history. Civilian authorities have filed criminal charges against 33 people. According to the Navy, an additional 550 active-duty and retired military personnel — including about 60 admirals who have come under scrutiny for possible violations of military law or ethics rules. The Navy says it has cleared more than half of those personnel, but has substantiated misconduct by about 70 people so far. It is keeping most of their names a secret.

Between 2006 and 2013, Francis handed out $1 million in lavish meals, alcohol and Cuban cigars, among other gifts. At his parties, naval officers reveled in the attention of an armada of prostitutes. Francis hosted such feasts and sex parties on 45 separate occasions over a span of seven years. He has pleaded guilty to bribery and defrauding the military of $35 million. Some officials believe, however, that the figure may have been significantly higher. (Source)

Former Government Contractor Owner Sentenced To Prison For Paying $460,000+ In Bribes To Air Force Contracting Official - December 8, 2022

Ryan Dalbec is the owner of Best Choice Construction LLC (Best Choice).

Dalbec agreed to pay over $460,000 in bribes to former U.S. Air Force Contracting Official, Brian Nash II, in exchange for confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson Air Force Base and Joint Base Elmendorf-Richardson (JBER).

The confidential bidding information Nash provided helped Dalbec and Best Choice win some of those contracts, including a $6,850,000 construction contract related to the F-35 aircraft program at Eielson Air Force Base. Dalbec and his wife, Raihana Nadem, also helped Nash launder the bribery proceeds through family members and third-party bank accounts to conceal the nature and source of the funds. (Source)

Former NSA Employee Pleads Guilty To Attempted Espionage / To Release Top Secret Classified Information - October 23. 2023

From June 6, 2022, to July 1, 2022, Jareh Dalke was an employee of the National Security Agency (NSA) where he served as an Information Systems Security Designer.

Dalke admitted that between August and September 2022, in order to demonstrate both his "legitimate access and willingness to share," he used an encrypted email account to transmit excerpts of three classified documents to an individual he believed to be a Russian agent.

In actuality, that person was an FBI online covert employee. All three documents from which the excerpts were taken contain NDI, are classified as Top Secret//Sensitive Compartmented Information (SCI) and were obtained by Dalke during his employment with the NSA.

On or about Aug. 26, 2022, Dalke requested $85,000 in return for all the information in his possession. Dalke claimed the information would be of value to Russia and told the FBI online covert employee that he would share more information in the future, once he returned to the Washington, D.C., area.

Dalke subsequently arranged to transfer additional classified information in his possession to the purported Russian agent at Union Station in downtown Denver.

Using a laptop computer and the instructions provided by the FBI online covert employee, Dalke transferred five files, four of which contain Top Secret NDI. The other file was a letter, which begins (In Russian & Cyrillic Characters) "My friends!" and states, in part, "I am very happy to finally provide this information to you. . . . I look forward to our friendship and shared benefit. Please let me know if there are desired documents to find and I will try when I return to my main office." The FBI arrested Dalke on Sept. 28, moments after he transmitted the files. (Source)

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.

In 2017, 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. 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)

U.S. Air Force Base Director Sentenced To Prison For 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)

U.S. Air Force Civilian Employee Sentenced To Prison To $2.3 Million+ Bribery And Government Contract Fraud Scheme Over 11 Years - April 25, 2023

Keith Seguin, a former civilian employee at Randolph Air Force Base in San Antonio, admitted to receiving millions of dollars in bribes in connection with a government contract fraud scheme that spanned more than a decade and impacted hundreds of millions of dollars in contract awards.

QuantaDyn Corporation is a software engineering company based in Ashburn, Virginia. Its owner, David Bolduc and Seguin all conspired to secure government contracts. Seguin used his position to steer lucrative contracts and sub-contracts to QuantaDyn for aircraft and close-air-support training simulators.

Seguin, who was intimately involved in the government contracting process, leaked confidential competitor proposals to a prime contractor who would then subcontract the work to QuantaDyn. He also leaked confidential government budget information to prime contractors and to QuantaDyn, enabling them to maximize profits at government expense. Seguin admitted to accepting more than $2.3 million in bribes from Bolduc and QuantaDyn from 2007 to 2018. (Source)

U.S. Navy Service Member Sentenced To Prison For $2 Million Insurance Fraud Scheme - October 17, 2023

Christopher Toups, who at the time of his crimes was a Chief Petty Officer in the U.S. Navy. He admitted that he and others defrauded an insurance program meant to compensate service members who suffered serious and debilitating injuries while on active duty.

Participants in the scheme obtained approximately $2 Million in payments from fraudulent claims submitted to Traumatic Service Members Group Life Insurance Program (TSGLI). Toups personally obtained about $400,000. TSGLI was funded by service members and the Department of the Navy.

Toups admitted that from 2012 to 2015, he conspired with his then spouse Kelene McGrath, Navy Dr. Michael Villarroel, and others to obtain money from the United States by making claims for life insurance payments based on exaggerated or fake injuries and disabilities. (Source)

Navy IT Manager Sentenced To Prison For Hacking a Computer Database, Stealing 9,000 People's Identities & Selling Information For $160,000 In Bitcoin - October 16, 2023

Marquis Hooper is a former Navy IT Manager.

In August 2018, Hooper opened an online account with a company that runs a database containing the PII for millions of people. The company restricts access to the database to businesses and government agencies that have a demonstrated, lawful need for the PII. Hooper, however, opened his database account by falsely representing to the company that the Navy needed him to perform background checks.

After Hooper opened his database account, he added his wife and co-defendant, Natasha Chalk, to the account. They then stole over 9,000 people's PII and sold it to other individuals on the dark web for $160,000 in bitcoin. At least some of the individuals to whom Hooper and Chalk sold the PII used it to commit further crimes. (Source)

U.S. Navy Sailor Pleads Guilty To Receiving $14,000+ In Bribes And Transmitting Sensitive U.S. Military Information To Chinese Intelligence Officer - October 10, 2023

Petty Officer Wenheng Zhao worked at Naval Base Ventura County in Port Hueneme, and held a U.S. security clearance.

Between August 2021 and at least May 2023, Zhao admitted receiving at least $14,866 in at least 14 separate bribe payments from the intelligence officer. In exchange for the illicit payments, Zhao surreptitiously collected and transmitted to the intelligence officer sensitive, non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao admitted he entered restricted military and naval installations to collect and record this information.

Zhao specifically admitted to transmitting plans for a large-scale maritime training exercise in the Pacific theatre, operational orders, and electrical diagrams and blueprints for a Ground / Air Task Oriented Radar system located in Okinawa, Japan.

Zhao further admitted to using sophisticated encrypted communication methods to transmit the information, destroying evidence, and concealing his relationship with the intelligence officer. (Source)

Former U.S. Army Employee Arrested For Accepting $400,000+ In Bribery And Kickback Scheme Involving Defense Contracts - May 15, 2023

Young Kim while acting in his capacity as Chief of the Design Branch (2017-2021) at Army Garrison Yongsan / Casey in Korea (USAG-Y/C), developed a scheme to enrich himself through bribes and kickbacks from various manufacturers and suppliers of parts used in U.S. Army contracts.

Kim helped ensure that certain Army contracts included the use of parts manufactured or supplied by specific companies. Some of these parts included blast doors, blast valves, shock mounts, and shock isolators (Equipment Designed To Protect Army Personnel In The Event Of An Attack). In return, the companies manufacturing or supplying those parts collectively sent over $400,000 in kickbacks to Kim. A significant portion of these funds were laundered through bank accounts controlled by Kim's adult relatives, including one account held in the name of a shell company and were ultimately used to enrich Kim and to pay for bills and expenses incurred by Kim. (Source)

Former Army Employee Charged For Theft Of $800,000+ Of Military Heavy Equipment - May 10, 2023
From November 2021 through December 2021, Tamilo Fe'a stole military heavy equipment, including vehicles, semi-trailers, generator trailers, flatbed trailers, refrigerator trailers, armored office trailers, tractors, and box vans from the Hawthorne Army Weapons Depot in Hawthorne, Nevada. The total value of the stolen property was over $800,000.00.

From September 2020 to August 2021, Fe'a made about 69 transactions with a fuel fleet credit card for his personal benefit at various gas stations in Nevada, Arizona, New Mexico, and California. (Source)

2 Army Officers (Husband, Wife) Plead Guilty To The Theft Of $2 Million+ Of Government Property / Sold Equipment And Profited $1. 8 Million+ - April 21, 2023
2 Army Officers (Husband, Wife) have been convicted in a multi-year activity involving the theft of more than $2 Million in government property. Chief Warrant Officer Three (CW3) Christopher Hammond pled guilty to theft / possession of government property and money laundering. His wife Major Heather Hammond was convicted for spending money laundering proceeds and aiding and abetting.

CW3 Hammond used his position to requisition government property intended for his unit at Ft. Bragg. The property was never logged into inventory at the base but was instead sold by Hammond to various individuals. In a two-year period, CW3 Hammond received at least $1.8 million in wire transfers related to the sales, which he deposited into bank accounts controlled by him and his wife. The investigation traced about 200 items sold by CW3 Hammond or held in his home as having been issued to Hammond's military unit.

Major Hammond knowingly allowed use of her bank accounts, even suggesting the use of her accounts so the money would not go into Chief Hammond's bank account. The fraud was uncovered when a supplier noticed that items procured under a government contract were being sent in for warranty repairs by a private individual. (Source)

And Many More.....

LAW ENFORCEMENT
Special Agent For Homeland Security Investigations Sentenced To Prison For Accepting $50,000 In Kickbacks From Informant - October 23, 2023
Anthony Sabaini was assigned to the Oakbrook Terrace, Illinois field office of Homeland Security Investigations (HSI), a criminal investigative unit within DHS.

Sabaini maintained a corrupt relationship with an HSI confidential informant and tipped off the informant to sensitive investigations conducted by other law enforcement agencies, including the FBI and DEA. In exchange for Sabaini's protection, the informant paid Sabaini at least $50,000. Sabaini also stole cash from drug dealers and pocketed money from HSI that had been earmarked for investigative activity.

Sabaini deposited more than $250,000 into a bank account for which he was the sole signatory. He made the deposits in more than 160 transactions, with the amount of each deposit being less than $10,000. The deposits were structured in an effort to evade federal reporting rules, which require financial institutions to notify the U.S. Department of the Treasury about transactions of more than $10,000.

The evidence also showed that Sabaini lied on official HSI memoranda in 2017 and 2018 to protect his corrupt relationship with the informant. (Source)

Las Vegas Police Officer Convicted Of Committing 3 Casino Robberies Taking $164,000+ - July 14, 2023
Caleb Rogers stole approximately $73,810 from a casino in the western part of Las Vegas on November 12, 2021. A few months later, on January 6, 2022, he robbed a casino in North Las Vegas of approximately $11,500. In both robberies, he walked directly to the casino's cashier cage and demanded money from the cashiers.

The third robbery occurred on February 27, 2022, in which Rogers ran toward two casino employees in the sportsbook area and yelled: "Get away from the money. I've got a gun. I will shoot you".

Rogers climbed over the counter and shoved one of the employees to the floor, before grabbing approximately $78,898 and placing it into a bag. Rogers fled when the employees triggered an alarm. As Rogers ran toward the parking garage, a casino security officer tackled him.

Rogers drew a .357 caliber revolver and, with his finger on the trigger, threatened: "I'm going to shoot you!" Security officers were able to disarm Rogers and restrain him until Las Vegas Police Officers arrived. The officers arrested Rogers and seized his firearm. Checking the revolver's serial number, officers learned that it belonged to the LVMPD. (Source)

Police Chief Sentenced To Prison For Accepting $175,000+ In Bribes For $5.7 Million Contract Award - August 5, 2022
Tim Vasquez is the former San Angelo Texas Chief of Police.

Vasquez used his official position to help Dailey & Wells Communications, Inc., a radio system vendor, land a $5.7-million-dollar contract with the City of San Angelo, Texas.

In return, Dailey & Wells and its affiliates funneled Vasquez and his band, Funky Munky, more than $175,000. Dailey & Wells and its affiliates also provided him tickets for luxury suites at Dallas Cowboys and San Antonio Spurs games, tickets for a luxury suite at Journey concert, and free use of a luxury condominium at Alteza Condos in San Antonio.

