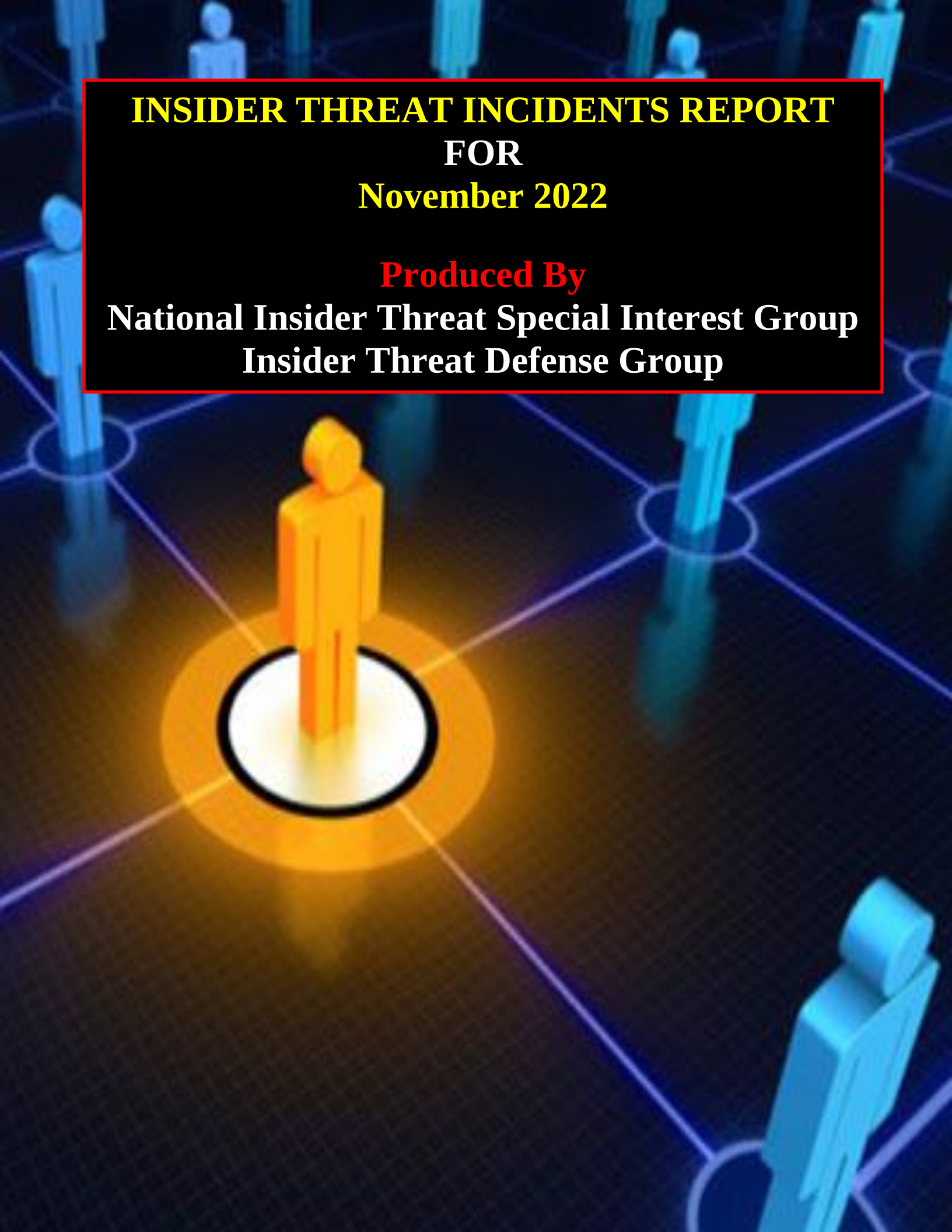


INSIDER THREAT INCIDENTS REPORT
FOR
November 2022

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **4,200+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

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

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees.

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

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

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

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 23 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM CC2 & Other Sources) and be expanded.