Dailey & Wells cut a $10,000 check to Funky Munky Band. Vasquez deposited the funds into his personal checking account. For 8 years Vasquez received yearly payments of approximately $8,000 from Dailey & Wells or its affiliates, either made out to Vasquez or his band. (Source)

3 Individuals (2 Of Them Police Officers) Are Charged In Role With Conspiracy To Steal Government Property From Army Depots - May 25, 2023
Kelvin Battle, Steve Bonner and Shane Farthing are each charged with one count of conspiracy to steal United States property. Battle and Bonner are also each charged with an additional count related to specific instances of stealing or selling property stolen from the Anniston Army Depot (ANAD). Six other individuals have pleaded guilty or agreed to plead guilty to offenses related to the theft of property from ANAD.

Battle and Farthing, who were police officers at ANAD, and other civilian employees of the Directorate of Emergency Services, stole military property from warehouses at ANAD. Bonner acted as a middleman, selling stolen property directly to buyers and delivering stolen property to the owner of a military surplus store. The stolen items included equipment that was designed to be attached to military weapon systems to provide operators with instant nighttime engagement capabilities and / or improved target acquisition. (Source)

Police Chief Sentenced To Prison For Illegally Trafficking 200 Fully Automatic Machine Guns / Receiving $11,000+ In Kickbacks - June 2, 2022

Dorian LaCourse is the former Chief of Police in the Village of Addyston, Ohio. 2 federally licensed firearms dealers in Indiana were his coconspirators, Johnathan Marcum and Christopher Petty.

LaCourse, Marcum, and Petty, illegally exploited a law enforcement exception to the federal ban on the possession or transfer of fully automatic machine guns.

As Chief of Police, LaCourse signed multiple demonstration letters falsely stating that the Village of Addyston Police Department was interested in purchasing various types of machine guns, including military-grade weapons, and asking that Marcum and or Petty give the demonstration. Marcum and Petty then sent the letters to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to obtain the weapons. The Village of Addyston has approximately 1,000 residents, and one full-time police officer.

LaCourse also placed direct orders for German-made machine guns that were purported to be paid for by the Police Department. In fact, the purchases were fully funded by Marcum and Petty and intended to bypass restrictions on the importation of such weapons by anyone other than the police or the military.

The Addyston Police Department was never authorized to purchase any of the machine guns, and the Indiana gun dealers never provided any demonstrations of machine guns to the police department. Instead, the gun dealers resold the machine guns at a significant profit. In some instances, a gun dealer resold illegally acquired machine guns for five or six times the purchase price. The conspirators purchased or caused the importation of approximately 200 fully automatic machine guns. LaCourse received over $11,500 from the gun dealers for his role in the scheme. (Source)

And Many More.....

COVID-19 FRAUD SCHEMES INVOLVING EMPLOYEES

Chief Finance Officer, Controllers, Corporate Officers Charged In For Role In $53 Million COVID-19 Fraud Scheme - June 28, 2023

14 people were involved in a COVID-19 Paycheck Protection Program fraud scheme that involved $53 Million in loan proceeds being fraudulently obtained. This case is the largest investigated by the Pandemic Response Accountability Committee Fraud Task Force to date.

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 Small Business Administration Employee Sentenced To Prison For Role In $11 Million COVID-19 Relief Fraud / $2.3 Million Kickback Scheme - May 25, 2023

Lakeith Faulkner was an employee of the Small Business Administration (SBA).

He used his position to assist borrowers in submitting over $11 Million worth of fraudulent loan applications for Economic Injury Disaster Loans, which were intended to help small businesses recover from the economic impacts of the COVID-19 pandemic. In return for his assistance in submitting the fraudulent loan applications, those borrowers paid Faulkner and his co-defendant, Norman Beckwood, $2.3 Million. (Source)

Department of Veterans Affairs Nurse Sentenced To Prison For Role In Leading $3.5 Million COVID-19 Fraud Scheme - August 23, 2023

From April 2020 through March 2021, Heather Huffman lead and organized several others, including family members and close friends, in a conspiracy to defraud at least five state workforce agencies, including the Virginia Employment Commission, the Washington State Employment Security Department, and the California Employment Development Department, of more than $3.5 Million in unemployment insurance benefits.

Huffman's conspiracy specifically targeted benefits that had been expanded to offset the economic impacts of the COVID-19 pandemic. Huffman and others filed false and misleading applications in the names of identity theft victims, witting co-conspirators, and inmates of state and federal prisons. Huffman and her conspirators included in these applications materially false wage and employment histories and false contact information, such as physical and mailing addresses, email addresses, and phone numbers, that did not, in fact, belong to the purported applicants.

Huffman and her conspirators submitted more than 220 applications in the names of more than 120 individuals to at least five different states through which they sought to receive more than $3.5 Million and actually obtained more than $2 Million.

Huffman's sentencing was originally scheduled for November 29, 2022, but she failed to appear that day without notice or explanation. Prior to her disappearance, Huffman took measures to flee prosecution and conceal her whereabouts, including depleting her bank accounts, selling her vehicle, and turning her phone off. Through means unknown, Huffman obtained the PII of a real person, assumed that person's identity, and procured counterfeit government identification and credit cards in the name of her false alias.

Following Huffman's disappearance, the United States Marshals Service (USMS) opened a fugitive investigation. This extensive, months-long investigation uncovered evidence that the defendant, under a false identity, was living and working as a registered nurse in Kansas. On March 4, 2023, approximately 95 days after Huffman's flight from prosecution, she was apprehended by the USMS in Kansas at an Extended Stay hotel. (Source)

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

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

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

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

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

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme.

Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman. Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. **Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items**. (Source)

Former IRS Revenue Agent And 5 Five Other Individuals Charged In $3 Million COVID-19 Kickback Fraud Scheme - May 10, 2023

6 defendants have been charged with a variety of crimes in connection with an alleged scheme to obtain millions of dollars by submitting fraudulent loan applications through the U.S. government's Payroll Protection Program (PPP).

Central to the allegations in the charging documents is the role of Frank Mosley a former IRS Revenue Agent and City of Oakland Tax Enforcement Officer. Mosley conspired with others to submit fraudulent PPP-loan applications and then, after securing the proceeds from the loans, used his share of the illegally-obtained proceeds for personal investments and expenses. The defendants, including Mosely, received approximately $3 million as a result of submitting fraudulent loan applications under the PPP program. (Source)

U.S. Postal Service Employee Sentenced To Prison For Role In $2 Million COVID-19 Relief Fraud Ring - August 17, 2023

Tiffany McFadden was a U.S. Postal Service employee.

McFadden was the leader of a scheme responsible more than 400 fraudulent Paycheck Protection Program PPP loan applications. McFadden and her co-conspirators manufactured false and fraudulent documents claiming businesses that in truth did not exist and did not lose money due to the COVID-19 pandemic. As a result, McFadden and others received more than $2,000,000 in loans, often approximately $20,000 at a time, that they were not entitled to. Those loans were later fully forgiven by the U.S. Government.

McFadden and others recruited loan applications by word of mouth, manufactured false and fraudulent tax and business documents, and then applied for and obtained forgiveness for the loans. In exchange for her services, McFadden received a portion of the fraudulently obtained funds. (Source)

NASA - JPL Employee Pleads Guilty To COVID-19 Economic Relief Program Fraud ($151,000) / Used Some Proceeds To Grow Marijuana - July 24, 2023

Armen Hovanesian was a Cost Control And Budget Planning Resource Analyst for the NASA-Jet Propulsion Laboratory (JPL).

From June 2020 to October 2020, Hovanesian submitted three loan applications in the names of business entities under his control to the Economic Injury Disaster Loan Program (EIDL), a program administered by the Small Business Administration (SBA) that provided low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters, including businesses impacted by the COVID-19 pandemic.

Hovanesian certified to the SBA under penalty of perjury that he would "use all the proceeds" of the loans for which he applied and caused others to apply for "solely as working capital to alleviate economic injury caused by disaster" consistent with the terms and limitations of the EIDL program. **But Hovanesian instead applied those proceeds toward his own prohibited personal benefit to repay a personal real-estate debt and fund his illegal marijuana cultivation.** Hovanesian fraudulently caused the SBA to transfer via interstate wire EIDL proceeds totaling $151,900. (Source)

And Many More.....

FRAUD BY BANK EMPLOYEES

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

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

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

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent.

In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts.

Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding". (Source)

Former 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 a bank., 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)

Wells Fargo Former Bank Manager Pleads Guilty To Embezzling $1.2 Million+ From Bank Customers - October 12, 2023

Brian Davie worked for Wells Fargo from March of 2014 until he was fired in June 2019.

Davie used his position as a Manager at the branch to conduct unauthorized transactions. Davie had access to customer files containing information about bank account balances. Davie hid his criminal activity by repeatedly exchanging cashier's checks until they were small enough to cash without triggering banking reporting requirements.

Some of Davie's victims had dementia or had limited English skills and did not understand banking transactions.

In at least one case, Davie failed to file the paperwork to install a victim's relative as a co-signer on the victim's accounts. That failure prevented the relative from being able to monitor the account and detect the fraudulent transactions.

Davie deposited some of the stolen money in an account he created in the name of a relative's business. He made some of the cashier's checks payable to that relative or to the business account he created. Much of the money was withdrawn as cash.

In all Davie embezzled $1,279,840 from victim accounts. Wells Fargo reimbursed victims for their losses. Judge Settle will determine the amount of restitution at sentencing. (Source)

Wells Fargo Banker Sentenced To Prison For Role In $3.8 Million International Money Laundering Kickback Scheme - February 27, 2023

Leopoldo Aguilera abused his position of trust as a personal banker with Wells Fargo Bank by opening bank accounts with false identities and wire transferring millions of dollars to Mexico. Aguilera conducted these transactions in exchange for thousands of dollars in cash payments from the criminal organization. The FBI's investigation linked these funds to the sale of narcotics by a Mexican drug cartel, specifically the sale of multi-kilogram amounts of fentanyl in the Midwest.

Aguilera admitted to opening 26 bank accounts for the money laundering organization, including eleven that were created by Aguilera using fictitious identities.

Aguilera used his position as a personal banker with Wells Fargo Bank to knowingly enter false names, passport numbers, and dates of birth on the fictitious bank accounts. These 11 fictitious accounts alone were used by the criminal organization to wire transfer a total of $3.8 million to Mexico. A majority of those wire transfers were conducted by Aguilera himself. Aguilera's use of these fictitious accounts was identified by Wells Fargo and brought to the attention of the FBI. Agents arrested Aguilar and disrupted the scheme shortly after. (Source)

Wells Fargo Branch Manager Sentenced To Prison For Helping Drug Trafficking Ring Launder $400,000+ / Received Kickbacks - March 8, 2023

Stephen Reyna was the Branch manager of a Wells Fargo in Texas. While serving in that position and utilizing his position and knowledge of the banking industry, Reyna assisted a drug trafficking organization to launder $410,000 in drug sale proceeds.

The organization would transport multi-kilogram cocaine loads from the Rio Grande Valley to northern states. Upon successful delivery, thousands of dollars in drug proceeds would then be dispersed through multiple Wells Fargo bank accounts in the northern states.

Reyna would coordinate with multiple co-conspirators in the Rio Grande Valley to launder the funds through their accounts at Wells Fargo. Reyna ensured the proceeds were successfully withdrawn from his branch.

Co-conspirators would frequently pay Reyna in cash right after he helped them get their drug proceeds out of the bank. Reyna ultimately admitted he suspected the funds were from illegal activity, including narcotics trafficking. (Source)

And Many More.....

HEALTH CARE FRAUD BY EMPLOYEES

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 a strategically coordinated 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 a software and services companies conspired to generate and sell 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)

Hospice Medical Director Sentenced To Prison For Role In $150 Million Fraud / Kickback Scheme - September 27, 2023

From 2009 to 2018, Jesus Cadena served as the Medical Director of the Merida Group, a large health care company that operated dozens of locations throughout Texas. He was a physician but the Texas Medical Board later suspended his medical license.

Also convicted in 2019, were co-conspirators Rodney Mesquias, Henry McInnis and Francisco Pena.

Evidence at the trial showed that the Merida Group marketed their hospice programs through a group of companies.

They enrolled patients with long-term incurable diseases such as Alzheimers and dementia as well as patients with limited mental capacity who lived at group homes, nursing homes and in housing projects. In some instances, Merida Group marketers falsely told patients they had less than six months to live. They also sent chaplains to the patients based on the false pretense they were near death.

In order to bill Medicare for these services, the Merida Group hired Cadena and other medical directors, but made payment of their medical director fees contingent upon an agreement to certify unqualified patients for hospice.

In addition to regular medical director payments, Cadena received luxury trips, bottle service at exclusive nightclubs and other perks in exchange for his certification of unnecessary hospice patients. In exchange for these illegal kickbacks, Cadena himself certified over $18 million in unnecessary hospice services as part of the over $150 million conspiracy. (Source)

Former Medical Office Nurse Charged For Role In $1.2 Million+ Health Care Fraud Conspiracy / Received $90,000 In Kickbacks- February 28, 2023

Ashley Valenti was previously an Advanced Practice Nurse at a medical office in Pennsville, New Jersey during this fraud conspiracy.

Valenti was previously charged with Vincent Tornari and Brian Sokalsky in a 33 count indictment in June 2020.

Tornari hired Valenti's live-in boyfriend to be a Sales Representative for his company which promoted compound medications, even though Valenti's boyfriend had no background or experience in medicine and pharmaceutical sales.

Tornari and Valenti's boyfriend had an agreement that the boyfriend would receive a commission on all prescriptions authorized by Valenti. Valenti then authorized numerous medically unnecessary prescription medications associated with Tornari and her boyfriend, including her patients, staff members and co-workers at the medical office where she worked, and her children, for the sole purpose of financially benefiting herself, her boyfriend, and Tornari.

In exchange for authorizing the prescriptions, Valenti's boyfriend paid her half of his commissions that he received from Tornari.

As a result of the scheme, health insurance paid over $1.2 Million for medically unnecessary medications and Valenti received over $90,000 in kickbacks for signing the prescriptions. (Source)

Sales Representative For Medical Diagnostic Laboratory Sentenced To Prison Role In $4.6+ Million Health Care Fraud / $350,000 Kickback Scheme - October 3, 2022

Steven Monaco was a leader of two related fraud schemes that resulted in millions of dollars of loss to public health insurance plans.

In the first scheme, Monaco, as a Sales Representative for a medical diagnostic laboratory, orchestrated a kickback scheme with a doctor, Daniel Oswari. Monaco arranged for Oswari's medical assistant to be placed on the payroll of the laboratory while continuing to work as a medical assistant for Oswari's practice. In exchange, Oswari referred all his lab work to the laboratory for testing between late 2013 and 2016, and Monaco received $36,000 in commissions from the laboratory.

In the second fraud scheme, Monaco and his conspirator, pharmaceutical sales representative Richard Zappala, discovered that certain insurance plans including New Jersey state and local government plans, paid for very expensive compounded prescription medications between 2014 and 2016.

Monaco and Zappala organized a scheme in which they received a percentage of the insurance reimbursement for compounded medication prescriptions that they arranged. As a result of this scheme, Monaco received approximately $350,000 and caused a loss of over $4.6 million to the insurance plans. (Source)

Pharmacy Employee Admits Participating In $2.4 Million Kickback And Bribery Scheme - December 22, 2022

Srinivasa Raju had various responsibilities at the Morris County Pharmacy, including coordinating prescription deliveries and soliciting business.

From January 2019 through February 2021, Raju worked with other pharmacy personnel to pay kickbacks and bribes to medical employees in two different doctors' offices in Jersey City, New Jersey.

In exchange, those employees steered numerous, high-value prescriptions to the pharmacy where Raju worked. Raju and his conspirators paid as much as $150 for each prescription and used various tactics to conceal many of those bribe payments. Overall, the pharmacy received over $2.4 million in Medicare reimbursement payments based on prescriptions derived from the kickback scheme. (Source)

And Many More.....

PERSONAL ENRICHMENT - EMPLOYEES LIVING THE LIFESTYLES OF THE RICH AND FAMOUS USING THEIR EMPLOYERS MONEY

Former Company Chief Financial Officer Charged For Using $35 Million In Company Cash To Invest In Cryptocurrency Venture He Owned - May 17, 2023

Nevin Setty was hired as the CFO of a private company in March 2021.

The company was raising capital for its work in multiple rounds of funding. The company adopted an investment policy statement that called for company cash to be invested only in fixed income instruments payable in U.S. dollars. Only certain types of conservative investments were approved.

Despite the fact that Shetty helped draft the policy and disseminate it, he moved $35 million in company funds to a cryptocurrency platform he controlled as a side business.

Shetty created that side business, called HighTower Treasury, in February 2022. In March 2022, he was told he could not continue as CFO at his employer due to concerns about his performance. Shortly after he got this news, Shetty secretly transferred the funds out of the company's account.

Between April 1 and 12, 2022, Shetty transferred $35,000,100 of his employer's money to an account for HighTower. No one else at the company knew of these transfers.

The cryptocurrency investments soon began declining and by May 2022, the value of the $35 million investment was nearly zero. (Source)

Morgan Stanley Financial Advisor Sentenced To Prison For Executing A $7 Million Ponzi Scheme / Used Funds For Personal Use - May 24, 2023

Shawn Good was employed as a registered representative and investment advisor for Morgan Stanley Smith Barney, LLC in Wilmington.

From 2012 to February 2022, Good executed a scheme to obtain money through an investment fraud commonly known as a Ponzi scheme. Specifically, Good solicited investments from business clients and others for purported real estate projects and tax-free municipal bonds, touting these opportunities as low-risk investments that would pay returns of between 6% and 10% over three- or six-month terms.

At least 12 victims invested approximately $7,246,300 based on false statements and misrepresentations made by Good. Instead of investing in land development or bonds, **Good used the money for personal expenditures including his Wilmington residence; a condominium in Florida; luxury vehicles including a Mercedes Benz, a Porsche Boxster, a Tesla Model 3, an Alpha Romeo Stelvio, and a Lexus RX350; fine dining; and vacations to Paris, France; Cinca Terra, Italy; Jackson, Wyoming; Las Vegas, Nevada; and other destinations**. To lend credibility to the Ponzi scheme and to elude detection, Good also used a portion of investor funds to make payments to earlier investors. (Source)

Finance Director That Worked At 2 Non-Profit Organizations Sentenced To Prison For Embezzling $3 Million+ Over 11 Years / Used Funds To Pay For Credit Cars Bills, Gambling, Vacations, Etc. - September 5, 2023

In 1999 Susana Tantico began working for a non-profit that provides healthcare to underserved populations. Ultimately, Tantico became the non-profit's Finance Director.

Between 2011 and June 2020, Tantico secretly embezzled millions of dollars from the healthcare organization. Bank records are available only for the period beginning in December 2016. Between December 2016 and 2020, Tantico stole nearly $2.3 million from the healthcare non-profit. She used the non-profit's debit and credit cards to withdraw $1.6 million at casinos for gambling. She also used the debit and credit cards to pay for personal vacations, such as a $26,000 family trip to Florida, and trips to Las Vegas and San Diego. Tantico also used the healthcare non-profit's debit and credit cards for more than $83,000 worth of purchases at Nordstrom, and $40,000 worth of purchases at Apple stores.

After running up these expenses, Tantico used the non-profit's funds to pay the credit card bills and disguised the payments as legitimate expenses. For example, she categorized expenses for one vacation as "pharmacy supplies" in the accounting system.

In 2020, Tantico went to work as Finance Director for a different non-profit, one with a focus on criminal justice issues.

Tantico used more than $485,000 of the non-profit's funds for gambling at casinos. She transferred $21,000 from the non-profit to pay her home mortgage. She also transferred money to her personal bank account. Tantico then altered the bank records to hide the embezzlement.

At one point, Tantico was questioned by one of the organization's banks about the pattern of withdrawals at casinos. She claimed that the non-profit held youth programs at the casinos, and that the withdrawals were for cash prize giveaways. In all, Tantico stole nearly $893,000 from the non-profit.

The non-profit has incurred $132,000 in costs to forensically audit its books, fix its accounting procedures and records, and reply to vendors. (Source)

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

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 Financial Controller Sentenced To Prison For Embezzling $690,000+ For 9 Years / Used Money For Vacations, Paying Debts, Home Improvements, Etc. -May 4, 2023

From 2012 to December of 2021, Tammy Scudder devised and participated in a scheme to defraud her employer of more than $600,000.

Scudder used her position as Controller to exploit a vulnerability in the company's accounting system. Scudder knew that the company's group health plan bank account was difficult to double-check because it was funded based upon the total amount of the weekly claims on the list it received from another company, rather than by each claim individually. Scudder accessed the company's accounting software to generate and print a company check to herself, signed using another employee's signature stamp. After Scudder printed the check, she concealed the theft by altering and falsifying the victim company's accounting records.

Scudder used the stolen money to take vacations, pay off personal debts, fund her children's educational expenditures, and by make improvements to her residence. Between February 2012 and December 2020, Scudder generated 154 false and fraudulent checks totaling $693,708.75. (Source)

Former Employee Of 38 Years Pleads Guilty To Embezzling $2.2 Million Over 9 Years / Used Money To Pay Credit Card Bills - March 15, 2023

Christine Fletcher worked for a company and various other entities owned by her employer for approximately 38 years. She managed her employer's various Bank of Oklahoma Financial (BOKF) and Trust Company of Oklahoma bank accounts. She prepared and provided financial statements and related information to the company's tax preparer.

Fletcher admitted that from December 2012 to May 2021, she embezzled funds for her own personal gain from her employer in the approximate amount of $2,188,870. (Source)

Former Energy Company Executive Sentenced To Prison For $15 Million Investment Fraud / Used Funds For Personal Expenses - January 24, 2023

Between November 2012 and May 2015, Joey Dodson engaged in a scheme to defraud investors while serving as the Executive Chairman and Managing Partner of Citadel Energy, which provided fluid-management services to oil and gas companies.

In his role, Dodson was responsible for raising funds, controlling the bank accounts, and disseminating financial information to investors for three limited partnerships affiliated with Citadel.

As part of the scheme, Dodson made materially false and misleading representations and omissions to prospective and existing investors about the intended use of investor funds, the status of a potential acquisition by a private-equity firm, and Dodson's own compensation.

After inducing victims to invest, Dodson pooled the funds from the limited partnerships and conducted multiple transfers between Citadel related accounts in order to divert investor funds for his own benefit and to conceal his actions. Dodson fraudulently raised over $15.6 million from more than 50 investors and misappropriated $1.3 million in investor funds, which he used to pay for his personal expenses and to repay earlier investors in unrelated entities known collectively as Duke Equity. After Dodson's misappropriation was discovered, the limited partnerships were placed into bankruptcy and the investors suffered a total loss of their investments. (Source)

Employee Promoted To CEO Sentenced To Prison For Embezzling $15 Million+ From Employer / Used Company Credit Cards To Pay For $6 Million In Personal Expenditures - November 3, 2022

Donna Steele began working for company's shipping department in 1999. Over the next 20 years, Steele was promoted to various positions within the company, including to the position of Chief Executive Officer (CEO), which she held until she was terminated in January 2020.

From 2013 to January 2020, Steele executed an extensive scheme to defraud her employer, a privately held U.S. based subsidiary of a foreign company that manufactures carbide products.

While serving as Vice President and later as CEO, Steele used her positions to embezzle funds from the company in a number of ways, including through fraudulent company credit card purchases, company checks, Quickbooks transactions, and wire transfers.

Steele used company credit cards to pay for $6 million in personal expenditures, including to make high-end retail store purchases, to pay for a family wedding, and to make purchases related to Opulence by Steele, a luxury clothing and boutique company owned by the defendant.

Steele also issued and caused to be issued to herself approximately 98 checks totaling more than $2.8 million from the company's bank accounts, which Steele deposited into her personal bank account. Steele caused 127 fraudulent and unauthorized wire transfers to be executed as Quickbooks transactions, transferring more than $4.7 million from the company's bank accounts to her personal bank account.