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

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR NOVEMBER 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

U.S. Postal Carrier And Co-Conspirator Are Charged For $8.3 Million+ Mail Theft Scheme - November 21, 2022

Kiara Padgett was employed by the U.S. Postal Service as a Mail Carrier with a postal route in West Charlotte, North Carolina.

From August 2021 to November 2022, Padgett allegedly used her position as a postal carrier to steal incoming and outgoing checks of businesses and individuals, which she then sold to other individuals located in Charlotte and Maryland. Padgett stole was more than $8.3 million. Between August 2021 and June 2022, Padgett received payments for her role in the scheme totaling at least $13,698.

The indictment filed against Hager alleges that, between August 2021 and November 2022, Hager and his co-conspirators obtained stolen checks from Padgett. The co-conspirators allegedly deposited the stolen checks into bank accounts Terrell Hager and others controlled, and then made cash withdrawals before the financial institutions detected the fraud. Over the course of the scheme, Hager and his co-conspirators allegedly deposited more than $27,000 in stolen checks and money orders. Hager also allegedly posted online for sale over 400 stolen checks totaling over $7.3 million. The checks posted by Hager were allegedly stolen from Padgett's postal route in West Charlotte. According to today's court proceedings, Hager was on probation with the state of North Carolina when he committed the fraud. (Source)

U.S. Postal Service Mail Carrier Pleads Guilty To Stealing $2,700 Of Gift Cards, Cash And Jewelry From Mail - November 10, 2022

A former U.S. Postal Service Mail Carrier Breanna Wares pleaded guilty that she stole approximately $2,700 worth of gift cards, cash and jewelry from customers.

Wares stole these items from approximately 20 customers along her route near Camp Pendleton at the Brooks Street Station in Oceanside, CA.

The investigation determined that Wares unlawfully redeemed over 30 Target gift cards that had been placed in the mail, totaling more than $1,400. During a search of Ware's personal vehicle, agents discovered more than 40 gift cards valued at more than $1,300. Agents also found sheets of stamps, jewelry, foreign currency, rifled and unrifled First Class Mail greeting card envelopes. Agents also found a Trader Joe's gift card in Wares' wallet. (Source)

U.S. Postal Carrier Pleads Guilty To Attempting To Bribe U.S. Postal Supervisor To Divert Packages Of Cocaine - November 2, 2022

John Noviello was a Mail Carrier for the U.S. Postal Service.

On Feb. 15, 2022, Noviello approached a U.S. Postal supervisor seeking their assistance in a scheme to divert postal packages suspected of containing cocaine. Noviello offered to pay the supervisor $1,750 per kilogram of cocaine successfully obtained from any diverted packages. On Feb. 17, 2022, Noviello left $850 in cash, concealed in a Dunkin' bag, inside the supervisor's vehicle in an attempt to encourage the supervisor to agree to the scheme. Noviello, referring to the $850, later commented to the supervisor, "that was a nice envelope for starters." After contacting authorities, the supervisor conducted a controlled purchase from Noviello during which the defendant distributed approximately 3.7 grams of cocaine for $200. (Source)

Former Department of Transportation Employee Charged With Extortion And Accepting $2,000 Bribe - November 14, 2022

Patrick Gorena was a Border Investigator for U.S. Department of Transportation (DOT) Federal Motor Carrier Safety Administration.

In exchange for minimizing purported safety violations he encountered while auditing a trucking company, which would have exposed the company to potential fines and the loss of their ability to operate, Gorena allegedly demanded a $3,500 cash payment. The charges allege Gorena ultimately accepted a $2,000 bribe from an undercover law enforcement officer posing as a representative of the trucking company. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Navy Nuclear Engineer & Wife Sentenced To Prison For Espionage-Related Offenses - November 9, 2022

Jonathan Toebbe, 44, of Annapolis, was sentenced today to 19 years and 4 months of incarceration and fined $45,700. His wife, Diana Toebbe, 46, was sentenced to 21 years and 10 months of incarceration and fined $50,000. The Toebbes pleaded guilty to the conspiracy in August 2022.