During the same time period, Steele executed at least 117 fraudulent and unauthorized bank wires, totaling more than $2.2 million, from the company's bank accounts to her personal bank account. (Source)

Former Company IT Director Charged With Embezzling $1 Million+ For 10 Years / Used Funds For Himself, Family, Friends - December 7, 2022

Juan Hicks who the IT Director for the AT Wall Companies. Hicks used his access to the company's computer network; his purchasing authority for computer hardware, software, and other equipment; his management authority over the company phone systems and internet services; and his access to company credit cards to orchestrate schemes in which he obtained goods and services for himself, family members, and friends, and paid personal expenses for Hicks and his family.

During a cyber-attack which took place in March 2022, AT Wall Companies hired forensic analysts to determine the source of the attack and to identify vulnerabilities.

According to company officials, during that inquiry, Hicks refused to provide his computer and passwords, as per company policy. An internal investigation provided by the company to the police department, Homeland Security Investigations, and the United States Attorney's Office subsequently revealed that Hicks had allegedly embezzled over $ 1 Million from the company since 2012.

Hicks' alleged fraud included getting reimbursement for false expense reports and fraudulent invoices he created; enrolling family members on the company's wireless phone service plan and issuing company phones to himself and six family members; purchasing airline and entertainment tickets for himself and family members; and using a company credit card to make purchases at retail stores and payments for auto repairs. (Source)

And Many More.....

UN-AUTHORIZED SALARY ENRICHMENT FRAUD SCHEMES BY EMPLOYEES

Equifax Monitored 1,000 Remote Workers, Fired 24 Found Employee That Were Found To Be Juggling 2 Jobs - October 14, 2022

"Equifax conducted an investigation into a number of employees suspected of holding dual, full-time employment that conflicted with their roles at our company," Equifax spokesperson Kate Walker said in a statement. "As a result, several employees who violated our company code of conduct and outside employment policy, which were in effect at the time of the investigation, were recently terminated." (Source)

Former Chief Financial Officer Pleads Guilty To Embezzling $3 Million+ By Increasing Salary - June 29, 2023

From 1998 to 2017 David Katz worked for Durand and Associates (D&A), a property management company that specialized in servicing homeowner associations (HOA's). Katz started as an accountant and eventually becoming Chief Financial Officer (CFO).

Between 2012 and 2017, Katz embezzled over $3 million from D&A and its client HOAs.

As the CFO of D&A, Katz was responsible for the payroll. He 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)

Senior Vice President of Finance Charged With Embezzling $2.7 Million+ Company By Inflating His Salary / Bonuses - August 25, 2023

Aubrey Shelton embezzled approximately $2.7 Million from his employer, a San Francisco-based automobile services and technology company where Shelton worked as the Senior Vice President of Finance.

From November 2013 and through December 2021, Shelton used his exclusive control over the company's payroll processing software to inflate his salary and bonuses over the authorized amounts and to direct the payroll processor to cause the company to pay him large amounts categorized as Executive Loan, Misc. Reimbursement, Mileage Reimbursement, or other reimbursements that were not authorized or expended by Shelton. (Source)

Law Firm Financial Controller Defrauds Firm Out Of $1.4 Million+ By Inflating Salary Over 3 Years - August 23, 2023

Christiane Irwin who worked for a law firm and was responsible for submitting payroll each week.

She falsely inflated her salary, which was set at approximately $140,000 annually. In accordance with her fraudulent payroll submission, the firm's payroll vendor transferred her purported pay from the firm's bank account into her bank account every two weeks. Over the course of three years, from 2019 to 2021, Ms. Irwin took home $1.48 Million in fraudulently obtained funds. (Source)

Former Office Manager For 27 Years - Sentenced To Prison For Embezzling $700,000 By Increasing Salary / Used Funds To Purchase Cars, Renovate Home, Etc.- December 15, 2022

Pamela Smith was employed as an Office Manager for a family-owned construction company for 27 years. As part of her duties, Smith was responsible for handling the company's payroll and had access to the company's business accounts.

Dating back to at least 2008, Smith made payments on multiple personal credit cards directly from the company's business bank accounts without her employer's permission. Beginning in 2013, Smith altered her payroll to increase her weekly salary without her employer's permission. She began with a $1,000 per week increase, and, by the time her employer discovered the fraud, she was embezzling $2,000 per week.

In total, Smith stole at least $700,000 from her employer. She used the funds to purchase cars, renovate her home, and otherwise live above her means. Smith took numerous steps to conceal her criminal activity, including transferring money between business bank accounts, limiting access to the company's monthly banking statements, and altering the company's general ledger.

The court also entered an order of forfeiture for Smith's residence, which was substantially remodeled using stolen funds, as a substitute asset. (Source)

Former Director Of Finance Sentenced To Prison For Embezzling $650,000 For 10+ Years / He Padded Budget, Increased His Salary - August 4, 2022

Chris Benavides was the former Finance Director at La Jolla Music Society. He embezzled more than $650,000 from the non-profit over a 10-year period.

Benavides oversaw the budgeting process and human resources. Over the years he regularly claimed that many staff salary increases were not possible due to budgetary constraints. However, during that same period, Benavides was stealing for himself an average of about $65,000 per year.

Forensic review revealed that over the years Benavides' theft became more and more sophisticated. He regularly planned his theft in advance of each fiscal year, budgeting for the amount that he would take over the next 12 months and imbedding those expenses in various budget lines. This ensured that none of the expense lines would show conspicuous variances when reviewed by other staff, board members or auditors. It was also discovered he regularly signed or forged checks for his personal benefit and made false entries in the books to hide what he was doing. (Source)

Former Dermatologist Office Manager Charged With Embezzling $490,000 By Giving Herself Unauthorized Salary Increases / Used Funds For Rent, Tuition, Travel, Etc. - December 15, 2022

Tianna Keller used her position as the Dermatologist Office Manager, and her authority to sign office documents, and her position as benefits manager to orchestrate schemes to enrich herself, her son, and a friend.

Keller defrauded the practice of approximately $490,000. She allegedly did this by giving herself unauthorized salary increases totaling approximately $185,061; adding family members and a friend to the payroll and providing them with unauthorized gross wages totaling approximately $46,703; failing to deposit nearly $108,000 in patient cash payments; issuing dozens of checks payable to herself and others, signing the name of the medical practice's owner without his permission; and using company funds and credit cards as payment for her rent, a daughter's tuition, restaurant, grocery, retail and other personal and travel expenses; and personal services.

Keller authorized continued enrollment and payment for family medical insurance coverage for her son, Brandyn Coffman and his family, even after his self-termination as a data clerk at the medical practice, authorizing payment of nearly $40,000 for this coverage. Blue Cross Blue Shield paid more than $14,000 in claims submitted by Coffman and his family. (Source)

Former Human Resources Director Sentenced To Prison For Stealing $118,000 In Employee Paycheck Scheme - November 18, 2020

The former Human Resources Director for Oconee County, Georgia has admitted to stealing taxpayer money in a complicated paycheck scheme.

Sherry Turner-Seila was employed as the Human Resources Director for Oconee County. As such, she was one of the few employees with access to the County's payroll system, which transferred funds directly from the county bank account to the bank accounts of county employees.

From July 2016 to July 2019, Turner-Seila concocted a scheme where she would use that access to temporarily change a former employee's direct deposit information to her own personal bank account's direct deposit information. In all, Turner-Seila stole $118,451.80 from Oconee County taxpayers. (Source)

And Many More.....

FRAUDULENT INVOICING - SHELL COMPANY FRAUD SCHEMES BY EMPLOYEES

Former Amazon Manager Sentenced To Prison For As Mastermind In $9.4 Million Fake Invoice Fraud Scheme Involving 6 Other Employees' - July 5, 2023

Kayricka Wortham fraudulently used her position at Amazon to submit more than $10 Million in fictitious invoices for fake vendors, causing Amazon to pay approximately $9.4 million to Wortham and her other 6 co-conspirators.

From about August 2020 to March 2022, Wortham worked as an Operations Manager at the Amazon Warehouse in Smyrna, Georgia. In her position, Wortham supervised others and acted with the authority to approve both new vendors and the payment of vendor invoices for Amazon.

Wortham, who was the leader of the scheme, provided fake vendor information to unknowing subordinates and asked them to input the information into Amazon's vendor system. Once the information was entered, Wortham approved the fake vendors, enabling them to submit invoices.

Wortham approved the invoices, causing Amazon to transfer millions in fraudulent proceeds to bank accounts controlled by her and her co-conspirators.

Wortham conspired with others, including Brittany Hudson, in the scheme. Hudson was in a relationship with Wortham and owned a business. Hudson allegedly worked with Wortham to submit millions in fictitious invoices for fake vendors to Amazon. **Wortham and Hudson purchased expensive real estate and luxury cars, including a nearly $1 Million home in Smyrna, Georgia, a 2019 Lamborghini Urus, a 2021 Dodge Durango, a 2022 Tesla Model X, a 2018 Porsche Panamera, and a Kawasaki ZX636 motorcycle, all with fraudulent proceeds from the scheme.**

Wortham also recruited co-conspirators Demetrius Hines, who was in Loss Prevention at Amazon, and Laquettia Blanchard, who worked as a Senior Human Resources Assistant at the company. Hines also recruited Jamar L. James, Sr., another Operations Manager at Amazon's location in Duluth, Georgia, into the scheme. Like Wortham, James allegedly approved fake vendors and fictitious invoices, including after Wortham left Amazon in March 2022. (Source)

Former Health Care Executive Convicted Of $4 Million+ Fake Vendor Scheme Over 8 Years - October 23, 2023

Shawn Rains was an executive at OrthoNet, a healthcare claims processing company based in White Plains, New York.

Between approximately 2009 and 2017, Rains and Joseph Maharaj, another OrthoNet executive, designed and executed a scheme to defraud OrthoNet of over $4 million and to launder the fraud proceeds. Rains conspired with Maharaj and others to create fake vendors that purported to do work on behalf of OrthoNet. Rains, Maharaj and their co-conspirators then signed invoices approving payment for the fake work, and OrthoNet sent payments to the fake vendors. Rains, Maharaj and their co-conspirators then converted the money to cash to hide the source of the fraud proceeds and split it up amongst themselves. (Source)

Former Employee Pleads Guilty To Embezzling $1.7 Million Over 8 Years By Creating Fake Invoices - September 19. 2023

Gina Lonestar was a Director in the Facilities Department of Men's Wearhouse. She was promoted to Senior Director of Facilities and Corporate Services, and then to Vice President of Construction, Maintenance, and Facilities.

Lonestar admitted that, in December 2010, she devised a scheme to create a fake vendor to defraud Men's Wearhouse and later Tailored Brands (Men's Wearhouse's Parent Company) of money by submitting and approving false invoices for the fake vendor to the accounts payable department. Lonestar created a document stating the vendor was a sole proprietorship associated with a family member and then began submitting and approving invoices falsely claiming the vendor was performing work at Men's Wearhouse stores throughout California, such as inspections and handyman work. Lonestar admitted that she submitted and approved false invoices in the name of the fake vendor for approximately eight years, defrauding her employer of over $1.7 Million, which was paid to her joint checking account. Lonestar admitted that the vendor did not exist and the family member with whom she co-owed the company performed none of the work for which she provided invoices.

Lonestar's scheme ended in 2019 when the company discovered the conduct during an internal audit. (Source)

Former Accounting Manager Sentenced To Prison For Embezzling $2.5 Million+ Over 8 Years By Creating Fake Company / Used Funds For Drug Addiction - August 29,, 2023

Christin Guillory was an Accounting Manager at a manufacturing company. She stole more than $2.5 Million from her employer by transferring funds to accounts she set up in the names of fake companies and then routing the funds to her own bank accounts.

In April 2013, Guillory set up an account with payment processor Square that used a display name that made it appear it was an account of a commercial shipping company. Between 2014 and 2019, Guillory secretly paid $1,695,591 to that account and then transferred the money to her own bank accounts. She made false entries in the company books to conceal the theft.

In 2019, Guillory stopped using Square for her fraud and instead used two PayPal accounts. She gave one of the PayPal accounts a display name similar to that of her employer. For the second account, she used the name of a shipping company with which she had no affiliation. In 2020 and 2021, she caused the transfer of $604,000 to the PayPal accounts and made false accounting entries to cover her tracks. She then transferred the bulk of the money for her own use.

Becoming more brazen, between August and November 2021, Guillory transferred $247,000 directly from company accounts to her own bank accounts. Again, she made fraudulent accounting entries and reused legitimate invoices to make it appear the payments were for appropriate business purposes. In all, Guillory made at least 867 secret transactions using interstate wires that totaled $2,536,086.

Guillory used the stolen money to support her prescription drug addiction.

The scheme was detected when a financial institution reported irregularities. (Source)

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

Bhaskarray Barot was the Procurement Manager at his company.

From July 2018 to August 2022, 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. 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)

Former Chief Engineer Of Facilities For Rail System Company Charged For Role In $8 Million+ Fake Invoice Scheme - April 5, 2023

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

Pigsley also operated a separate construction company called Pigman Group.

John Rafferty was the General Manager of LJ Electric, Inc., an electrical supply vendor to which Keolis paid over $17 million between 2014 through 2021.

Between July 2014 and November 2021, Pigsley and Rafferty allegedly defrauded Keolis of over $4 million through a false LJ Electric invoicing scheme. Rafferty purchased vehicles, construction equipment, construction supplies and other items for Pigsley, Pigman Group and others. Pigsley then directed Rafferty to recover the cost of these items by submitting false and fraudulent LJ Electric invoices to Keolis. The fraudulent LJ Electric invoices included a percentage profit that Rafferty allegedly kept for himself.

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

Former IT Director Admits To Embezzling $1 Million+ For 10 Years With False Invoices & Expense Reports / Used Money For Personal Expenses - March 16, 2023

Juan Hicks is the former IT Director for a metals fabrication and supply company.

Hicks admitted that he defrauded AT Wall Companies by: creating false invoices and expense reports payable to himself; altering legitimate credit card statements to make purchases appear to be business expenses, when, in fact, they were for Hicks' personal expenses; issuing company phones to himself and six family members and then enrolling the phones on the company's wireless phone service plan; by submitting invoices and using company credit cards to purchase airline and entertainment tickets for himself, family members and friends; and by also using those company cards to make purchases at retail stores and auto repair centers.

Hicks' criminal conduct came to light in March 2022, when AT Wall Companies hired forensic analysts to determine the source of a cyber attack and to assess vulnerabilities in its computer system. Hicks refused to provide his computer and passwords, as per company policy. Information and analysis provided by the company to the Warwick Police Department, Homeland Security Investigations, and the United States Attorney's Office subsequently revealed that Hicks had embezzled over one million dollars from the company since 2012. (Source)

Former County Employee Pleads Guilty To Stealing $1.7+ Million In County Funds By Falsifying Invoices - January 3, 2023

Kevin Gunn pleaded guilty to defrauding Wayne County in Detriot, out of nearly $2 million in taxpayer funds. Gunn and another county employee John Gibson, engaged in a scheme to make unauthorized purchases of generators and other power equipment from retailers in southeast Michigan which they sold for personal profit.

Between January 2019, and August 2021, Gunn and Gibson solicited approved Wayne County vendors to purchase generators and other power equipment from local retailers on behalf of Wayne County. The vendors would then submit invoices for these items to Wayne County. In order to conceal the scheme to defraud, Gunn instructed the vendors to falsify the invoices they submitted to the Roads Division, and list items the vendors were authorized to sell to the county under their contracts, rather than the generators and power equipment they were unlawfully acquiring at Gunn's and Gibson's request. Roads Division employees would then approve and pay each vendor's invoice. After these fraudulent purchases were verified and approved by Roads Division employees, Gibson took possession of the equipment, paid Gunn for the items, and resold the generators and other items for personal profit.

A review of invoices from Wayne County vendors revealed that between January 16, 2019, and August 3, 2021, Wayne County vendors purchased 596 generators, and a variety of other power equipment including lawnmowers, chainsaws, and backpack blowers. The purchase of these items was not authorized under any vendor contract with Wayne County nor were the items ever provided to or used by Wayne County. The total value of equipment purchased as part of the scheme was approximately $1.7 million in taxpayer funds. (Source)

And Many More.....

EMPLOYEE FRAUD, EMBEZZLEMENT, BRIBERY, KICKBACKS, EXTORTION, MONEY LAUDERING

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Role In $1.6 BILLION+ Bribery & Money Laundering Scheme / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

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

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

Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating Managing Director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite, conspired to pay more than a BILLION dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

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

Through its work for 1MDB during that time, Goldman Sachs received approximately $600 Million in fees and revenues, while Ng received $35 Million for his role in the bribery and money laundering scheme. In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

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

Former Government Contractor Owner Sentenced To Prison For Paying $460,000+ In Bribes To Air Force Contracting Official - December 8, 2022

Ryan Dalbec is the owner of Best Choice Construction.

Dalbec agreed to pay over $460,000 in bribes to former U.S. Air Force Contracting Official, Brian Nash II, in exchange for confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson Air Force Base and Joint Base Elmendorf-Richardson.

The confidential bidding information Nash provided helped Dalbec and Best Choice win some of those contracts, including a $6,850,000 construction contract related to the F-35 aircraft program at Eielson Air Force Base. Dalbec and his wife, Raihana Nadem, also helped Nash launder the bribery proceeds through family members and third-party bank accounts to conceal the nature and source of the funds. (Source)

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 remediation of 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 his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. (Source)

Former California Department Of Transportation Manager Pleads Guilty To Bid Rigging & Receiving $800,000+ In Bribes (Cash, Home Remolding, Etc.) - April 11, 2022

Choon Foo Keith Yong was a former contract manager for the California Department of Transportation (Caltrans). He pleaded guilty for his role in a bid-rigging and bribery scheme involving Caltrans improvement and repair contracts.

Yong and his co-conspirators engaged in a conspiracy, from early 2015 through late 2019, to thwart the competitive bidding process for Caltrans contracts to ensure that companies controlled by Yong's co-conspirators submitted the winning bid and would be awarded the contract.

Yong received the bribes in the form of cash payments, wine, furniture and remodeling services on his home. The total value of the payments and benefits Yong received exceeded $800,000. (Source)

Former Coal Company Vice President Charged In $143 Million Foreign Bribery, Money Laundering And Wire Fraud Scheme - March 31, 2022

Charles Hobson was the Vice President of a coal company in Pennsylvania. Hobson was responsible for the company's business relationship with Al Nasr, an Egyptian state owned and controlled company.

Hobson engaged in the bribery and money laundering scheme between late 2016 and early 2020. Hobson and a sales intermediary paid bribes to Al Nasr officials in Egypt to obtain approximately $143 million in coal contracts. Hobson conspired to secretly receive a portion of the commissions paid to the sales intermediary as kickbacks. (Source)

And Many More.....

EMPLOYEE COLLUSION WITH OTHER EMPLOYEES OR EXTERNAL CO-CONSPIRATORS

13 Individuals (NYPD Police Officer, Doctors, Attorney, Others) Charged In $100 Million Healthcare Fraud, Money Laundering, And Bribery Scheme / One of the Largest No-Fault Automobile Insurance Fraud Takedowns in History - January 12, 2022

Of the 13 defendants, 8 are charged in an indictment detailing conspiracies to commit healthcare fraud, money laundering, bribery, and obstruction, making false statements to federal authorities, and aggravated identity theft.

The 13 defendants charged are alleged to have collectively perpetrated one of the largest no-fault insurance frauds in history. In carrying out their massive scheme, among other methods, they allegedly bribed 911 operators, hospital employees, and others for confidential motor vehicle accident victim information. With this information, they then endangered victims by subjecting them to unnecessary and often painful medical procedures, in order to fraudulently over bill insurance companies. (Source)

20 Individuals Involved In DMV Corruption / Bribery Scheme (DMV Employees', Trucking School Owners) - November 14, 2022

This incident included bribery of public officials, identity fraud, unauthorized access of computers, and conspiracies to commit those offenses. The individuals involved included corrupt DMV employees who took bribes, trucking school owners and affiliates who bribed them and others who participated in the conspiracies.

The individual involved helped put unqualified commercial drivers on the nation's highways operating large commercial vehicles even though those drivers had not passed the necessary written and driving tests. DMV employees accepted bribes to enter fraudulent test scores for applicants who had not even taken the tests or who could not pass them. Various trucking schools in California looked for corrupt DMV employees they could bribe to help failing or unqualified students get their commercial licenses anyway. In total, hundreds of fraudulent commercial driver license permits and licenses were issued as a part of these schemes, jeopardizing public safety. (Source)

Program Manager For District Of Columbia's Department Of Youth Rehabilitation Services Sentenced To Prison For Role In Identity Theft And Tax Fraud Scheme Involving 130 People - May 3, 2016

Marc Bell is a former employee of the District of Columbia's Department of Youth Rehabilitation Services (DYRS). Bell admitted taking part in a massive and sophisticated identity theft and false tax return scheme that involved an extensive network of more than 130 people, many of whom were receiving public assistance.

The scheme involved the filing of at least 12,000 fraudulent federal income tax returns that sought refunds of at least $42 million from the U.S. Treasury. The false tax returns sought refunds for tax years 2005 through 2013 and were often filed in the names of people whose identities had been stolen, including the elderly, people in assisted living facilities, drug addicts and incarcerated individuals. Refunds also were sent to people who were willing participants in the scheme. The refunds listed more than 400 taxpayer addresses located in the District of Columbia, Maryland and Virginia. (Source)

Armored Truck Driver Found Guilty For Role In Staged Armored Truck Robbery Of $1.9 Million - March 22, 2023

Terry Pollard was convicted for conspiracy to commit bank larceny and bank larceny. The convictions arose from a January 2021 incident during which Pollard and his four codefendants staged an armed robbery of a Garda armored cash transport truck carrying $1.9 million in South Carolina.

Pollard's codefendants Quantavius Murphy, Anthony Burge, Thomas Calhoun, and James Sewell all previously pleaded guilty to the charges.

In early January 2021, Sewell, a Garda Armored Truck Driver, recruited Pollard and the other codefendants to stage his robbery. After formulating the plan over Snapchat, Pollard, Murphy, Burge, and Calhoun traveled from Cedartown to Sewell's apartment in North Charleston on January 15, 2021. Later that day, they drove around North Charleston looking for the best location to stage the theft. On January 16, 2021, Sewell parked his truck full of money outside an ATM in North Charleston. Pollard and the other codefendants approached Sewell and pretended to restrain him at gunpoint. They then loaded $1.9 Million in cash into black trash bags and immediately fled back to Cedartown. (Source)

And Many More.....

THEFT OF TRADE SECRETS / EMPLOYEES SPYING FOR CHINA

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

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

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

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

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

Former Samsung Electronics Executive Charged With Stealing $233 Million Worth Of Trade Secrets For China Chip Factory - June 12, 2023

SK Hynix was a Vice President at South Korea's Samsung Electronics.

Hynix is accused of illegally acquiring Samsung data to build a rival factory 1 mile away from a Samsung chip manufacturing facility in Xian, China.

Prosecutors said they estimated the theft of data to have caused at least 300 billion won ($233 million) worth of losses for Samsung Electronics.

Prosecutors said they had indicted six other people for their suspected involvement, including an inspection company employee accused of leaking the architectural plan of Samsung's semiconductor factory. (Source)

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 stole ADI trade secrets 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. 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. 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)

Former Employee Arrested For Stealing Sensitive Software From His U.S. Employers To Build A Competing Business In China - May 16, 2023

Liming Li worked for Company #1 from 1996 to 2018 and then worked at Company #2 from 2018 until November 2019. Shortly before beginning his employment with the Company #2, Li and his wife established their own business, JSL Innovations, which was based out of their home.

After Company #2 terminated Li, company security discovered that Li was using his company-issued laptop to attempt to download files from Company #2's root directory onto his personal external hard drive. Company security searched Li's company-issued laptop and found a folder labeled China Government.

That folder allegedly contained numerous documents showing Li's efforts to participate in the PRC's Thousand Talents Program and to use JSL Innovations to provide services and technology to PRC business and government entities related to the export-controlled and trade secret technology that Li took from his former employers.