Jonathan Toebbe was an employee of the Department of the Navy who served as a Nuclear Engineer and was assigned to the Naval Nuclear Propulsion Program. He held an active national security clearance through the Department of Defense, giving him access to "Restricted Data" within the meaning of the Atomic Energy Act. Restricted Data concerns design, manufacture or utilization of atomic weapons, or production of Special Nuclear Material (SNM), or use of SNM in the production of energy, such as naval reactors. Jonathan Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships.

Toebbe sent a package to a foreign government, listing a return address in Pittsburgh, Pennsylvania, containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was really an undercover FBI agent. Toebbe continued this correspondence for several months, which led to an agreement to sell Restricted Data in exchange for thousands of dollars in cryptocurrency.

On June 8, 2021, the undercover agent sent $10,000 in cryptocurrency to Jonathan Toebbe as "good faith" payment. Shortly afterwards, on June 26, Jonathan Toebbe serviced a dead drop by placing an SD card, which was concealed within half a peanut butter sandwich and contained military sensitive design elements relating to submarine nuclear reactors, at a pre-arranged location. After retrieving the SD card, the undercover agent sent Jonathan Toebbe a $20,000 cryptocurrency payment. In return, Jonathan Toebbe emailed the undercover agent a decryption key for the SD Card. A review of the SD card revealed that it contained Restricted Data related to submarine nuclear reactors. On Aug. 28, Jonathan Toebbe made another "dead drop" of an SD card in eastern Virginia, this time concealing the card in a chewing gum package. After making a payment to Jonathan Toebbe of $70,000 in cryptocurrency, the FBI received a decryption key for the card. It, too, contained Restricted Data related to submarine nuclear reactors. The FBI arrested Jonathan Toebbe and his wife on Oct. 9, after he placed yet another SD card at a pre-arranged "dead drop" at a second location in West Virginia. (Source)

Former Air Force Contracting Specialist Sentenced To Prison For Bribery Scheme Involving Millions in DOD Contracts - November 9, 2022

Brian Nash is a former U.S. Air Force Contract Specialist who was assigned to Joint Base Elmendorf Richardson (JBER).

Nash agreed to accept more than $460,000 in bribe payments in 2019 from a government contractor, Ryan Dalbec, who, along with his wife, Riahnna Nadem, owned a construction company called Best Choice Construction LLC.

In exchange, Nash provided Dalbec and Nadem with confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson AFB and JBER, which helped Best Choice win some of the contracts, including a construction contract related to the F-35 aircraft program at Eielson Air Force Base and contracts to perform construction and related services at JBER.

At the time Nash was caught he had received approximately $47,000 of the agreed upon bribe payments, much of which he laundered through family members to conceal the nature and source of the funds. The defendants committed multiple overt acts in furtherance of the bribery conspiracy, and between March and October 2019 Dalbec, Nadem and Nash laundered payments and proceeds from the bribery scheme to conceal their unlawful activities. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Homeland Security Investigations Agent Sentenced To Prison For Accepting $100,000 In Bribes From Person Associated With A Criminal Organization - November 21, 2022

Over an 18 month period that started in September 2015, Felix Cisneros accepted cash, checks, private jet travel, luxury hotel stays, meals and other items of value from a person who was associated with a criminal organization. Cisneros received approximately $100,000 in checks and gifts from Individual 1 in 2015 and 2016.

Cisneros accepted cash payments and other benefits to help an organized crime-linked person, including taking official action designed to help two foreign nationals gain entry into the United States. (Source)

3 New York City Correction Officers Charged With Fraud For Lying To Stay On Sick Leave For Over A Year - November 10, 2022

A Rikers Island New York City Department Of Correction Officer (DOC) Steven Cange fraudulently obtained more than $160,000 in salary by being on sick leave from March 2021 to the present. Although Cange claimed that he suffered from symptoms of vertigo and side effects from the COVID-19 vaccine, evidence obtained by law enforcement demonstrates that Cange was able to work. During his sick leave, Cange submitted more than 100 fraudulent medical notes to DOC demonstrating that he was at physical therapy or another medical provider when records subpoenaed from those providers demonstrate that Cange was not at those appointments. Law enforcement also observed Cange engaging in normal life activities with no apparent difficulty.

New York City DOC Officer Monica Coaxum fraudulently obtained more than $80,000 in salary by being on sick leave from March 2021 to May 2022, and her fiancée, Correction Officer Eduardo Trinidad, fraudulently obtained more than $140,000 in salary by being on sick leave from June 2021 to November 2022. Although Coaxum claimed to suffer from multiple injuries, evidence collected by investigators shows that she was able to work. During her sick leave, Coaxum submitted nearly 50 fraudulent medical notes to DOC stating that she had gone to a medical appointment at times law enforcement determined she was elsewhere. Additionally, evidence shows that on some occasions where Coaxum claimed to be injured and at home, she was traveling and at parties. When approached by law enforcement, Coaxum admitted to forging some medical documents.

Trinidad likewise obtained more than $140,000 by claiming to be too injured to work for over a year. Although he went to medical appointments with DOC wearing some combination of a sling, cane, and/or boot, photographic and video evidence during the same period showed Trinidad doing normal life activities like home improvement work, bowling and traveling abroad, without any difficulty or help from equipment like a boot, sling or cane. (Source)

Former Correctional Officer Pleads Guilty To Accepting Bribes To Smuggle Contraband Into Federal Prison - November 10, 2022

Kacie Deyo pleaded guilty today to accepting bribes while serving as a Correctional Officer at a federal prison in El Reno, Oklahoma.

Deyo accepted thousands of dollars of bribes in exchange for smuggling contraband into El Reno between March 3, 2021, and May 7, 2021. (Source)

STATE / CITY GOVERNMENTS

17 New York City & State Public Employees Charged With Fraudulently Obtaining $1.5 Million+ In COVID Relief Loans - November 30, 2022

These individuals were charged with submitting fraudulent applications for the U.S. SBA Paycheck Protection Program and Economic Injury Disaster Loans, Most of these individuals were currently or previously employed by New York City or New York State. (Source)

Across all of these schemes, the defendants collectively stole more than $1.5 million from the SBA and financial institutions that issued SBA-guaranteed loans and intended or attempted to steal hundreds of thousands of dollars more. (Source)

Former State Employee And 3 Others Charged For $1 Million+ COVID-19 Fraud Scheme - November 18, 2022

The 33 count indictment alleges that between May 2020 and January 2022, the four co-defendants conspired to commit wire fraud, and in fact committed wire fraud, by filing fraudulent unemployment claims in Michigan and elsewhere. The claims involved in the case were allegedly for claimants who were ineligible for benefits, for example because they did not have Michigan income or reside in Michigan.

Adelita Juarez was employed as an Unemployment Insurance Examiner by the State of Michigan during the relevant time period, and allegedly processed the claims to ensure they would be paid, including by clearing fraud notices. Her daughter, Francisca Juarez, allegedly received kickbacks in connection with the payment of the fraudulent claims. The remaining co-defendants, Evelyn De-Maya Vanderbilt and Michelle Giordano, allegedly obtained the personally identifiable information of the claimants, aided in the submission of the claims, and received some or all of the proceeds of the claims.

The proceeds of the scheme were allegedly funded in part by the Pandemic Unemployment Assistance, Pandemic Unemployment Compensation, and Lost Wages Assistance programs. The indictment alleges that the co-defendants stole at least $1,053,401. (Source)

Administrative Assistant To City Council Admits To Stealing $1.2 Million+ Of COVID Relief Funds - November 1, 2022

Michael DiMassa was a Connecticut State Representative who was also employed by the City of West Haven, most recently serving as the Administrative Assistant to the City Council.

From July 2020 through September 2021, the City of West Haven received approximately $1,150,257 in financial assistance from this fund. DiMassa, who was authorized to approve the designated relief funds for the reimbursement of COVID related expenditures incurred by West Haven, conspired with others to steal these funds and other West Haven funds through the submission of fraudulent invoices, and subsequent payment, for COVID relief goods and services that were never provided. (Source)

Former DMV Employee Sentenced To Prison For Role In $277,000+ Bribery Conspiracy Involving Commercial Driver License Testing - November 3, 2022

Shawana Harris was a long-time DMV employee who had the ability to update test scores for commercial driver's license applicants in California.