In March 2020, Li entered into an agreement with a PRC-based manufacturing company to serve as its Chief Technology Officer. Li's agreement with this employer required him to spend at least six months per year in the PRC.

Six months later, FBI agents executed a search warrant at LI's home and found numerous digital devices containing millions of files belonging to Company #1 and Company #2 and containing the source code for those companies' proprietary software. Although the source code files had been developed by and belonged to these companies, some of the files had been moved into folders labeled "JSL" or "JSL Projects." (Source)

Former GE Power Engineer Sentenced To Prison For Stealing Trade Secrets Using Steganography - January 3, 2023

Xiaoqing Zheng was employed at GE Power in Schenectady, New York, as an Engineer specializing in turbine sealing technology. He worked at GE from 2008 to 2018.

Zheng and others in China conspired to steal GE's trade secrets surrounding GE's ground based and aviation based turbine technologies, knowing or intending to benefit the PRC and one or more foreign instrumentalities, including China based companies and universities that research, develop, and manufacture parts for turbines.

Zheng used steganography (A Method To Hide A Data File Within Another File) to remove the files from the GE network. Through the steganography technique, Zheng placed the trade secret files into an innocuous looking digital photograph of a sunset. Zheng then e-mailed the photograph file of the sunset, which secretly contained the hidden GE trade secret files, from his GE email address to his personal e-mail address. (Source)

Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Start Company In China - May 9, 2022

From December 2012 through Aug. 31, 2017, Dr. Xiaorong You was employed as Principal Engineer for Global Research at Coca-Cola, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various bisphenol-A-free (BPA-free) technologies.

You stole valuable trade secrets related to formulations for BPA-free coatings for the inside of beverage cans. You was granted access to the trade secrets while working at The Coca-Cola Company in Atlanta, Georgia, and Eastman Chemical Company in Kingsport, Tennessee. The stolen trade secrets belonged to major chemical and coating companies including Akzo-Nobel, BASF, Dow Chemical, PPG, Toyochem, Sherwin Williams, and Eastman Chemical Company, and cost nearly $120,000,000 to develop.

You stole the trade secrets to set up a new BPA-free coating company in China. You and her Chinese corporate partner, Weihai Jinhong Group, received millions of dollars in Chinese government grants to support the new company (Including A Thousand Talents Plan Award). (Source)

Oil And Gas Company Employee Sentenced To Prison For Conspiracy To Steal Trade Secrets - November 15, 2022

Joshua Decker was a controller for the valve division of an oil and gas company that serves customers engaged in drilling and production.

In March 2017, while employed as the company, Decker registered with the Oklahoma Secretary of State a new company called Legacy Valve Systems (Legacy). He then recruited co-workers at the victim company to join him at Legacy.

From March to September 2017, Decker conspired to steal numerous trade secrets from the victim company. Decker and others acting at his direction downloaded the technical drawings, material specifications, and manufacturing instructions for the victim company's valves, and Decker transmitted the victim company's detailed financial information, including cost information and sales by product and customer by email to himself. Decker provided the victim company's drawings to an individual who copied them and replaced the victim company's logo with a Legacy logo to begin manufacturing and selling valves to compete with the victim company. Decker then directed others to delete all their text messages and files, including messages on an encrypted application, to conceal their theft from the victim company. (Source)

Former Pharmaceutical Executive Accused Of Stealing Trade Secrets And Giving Them To Boyfriend Who Was CEO Of Competitor - July 11, 2022

Drug company Teva is alleging that its former Chief Of Regulatory Affairs passed trade secrets to her boyfriend, who happened to be the CEO of a competitor company Apotex.

The lawsuit alleges that over a period of about two years ending in 2016, Teva employee Barinder Sandhu copied company files onto flash drives and passed them to Apotex CEO Jeremy Desai. Sandhu was fired in October 2016.

An internal investigation revealed that Sandhu created a folder on her Teva-issued computer called My Drive, which synced to a personal cloud account, and that she uploaded 900 Teva files to that folder, including trade secrets and other confidential information. She also copied files to as many as 10 USB drives, Teva alleges. The use of cloud backup and external drives violated the confidentiality agreement she signed upon accepting employment with the company.

Teva learned of Sandhu's actions from a former Apotex employee, who reported that Apotex used the information she shared with Desai to compete against Teva. (Source)

Terminated Vice President Uses Google Remote Desktop To Steal Trade Secrets - November 24, 2015

In late 2015, Atlantic Marine Construction Company, a Virginia Beach construction company, filed a lawsuit against a former Vice President of Construction and his new employer, alleging various causes of action arising out of the VP's trade secret theft. At first glance, this lawsuit reflects a familiar scenario: a departing employee steals proprietary data on his way out and later provides it to a competitor. This case includes an interesting twist, however. Atlantic Marine alleges that the VP stole the trade secrets at issue after he was terminated, using a software tool to access his former employer's network.

The former VP allegedly stole the information at issue using Google Chrome Remote Desktop, a program that allows users to remotely access and control one computer from another over the Internet. Atlantic Marine alleges that the VP installed the program on a work computer during his employment without authorization. Then, after his termination, the VP logged on to the software with his personal Gmail address and accessed Atlantic Marine's computer network at least 16 times to view, copy, and download various trade secrets, including proposal sheets with contract details, formulas used for calculating costs, and other valuable confidential data. (Source)

And Many More.....

THEFT OF COMPANY PROPERTY BY EMPLOYEES

Contract Employee Pleads Guilty To Role In Scheme To Steal Vehicles From Airport Car Rental And Transport Them To Nearby States - February 22, 2023

From May 2021 until October, 2021, Bernard Washington worked as a contractor for the Hertz Rent A Car at the Pittsburgh International Airport.

Between May and July 2021 Washington and co-conspirators accessed the Hertz parking lot and stole approximately 24 vehicles, at least three of which were transported across state lines from Pennsylvania to other states, including Maryland, Delaware, and Virginia. Washington and his co-conspirators provided these stolen vehicles to other individuals in exchange for payment. Washington also received at least two stolen vehicles from a co-conspirator, one of which had crossed state lines after being stolen. (Source)

IT Manager Sentenced To Prison For Stealing / Selling $1.5 Million+ Of IT Equipment From Employer - October 17, 2023

Todd Erickson served as the Information Technology Manager at a telecommunications company. Erickson was responsible for submitting requests to purchase equipment, such as computers and hard drives.

From at least January 2012 through February 2019, Erickson fraudulently submitted purchase requests for computer equipment that the company did not need. Thereafter, without the knowledge or approval of his employer, Erickson sold the items to third parties. He was also ordered to pay restitution of $1,596,328. (Source)

IT Employee Pleads Guilty To Stealing 850 Laptop Computers Worth $1.9 Million+ And Selling Them / Used Funds To Purchase Ferrari - August 14, 2023

Between 2015 and 2023, Bahram Khosropanah devised and repeatedly executed a scheme to misappropriate technology assets from his employer for his own personal gain.

Khosropanah held senior positions at a company that operates convenience stores across the country. His role focused on information technology, and he was responsible for purchasing computers and other electronics for the company. Upon receiving invoices for certain purchases, Khosropanah made unauthorized material modifications to the invoices before submitting them to his accounting department for approval.

Through these modifications, Khosropanah was able to misappropriate computers and electronics and conceal his misappropriations. He then sold the misappropriated assets on eBay and to a third-party wholesaler without the knowledge or consent of his employer.

Khosropanah sold approximately 850 laptops and other electronics, causing a loss of over $1.9 Million to his employer. Khosropanah used the proceeds from the fraudulent sales to purchase luxury cars, including a Ferrari. (Source)

Former Yale Med School Employee Sentenced To Prison For Stealing And Selling $40 Million in Electronics / Used Money For Cars, Real Estate, Travel - October 13, 2022

Beginning in approximately 2008, Jamie Petrone was employed by the Yale University School of Medicine (Yale Med), Department of Emergency Medicine. He most recently served as the Director of Finance and Administration for the Department of Emergency Medicine. As part of her job responsibilities, Petrone had authority to make and authorize certain purchases for departmental needs as long as the purchase amount was below $10,000.

Beginning at least as early as 2013, Petrone engaged in a scheme whereby she ordered, or caused others working for her to order, millions of dollars of electronic hardware from Yale vendors using Yale Med funds and arranged to ship the stolen hardware to an out-of-state business in exchange for money.

Petrone falsely represented on Yale internal forms and in electronic communications that the hardware was for specified Yale Med needs, such as particular medical studies, and she broke up the fraudulent purchases into orders below the $10,000 threshold that would require additional approval. An out of state business resold the electronic equipment to customers, paid Petrone by wiring funds into an account of a company in which she is a principal, Maziv Entertainment LLC.

Petrone caused a loss of approximately $40,504,200 to Yale. Petrone used the proceeds of the sales of the stolen equipment for various personal expenses, including expensive cars, real estate and travel. (Source)

University Network Systems Manager Sentenced To Prison For Purchasing IT Equipment For University Over 12 Years, Them Selling For Personal Benefit - August 24, 2023

Daniel Sickels previously worked as a Network and Systems Manager at Pennsylvania State University (PSU) Office of Development and Alumni Relations (ODA), located in State College, PA.

Sickels fraudulently acquired equipment through false representations to PSU ODA that the equipment was necessary to upgrade, replace, or maintain PSU ODA servers, when, in fact, Sickels knew that the equipment was not necessary. Sickels subsequently sold the equipment for his personal benefit to third parties. The scheme lasted from approximately 2005 to 2017, in Centre and Mifflin Counties. Sickels was also ordered to pay $267,264.87 in restitution. (Source)

Former Philadelphia Water Department Employee Sentenced To Prison For Stealing $150,000+ Of Assets - July 6, 2022

Thomas Staszak is a former employee of the City of Philadelphia Water Department (PWD).

On multiple occasions from approximately April 2017 through at least November 2018, Staszak accessed the PWD's computerized inventory control system without authorization, using log-in credentials associated with PWD employees under his supervision at a PWD storeroom. Staszak is then charged with creating false entries in PWD's electronic records to provide justifications for removing maintenance materials, for example bulk wire, from the storeroom. Staszak then physically took the materials from PWD's inventory, transported them to local scrap yards, sold the materials, and kept the proceeds. Staszak stole items valued at approximately in excess of $150,000 before he was caught. (Source)

Former YMCA Employee Sentenced To Prison For Fraudulently Ordering Cell 1,000 Phones For YMCA And Then Reselling Them For $600,000 In Cash - May 5, 2023

Celeste Santifer was a former employee of the YMCA of Metropolitan Washington (YMCA-DC). Santifer worked as an Office Manager at YMCA-DC from approximately 2007 until her termination in May of 2019.

While working at the YMCA-DC, Santifer devised a scheme to defraud Verizon Wireless by taking advantage of an arrangement with Verizon to sell YMCA-DC cell phones for its employees at a discounted price. From at least January 2016 through April 2019, Santifer placed online orders for discounted cell phones from Verizon that she personally received, disconnected from service, and sold to companies that buy and sell new or slightly used phones. Santifer ultimately ordered over 1,000 phones purportedly for YMCA-DC employees that she sold to third-party companies for money. The value of the phones to Verizon was $618,090. (Source)

And Many More.....

SABOTAGE / UN-AUTHORIZED USE OF EMPLOYERS NETWORK BY EMPLOYEES

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)

Wastewater Treatment Plant Facility Employee Sabotages Network Remotely After Resigning - July, 7, 2023

Prior to the attack on the Discovery Bay Water Treatment facility, Rambler Gallo was a full-time employee of a private Massachusetts based company. Gallo's company contracted with Discovery Bay to operate the town's wastewater treatment facility; the facility provides treatment for the water and wastewater systems for the town's 15,000 residents.

During Gallo's employment with his company from July of 2016 until December of 2020, Gallo was the company's Instrumentation & Control Tech, with responsibility for maintaining the instrumentation and the computer systems used to control the electromechanical processes of the facility in Discovery Bay.

While Gallo was employed with his company, he installed software on his own personal computer and on his company's private internal network that allowed him to gain remote access to Discovery Bay's Water Treatment facility computer network. In January of 2021, after Gallo had resigned from his company, he allegedly accessed the facility's computer system remotely and transmitted a command to uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels. (Source)

Former Employee Charged With Sabotaging Employers Database 3 Months After Being Terminated - May 30, 2023

Vamsikrishna Naganathanahall accessed a computer system belonging to his former employer, Vituity, after his company login privileges had been revoked. Naganathanahalli used his access to the computer system to replace real data with masked data causing damage to an important Vituity database.

Vituity comprises a group of companies based in Emeryville, California, including physician partnerships and other entities. Vituity maintained a computer database that was central to its business and was connected to systems responsible for hiring and payroll, among other functions.

In late May of 2022 Naganathanahalli was informed that his employment with Vituity would be terminated in June. After he was informed his employment would be terminated, but before his last day on the job, he changed a password to another employee's account so he would be able to gain access to a Vituity computer system after access to Vituity's computers using his own password was revoked. In September 2022, Naganathanahalli used the changed password to access a Vituity computer system remotely, change yet another employee's password, and then use that employee's account to overwrite the company's personnel data. (Source)

2 Employees' Of Mental Health Treatment Provider Charged With Sabotaging Network While Patients Were Receiving Treatments - June 27, 2023

Between September and December of 2021, Nathan Howe and Patrick 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 ATM Technician Sentenced To Prison For Tampering With ATM's - Then Robbed ATM Technicians Sent To Repairs ATM's - July 18, 2023

Johnson Saint-Louis was a former ATM technician who traveled around the southeast Florida tampering with ATMs serviced by his former employer. Over a two year period, Saint-Louis robbed four ATM technicians sent out to fix problems Saint-Louis had caused.

The FBI's financial investigation revealed that Saint-Louis, who had been unemployed since mid 2019, was making large cash deposits into his bank accounts ($89,939 in 2021) and gambling large amounts of money and losing $189,814 in 2021. (Source)

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

Casey Umetsu worked as an Information Technology Professional for a prominent Hawaii based financial company between 2017 and 2019. 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 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 Administrator Wipes Employer's Databases Causing Severe Impacts - May 15, 2022
Han Bing is a former Database Administrator for Lianjia, a Chinese real-estate brokerage giant.

Bing performed the act in June 2018, when he used his administrative privileges and root account to access the company's financial system and delete all stored data from two database servers and two application servers.

This has resulted in the immediate crippling of large portions of Lianjia's operations, leaving tens of thousands of its employees without salaries for an extended period and forcing a data restoration effort that cost roughly $30,000.

The indirect damages from the disruption of the firm's business, though, were far more damaging, as Lianjia operates thousands of offices, employs over 120,000 brokers, owns 51 subsidiaries, and its market value is estimated to be $6 billion.

Bing had repeatedly informed his employer and supervisors about security gaps in the financial system, even sending emails to other administrators to raise his concerns. However, he was largely ignored, as the leaders of his department never approved the security project he proposed to run. (Source)

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Network After Termination & The Sabotage Of 20+GB's Of Data - August 31, 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. 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. The credit union spent approximately $10,000 in remediating Barile's unauthorized intrusion and destruction of data. (Source)

Former Human Resources Manager Convicted Of Deleting Over 17,000 Files (All Of Employers Data) While Being Terminated - August 16, 2021
In January 2019, Medghyne Calonge was hired by an online provider of professional services. She was to serve as the head of Human Resources.

On June 28, 2019, Calonge was terminated for failing to meet the minimum requirements of her job after, among other things, she improperly downgraded a colleague's access to a computer system following an argument with the colleague.

While she was being terminated, and just before she was escorted from the building, Calonge was observed by 2 employees of repeatedly hitting the delete key on her desktop computer. Hours later she logged into a system which the company had invested 2 years and over $100,000 to build. During the next 2 days, she deleted over 17,000 job applications and resumes, and left messages with profanities inside the system. She completely destroyed all her employers' data. (Source)

Information Technology Assistant Manager Accused Of Crypto-Mining Using Employers Network - September 14, 2021

An information technology expert employed by a New York county has been arrested on suspicion of mining crypto-currency at work.

Christopher Naples is accused of covertly installing dozens of machines throughout his workplace and using them to mine Bitcoin and other types of crypto-currency as part of a secret illegal money-making scheme.

Naples was hired by Suffolk County back in 2000. His title was Assistant Manager of Information Technology Operations for the Suffolk County Clerk's Office.

Authorities said that the clandestine crypto-mining activity allegedly carried out by Naples ran up electricity bills in excess of $6,000 for his unsuspecting employer. The mining devices increased the temperature in some rooms by 20 degrees.

Naples is accused of installing 46 crypto-mining devices in six rooms inside the county center located in Riverhead, New York. Hiding places in which the devices were allegedly concealed included beneath the floorboards of the building, on top of or inside server racks and inside an electrical wall panel that was not in use. (Source)

Former Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million - December 9, 2020

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. 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. (Source)

Terminated Employee Sentenced To Prison For IT Sabotage / Data Theft Of Former Employers Network / Demands Ransom – January 23, 2020

In 2008, Kristopher Ives began working as a computer programmer for Gearbox Studios, a digital marketing agency. Ives eventually became Gearbox Studio's lead programmer for server architecture and support, a position of trust with access to the computer networks and data of both the company and the company's clients.

Between February and May 2015, after being terminated from his position, Ives illegally accessed Gearbox's computers to steal and tamper with data. He used this data to attack Gearbox's servers and various websites belonging to Gearbox customers. Ives deleted nearly 20,000 products from customer websites and changed prices for various items. Ives also stole names and credit card numbers from these Gearbox customer websites and threatened to release the information unless Gearbox made payment to a Bitcoin address. (Source)

Former IT Administrator Who Resigned After Company Acquisition Sentenced To Prison For Sabotaging Network Causing More Than $800,000 In Damages - May 30, 2020

Charles Taylor sabotaged his employer's network by changing router passwords and shutting down a critical command server. After resigning from his job in July 2018, Taylor caused more than $800,000 in damage to his former employer, which had to replace several routers and rebuild and restore its internal computer network.

Taylor had worked for his company since 2013. In 2018 the company was acquired by another company. Taylor kept his job as a Senior Systems Engineer after the merger, but he became unhappy with the owners of the now combined company and resigned in July 2018. (Source)

Terminated Employee Sentenced To Prison For IT Sabotage / Data Theft Of Former Employers Network / Demands Ransom – January 23, 2020

In 2008, Kristopher Ives began working as a computer programmer for Gearbox Studios, a digital marketing agency. Ives eventually became Gearbox Studio's lead programmer for server architecture and support, a position of trust with access to the computer networks and data of both the company and the company's clients.

Between February and May 2015, after being terminated from his position, Ives illegally accessed Gearbox's computers to steal and tamper with data. He used this data to attack Gearbox's servers and various websites belonging to Gearbox customers. Ives deleted nearly 20,000 products from customer websites and changed prices for various items. Ives also stole names and credit card numbers from these Gearbox customer websites and threatened to release the information unless Gearbox made payment to a Bitcoin address. (Source)

IT System Administrator Who Was On Suspension / Returns To Work And 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. (Source)

Former Citibank Employee Sentenced To Prison For Sabotaging And Shutting Down 90% Of The Network - July 28, 2016

Lennon Brown worked for Citibank first as a contract employee, and then, beginning in February 2013 as a full-time employee until December 2013.

Brown pleaded guilty that on December 23, 2013, hours after having a discussion with his supervisor about his work performance, he sabotaged the Citibank's network.

At approximately 6:03 p.m. on December 23, Brown transmitted a code and command to 10 core Citibank Global Control Center routers, and by transmitting that code, erased the running configuration files in 9 of the routers, resulting in a loss of connectivity to approximately 90% of all Citibank networks across North America. At 6:05 p.m. that evening, Brown scanned his employee identification badge to exit the Citibank Regents Campus.

At the sentencing, a text message was read that Brown sent shortly after the attack explaining his motive. "They were firing me. I just beat them to it. Nothing personal, the upper management needs to see what they guys on the floor are capable of doing when they keep getting mistreated." (Source)

Employee Who Was Aware That He Is Going To Be Fired Sabotages Company's Network Servers Costing Company $1 Million In Lost Business– September 22, 2014

When Risky Mitchell learned he was going to be fired from the oil and gas company EnerVest Operating, he remotely accessed their computer systems and reset the network servers to factory settings, essentially eliminating access to all the company's data and applications for its eastern United States operations.

Before his access to EnerVest's offices could be terminated, Mitchell entered the office after business hours, disconnected critical pieces of network equipment, and disabled the equipment's cooling system.

As a result of his actions, the company permanently lost some of its data and spent hundreds of thousands of dollars repairing equipment and recovering historical data. It took a month to bring the company's office back online, costing the company as much as $1 million in lost business. (Source)

And Many More.....

THREATS TO CRITICAL INFRASTRUCTURE BY EMPLOYEES

2023 Report States That Critical Infrastructure Leaders Are Concerned Over Insider Threat - April 20, 2023

Over 35% of critical national infrastructure (CNI) security leaders believe the economic downturn is forcing employees to turn to data theft and sabotage, according to the Bridewell Consulting Report.

Overall, the number of employee sabotage incidents at CNI firms surged by 62% year-on-year, according to the report.

Bridewell Consulting polled 1025 individuals with responsibility for cybersecurity in UK and US CNI firms across the communications, utilities, finance, government and transport and aviation sectors.

Many believe the cost-of-living crisis may be driving Insiders at these firms to do the bidding of cybercrime groups in return for a big pay-off.

Their suspicions are backed by hard evidence: the financial services sector was hit worse than any other industry sector studied for the report last year. Organizations in the vertical suffered on average 28 security incidents caused by employee sabotage over the previous 12 months, as well as 28 instances of data theft or misuse.

Challenging economic conditions are also putting pressure on CNI firms in other ways. Almost 65% of UK respondents said they had seen "some reduction" or a "significant reduction" in their cybersecurity budget, rising to 73% of U.S. respondents.

The communications sector has been impacted the least by these cuts, with 48% claiming to have seen no change in security budgets. At the other end of the spectrum, the transport and aviation (73%) and utilities sectors (69%) experienced the greatest falls. Utilities also includes energy, oil and gas companies. (Source)

Former Public Utility Employee Pleads Guilty To Installing Keylogger Devices On Work Computers - August 10, 2022

The Northern Ohio Public Utility (NOPU) provides Water, Electricity, Natural Gas and Telecom services to its customers

While working as an Operator with the NOPU, John Pelton purchased two physical keyloggers from eBay with the intent of using them at his place of employment.

On Jan. 12, 2021, Pelton installed the keylogger devices at his place of employment on two computers in a control room accessible only via an access badge. Pelton installed one keylogger on a control room computer connected to the internet and the utility's internal network and the other on a second computer used in the delivery of services. The keyloggers would allow Pelton to capture an administrator's password and access features that he otherwise was unable to access.

One of the computers Pelton installed a keylogger on collected data regarding the use of the utility's electrical system. The Operators at the utility have the capability to turn the power on and off throughout the network, and, if done incorrectly or inappropriately, an Operator could damage the transmission system, injure employees and possibly negatively impact the energy grid.

A physical keylogger is an electronic device that stores and can transmit every keystroke made on a keyboard. A keylogger is capable of intercepting employee login credentials, messages and any other information typed into a computer. These devices have built-in memory capable of storing approximately 16 million keystrokes and could be accessed wirelessly with any Wi-Fi-enabled device, such as a smartphone, allowing the user to download the captured keystrokes remotely. (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)

And Many More.....

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

EMPLOYEES THAT HAVE LOST THEIR JOBS BECAUSE OF THEIR CO-WORKERS ACTIONS

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)

And Many More.....

COMPANIES THAT HAVE GONE OUT OF BUSINESS BECAUSE OF MALICIOUS EMPLOYEES ACTIONS

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

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

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

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans. As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the bank in April 2017. This failure caused approximately $1 Billion in loss to the FDIC and the loss of approximately 500 jobs.

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

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

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

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

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

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

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

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

The loan ultimately defaulted, resulting in a loss of over $1 million. Zilberberg was focused on squeezing money out of it for himself, on the basis of lies. The bank collapsed just months after Zilberberg defrauded it. (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 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)

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)

Packaging Company Controller Sentenced To Prison For Stealing $195,000+ 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)

And Many More.....