Using her position as a public employee at the DMV, Harris accepted bribes in exchange for fraudulently updating test scores for people pursuing commercial driver's licenses. For at least 185 commercial license applicants, Harris used her access to DMV computers to enter fraudulent test scores indicating the applicants had passed written and / or behind the wheel commercial drive tests, when in reality the applicants had not passed those tests. Harris and a co-conspirator were typically paid at least $1,500 per applicant for fraudulently updating test scores, resulting in approximately $277,500 worth of corrupt bribes. (Source)

New York City Housing Authority Superintendents Plead Guilty To Accepting $20,000 In Bribes To Award Contracts - November 3, 2022

In February 2020, Leroy Gibbs, who was then employed as the Resident Buildings Superintendent at Douglass Houses in New York, New York, solicited and accepted approximately $2,000 in bribes from a confidential informant (C") in exchange for awarding no-bid contracts to the CI worth a total of approximately $9,950 from NYCHA for work at that NYCHA facility.

Between July 2021 and August 2022, Julio Figueroa, who was then employed as the Assistant Resident Buildings Superintendent at the Ft. Independence St.-Heath Ave. Houses in the Bronx, New York, solicited and accepted approximately $6,000 in bribes from the CI in exchange for awarding no-bid contracts to the CI worth a total of approximately $46,622 from NYCHA for work at that NYCHA facility. (Source)

3 Former City Officials And Former City Engineer Charged In Bribery Scheme (Cash, Concert / Football Tickets) - November 22, 2022

A federal grand jury in returned an indictment in charging three City of Canton Officials, and the former City Engineer, with criminal conspiracy charges relating to bribery and wire fraud.

Eric Gilkey and Andrew Grant, pleaded guilty to conspiring with Cleveland Anderson and Rudolph Warnock, Jr. in the bribery scheme.

Warnock is charged with having directed payments and rewards to Anderson, Gilkey, and Grant in exchange for preferential treatment that resulted in lucrative city engineering contracts for Warnock. The gratuities supplied by Warnock included thousands of dollars in cash, concert tickets, and football tickets in New Orleans, Louisiana. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former Business Manager Pleads Guilty To Embezzling $153,000+ From 2 Schools - November 9, 2022

Michelle Mille worked as a Business Manager for two schools, St. Teresa's and St. Luke's.

Miller Admitted Using Her Position To Commit Fraud:

She wrote checks from the schools' accounts to herself
She made excess salary payments to herself
She wrote checks to petty cash and pocketed the money.

To conceal this fraud, Miller at times forged the signature of the priest of St. Teresa's and St. Luke's. She also manipulated the parish's QuickBook accounts to make it look like St. Luke's was paying money to St. Teresa's when the money was actually going to her.

Miller took a total of $153,940.38 from St. Teresa's and St. Luke's that she was not entitled to receive. (Source)

Former School Official Pleads Guilty In $100,000+ Contract Kickback Scheme / Used Funds For Vacations, Vehicle, Home Furnishings - November 29, 2022

Sharon Gardner is the former Director of Food Services for the Hempstead Union Free School District (HUFSD)

Gardner's co-conspirator is Maria Caliendo. She is the owner of food service providers Smart Starts NY, Inc. (Smart Starts) and Prince Umberto's Restaurant.

Gardner, in her capacity as the Director of Food Services for HUFSD, helped secure lucrative contracts for Caliendo's company, Smart Starts, to provide prepackaged breakfast meals for Hempstead public school students.

In exchange, Caliendo kicked back a portion of the contract proceeds totaling more than $100,000 to Gardner through fraudulent payroll deposits and other payments. To conceal the illegal nature of the arrangement, those payments were deposited into a bank account that was created in the name of one of Gardner's family members.

The kicked back funds were spent by Gardner on international vacations, a leased vehicle, and home furnishings. Approximately $13,000 in kicked back funds were also withdrawn by Gardner in cash from ATMs located near her home and workplace. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee Pleads Guilty To Bank Bribery For Facilitating $2.2 Million+ Wire Fraud Scheme - November 10, 2022

From at least in or about 2018 through at least in or about May 2020, Luis Rivas who at the time of the offense was a Financial Sales Advisor at a Houston branch of a national bank.

Rivas agreed to accept payments in exchange for helping others open business bank accounts for phony companies. Those bank accounts were then used to receive more than $2.2 million in fraud proceeds. The money came from a business email compromise scheme in which businesses were defrauded by co-conspirators who impersonated, via email, individuals and businesses in the course of otherwise ordinary financial transactions, thereby fraudulently inducing the victims to transfer funds to bank accounts that the perpetrators controlled. The names of the phony companies used for the bank accounts that Rivas helped open were purposefully chosen to mirror the names of the true counterparties in those business transactions.

Rivas also helped the perpetrators access and launder the fraud proceeds. Rivas assisted with unfreezing, transferring, and withdrawing money in transactions designed to conceal and disguise the funds' source, ownership, and control.

Rivas was generally paid between $500 to $1,500 for each account that he helped open and each transaction where he provided assistance. He received, in total, approximately $45,000 for his corrupt insider services. (Source)

Bank Call Center Employee Admits To Role In Stealing Customer Identities To Steal $520,000+ - November 1, 2022

From August 2016 through August 2017, James Hill-Birdsong conspired with Lamar Melhado and others to defraud a Mount Laurel, New Jersey, bank.

Hill-Birdsong worked inside the call center and recruited other call center employees to participate in the scheme by stealing the identities and account information of customers who called into the bank's call center. The conspirator bank employees would then take photographs or screenshots of the bank customer's account information and signatures and would send that information to Hill-Birdsong and Melhado. The conspirators then had phony identification documents made in the names of the bank customers, and used various runners to go into bank branches and make unauthorized cash withdrawals. The conspirators also used the stolen identity information to conduct unauthorized online transfers of moneys from the customer's accounts. More then $520,000+ was stolen. (Source)

Former Bank Teller Sentenced To Prison For Embezzling $97,000 From Bank - November 7, 2022
David Ritter was employed as a Bank Teller at Summit Community Bank. From July 2020 until February 2021, Ritter embezzled more than $97,000 from five bank accounts. (Source)

Former Bank Employee Sentenced To Prison For Embezzling $38,000+ - November 9, 2022
Bailey Ricketts, age 27, was sentenced to one month in federal prison, followed by three months of home confinement, two years of supervised release, restitution in the amount of $38,135.43, and ordered to pay a $100 special assessment to the Federal Crime Victims Fund.

From August 2019 to November 2020, while employed at a bank, Bailey Ricketts knowingly embezzled $38,135 from the bank by transferring money into her own account and accounts belonging to her family members. (Source)

TRADE UNIONS

No Incidents To Report

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Facebook Fired Or Disciplined 24+ Employees For Improperly Taking Over User Accounts And In Some Cases Taking Bribes - November 17, 2022
Faceboook / Meta has fired or disciplined more than two dozen employees and contractors over the last year whom it accused of improperly taking over user accounts, in some cases allegedly for bribes.

Some of those fired were contractors who worked as security guards stationed at Meta facilities and were given access to the Facebook parent's internal mechanism for employees to help users having trouble with their accounts.

Meta says that in some cases workers accepted thousands of dollars in bribes from outside hackers to access user account.

A spokeswoman for Meta's security contractor, Allied Universal, said it "takes seriously all reports of violations of our standards of conduct." (Source)

Oil And Gas Company Employee Sentenced To Prison For Conspiracy To Steal Trade Secrets Worth $1.1 Million+ - 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. With its valve operations headquartered in Oklahoma City, the company manufactures compact manifold ball valves sold across the United States.

In March 2017, while employed as the controller at 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.