WORKPLACE VIOLENCE BY EMPLOYEES

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

Reta Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VMAC) 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 and she admitted to administering insulin to 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)

Bank Employee Who Killed 5 Employees' Was Told He Was Going To Be Fired - April 11, 2023

Connor Sturgeon worked at Old National Bank, a regional bank headquartered in Indiana. Sturgeon started working as an intern in 2018, and was working as a syndications associate and portfolio banker when the shooting happened.

He had been told that he was going to be fired. He left a note before the attack addressed to his parents and a friend telling them he was going to shoot up the bank. Sturgeon live streamed his killing of the 5 bank employees. Sturgeon was fatally shot by police. (Source)

Walmart Employee Kills 6 Co-Workers / His Manifesto Claims He Was Betrayed By Coworkers And He Felt Led By Satan - November 25, 2022

Andre Bing was a Walmart employee. He shot and killed 6 other employees and left a manifesto blaming the deadly violence on torment by coworkers and demonic influences.

The manifesto includes multiple anecdotes of what Bing believed was targeted harassment from his coworkers. He goes on to say he believed that those around him were intentionally harassing him and sabotaging his life.

The manifesto has recurring religious themes and references to both God and the demonic, with Bing writing, "Sorry everyone but I did not plan this I promise, things just fell in place like I was led by the Satan." The manifesto concludes by stating "My God forgive me for what I'm going to do." (Source)

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

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

A jury initially awarded more than $7 Billion in damages, 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)

Former FedEx Employee Shoots And Kills 8 Co-Workers Had Mental Health Problems - April 20, 2021
Bandon Hole worked at the FedEx facility between August and October 2020.

In April 2021, Hole returned to his former place of employment and fatally shot 8 people at a FedEx Ground facility. He had apparently been planning the attack for at least 9 months.

The FBI stated that 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)

Railway Employee Kills 9 Co-Workers - Was Disgruntled And Had Made Previous Threats About Killing Employees' - May 11, 2021
9 people were killed by a gunman (Sam Cassidy) at a Northern California Railway. They were shot in two separate buildings before Cassidy took his own life.

Since 2012 Cassidy was a Valley Transportation (VTA) employee, who worked first as a mechanic from 2012 to 2014, then as someone who maintained substations. He took he own life after the shooting.

Cassidy had two semi-automatic handguns and 11 loaded magazines on him at the time of the shooting.

His ex-wife said he had talked about killing people at work more than a decade ago. "I never believed him, and it never happened. Until now," Cecilia Nelms stated. She said he used to come home from work resentful and angry over what he perceived as unfair assignments.

An ex-girlfriend described Cassidy as volatile and violent, with major mood swings because of bipolar disorder that became worse when he drank heavily.

Several times while he was drunk, Cassidy forced himself on her sexually despite her refusals, pinning her arms with his body weight, the woman alleged in a 2009 sworn statement filed after Cassidy had sought a restraining order against her. (Source)

Virginia Beach Municipal Center Employee Kills 11 Co-Workers – He Was Fixated On Workplace Grievances - June 9, 2021
DeWayne Craddock worked in the city's public utilities department. He walked into his workplace of 9 years on May 31, 2019 and fatally shot 11 co-workers and a contractor who was getting a permit. 4 more people were seriously wounded in the attack and Craddock was killed by police.

In 2021, the FBI released a report that stated that Craddock's perceived grievances began in 2014, at which point he "purposely isolated himself by disengaging from relationships to conceal his intentions."

"The shooter's inflated sense of self-importance contributed to this conflict and led him to believe he was unjustly and repeatedly criticized and slighted," the FBI's Behavioral Analysis Unit stated. Violence was viewed by the shooter as a way to reconcile this conflict and restore his perverted view of justice."

The Virginia Beach Police Department said Craddock started having performance issues at work in 2017, the same year that he finalized a divorce from his wife. (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 a delivery man for the company killed a 75-year old woman while delivering her appliances.

The family of 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)

DEFINITIONS OF INSIDER THREATS

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

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

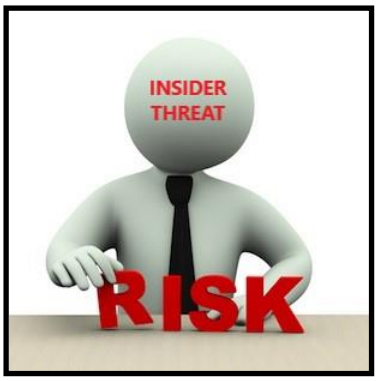
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

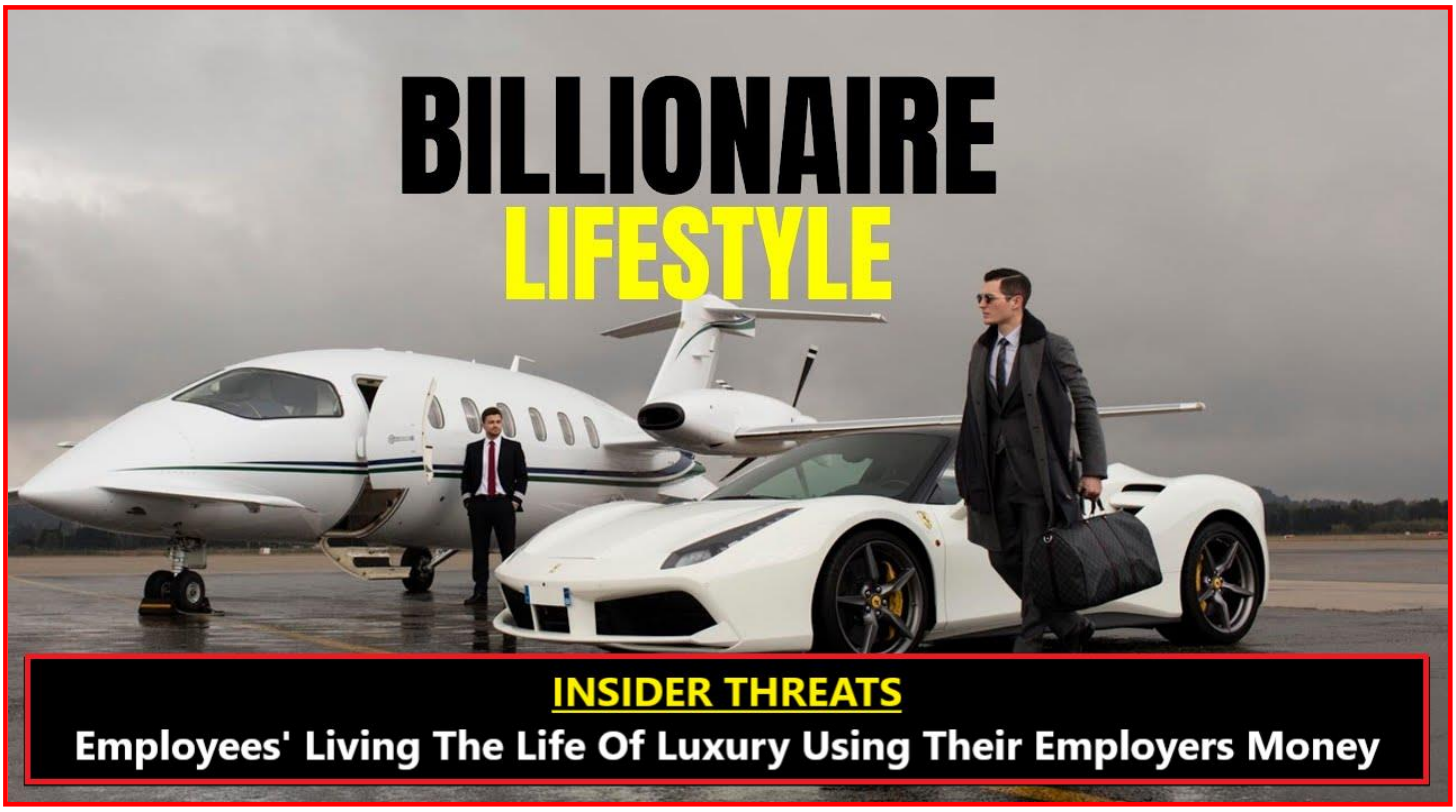
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

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

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ 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, Properties & Businesses

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

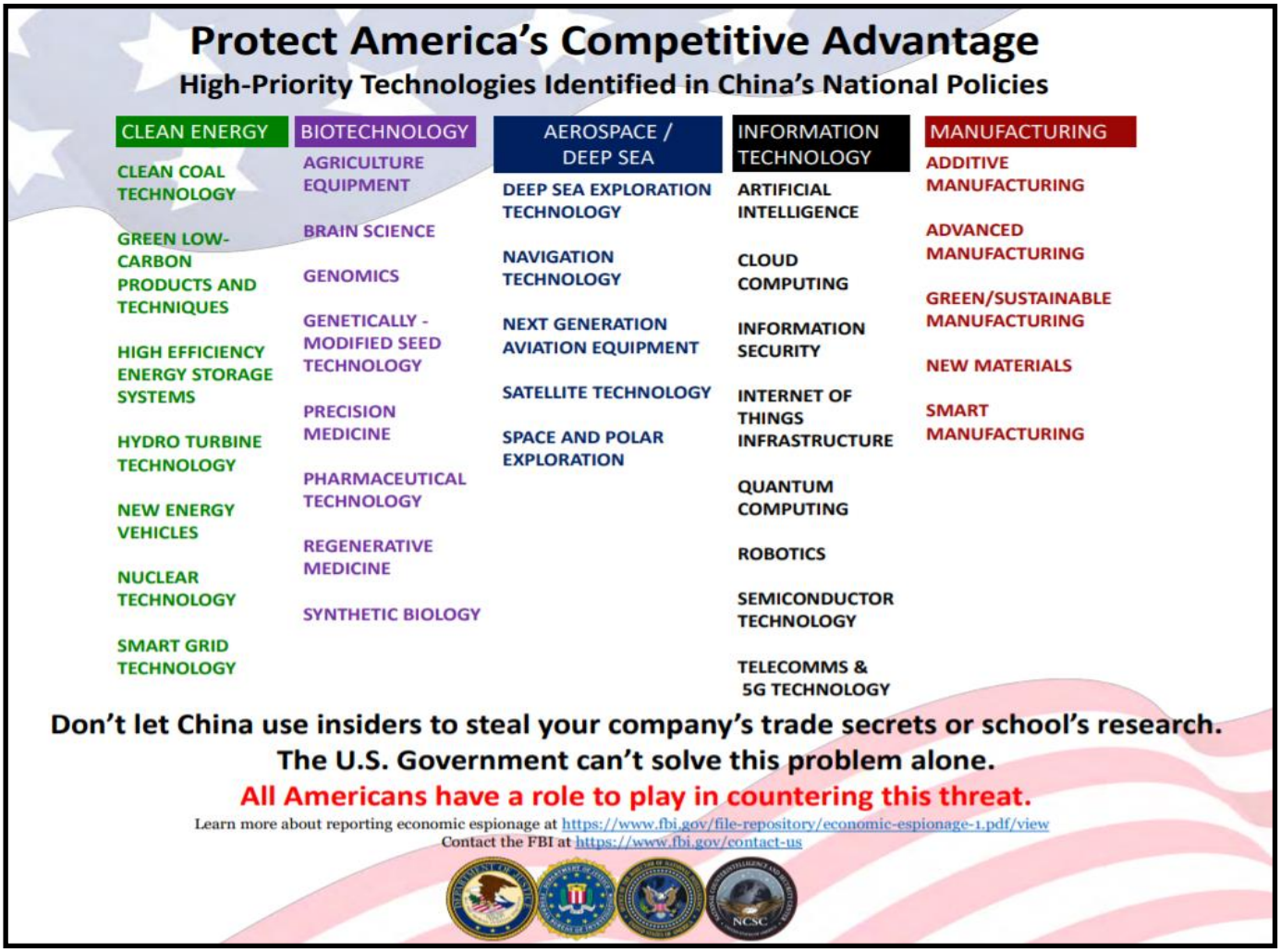
- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present
http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS REPORTS

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

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 (**4,900+ 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 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.insiderthreatdefensegroup.com / jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org