Decker was also ordered to pay a total of $1,116,885.49 in restitution to the victim oil company. (Source)

5 Former Hospital Employees Charged With Stealing Patients Information / Accepting Bribes - November 15, 2022

A federal grand jury has indicted 5 former Methodist Hospital employees for conspiring with Roderick Harvey, to unlawfully disclose patient information in violation of the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA.

Between November 2017 and December 2020, Harvey paid Kirby Dandridge, Sylvia Taylor, Kara Thompson, Melanie Russell, and Adrianna Taber to provide him with names and phone numbers of Methodist Hospital patients who had been involved in motor vehicle accidents. After obtaining the information, Harvey sold the information to third persons including personal injury attorneys and chiropractors. (Source)

CHINESE ESPIONAGE TARGETING U.S. COMPANIES / UNIVERSITY TRADE SECRETS

Chinese Government Intelligence Officer Sentenced To Prison For Espionage Crimes, Attempting to Steal Trade Secrets From Aviation Companies - November 16, 2022

The first Chinese government intelligence officer ever to be extradited to the United States to stand trial was sentenced today in federal court in Cincinnati.

Yanjun Xu was sentenced to 20 years in prison. Xu targeted American aviation companies, recruited employees to travel to China, and solicited their proprietary information, all on behalf of the government of the People's Republic of China (PRC).

Xu used aliases, front companies and universities to deceive aviation employees and solicit information. He identified individuals who worked for the companies and recruited them to travel to China, often initially under the guise that they were traveling to give a presentation at a university. Xu and others paid the individuals stipends on top of covering travel costs. (Source)

Employee Arrested For Stealing Trade Secrets For Chinese University - November 15, 2022

Yuesheng Wang was a researcher with Hydro-Quebec.

While employed by Hydro-Quebec, Wang allegedly used his position to conduct research for a Chinese university and other Chinese research centers. Wang published scientific articles and submitted patents in association with this foreign actor rather than with Hydro-Quebec.

Wang, an expert in battery technology, allegedly used information obtained from his work with Hydro-Quebec without the approval or knowledge of his employer, in effect using the company's intellectual property for the benefit of China. The alleged acts occurred between February 2018 and October 2022. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS /

Former Pharmacist Found Guilty For Her Role In $11 Million+ Scheme To Defraud The U.S. Military's Health Care Plan - November 23, 2022

Sandy Nguyen was a licensed Orange County, CA Pharmacist, and has been found guilty of nearly two dozen federal criminal charges for her role in a health care fraud scheme in which more than 1,000 bogus prescriptions for compounded medications were filled, costing Tricare, the U.S. Military's health care plan, more than $11 million in losses.

Nguyen was the Pharmacist in charge of the now defunct Wellness Pharmacy in Irvine, CA. From late 2014 to May 2015, Nguyen and others under her supervision filled approximately 1,150 compounded prescriptions for pain, scarring and migraines that Tricare reimbursed for tens of thousands of dollars per prescription. Nearly all of the prescriptions were sent to the pharmacy by so called marketers who were paid kickbacks of upwards of 50% of the Tricare reimbursements. (Source)

Unlicensed Medical Assistant Working For Physician Convicted In Her Role In $6 Million+ Fraud / Kickback Conspiracy - November 17, 2022

Rhonda Sutton worked as an unlicensed Medical Assistant for a Physician in Chicago and surrounding areas from at least 2009 until at least 2012.

Sutton conspired with others, including the owners of two home health care companies, to fraudulently certify Medicare beneficiaries for home health services for which those beneficiaries did not qualify.

Sutton forged her physician employer's signature on certification forms and supporting documentation, which caused Medicare beneficiaries to be enrolled in over 2,000 episodes of home health care at A&Z and Dominion home health agencies. Sutton provided the forged physician forms to A&Z and Dominion, which enabled A&Z and Dominion to submit claims to Medicare for services that the beneficiaries did not need and were not qualified to receive. The owners of A&Z and Dominion paid Sutton kickbacks in exchange for the forged physician forms. A&Z and Dominion received over $6 million from Medicare due to Sutton's fraudulent conduct. (Source)

Physician And Pharmaceutical Sale Rep Employee Plead Guilty To Roles In Prescription Drug Kickback ($331,000+) Conspiracy - November 1, 2022

Deepak Raheja was a Physician who specialized in Psychiatry and Neurology, practicing in Cleveland, Ohio. Raheja wrote prescriptions for a drug to patients that did not have the condition in exchange for money and other items of value.

Frank Mazzucco was employed by Avanir Pharmaceuticals as a regional business manager tasked with supervising pharmaceutical sales representatives in the region where Raheja practiced.

Between February 2011 and July 2016, Raheja, Mazzucco and other codefendants conspired together to increase the number of prescriptions Raheja and other coconspirators wrote for Nuedexta in exchange for the payment of monetary kickbacks and other items of value.

Raheja received approximately $331,550 in payments from Avanir between October 2011 and April 2016. During this time, Raheja wrote approximately 10,088 Nuedexta prescriptions – the highest in the country.

Raheja has agreed to a sentence of 30 months in prison, surrendering his medical license, at least $1,178,460.40 million in restitution and a fine to be determined. (Source)

Medical Assistant Charged With Stealing Patient Information For The Purpose Of Opening Credit Cards / Spending $31,000 And Leasing Apartments - November 11, 2022

Ashley Latimer was a Medical Assistant, and has been arrested for charges related to stealing patient information for personal use. Ashley Latimer used the information she collected from patient records and licenses to open credit cards, purchase items, and lease apartments.

An investigation found that Latimer used her cell phone to take photos of patient information forms and licenses while working at Axia Women's Health in Montgomery County, in Harrisburg, PA. She then used this information to open credit cards and spend more than $31,000 on purchases from Wayfair, an online furniture company, among other things. (Source)

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

Former Apple Employee Admits Role In Defrauding Company Out Of $17 Million - November 2, 2022

Dhirendra Prasad, who spent most of his decade at Apple working as a buyer in the Global Service Supply Chain department, admitted to "taking kickbacks, inflating invoices, stealing parts and causing Apple to pay for items and services never received," Prasad started these schemes in 2011 and continued them until 2018.

In one scam, Prasad shipped motherboards from Apple's inventory to CTrends, a company run by a co-conspirator, Don M. Baker. Baker harvested components from the motherboards, then Prasad organized purchase orders for those parts. After Baker shipped the components back to Apple, CTrends filed invoices for which Prasad arranged payment. In the end, the pair got Apple to pay for its own components and they split the proceeds of the scam.

Prasad also confessed to engaging in tax fraud. He directed payments from Robert Gary Hansen (Another Co-Conspirator Who Admitted Taking Part In The Schemes) straight to his creditors. Prasad arranged for a shell company to send sham invoices to CTrends with the aim of covering up illicit payments Baker made to him. This enabled Baker "to claim hundreds of thousands of dollars of unjustified tax deductions," the US Attorney's Office said. All told, prosecutors claim that the scams resulted in the IRS losing over $1.8 million. (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)

Construction Company Manager Pleads Guilty To Stealing $3.5 Million For Personal Use / Bought 5 Carat Diamond Ring - November 7, 2022

Michael Allen is the former Manager of ABB Construction, LLC.

Allen used his position to unlawfully divert $3.5 million in company funds for his own personal benefit. One of the items that Allen purchased with the stolen money was a 5.19 carat diamond ring for $113,250. (Source)

Company Bookkeeper Apprehended After 8 Years On The Run / Sentenced To Prison For Embezzling $2.2 Million+ - November 8, 2022

From July 2009 through December 2011, Russell Trapp was a Bookkeeper for Shelton Machinery, Inc., a Fishers-based distributor of advanced machines, drill-tap machines, production saws, and band saws. Trapp's duties included overseeing the preparation and mailing of checks to outside vendors.

Between September 2009 and December 2011, Trapp stole more than $2.2 million from Shelton Machinery by diverting checks made payable to one of Shelton Machinery's suppliers into his personal bank account. Trapp prepared fictitious or duplicate invoices for work that had already been billed and paid, as well as checks to pay the fictitious or duplicate invoices.

Trapp was arrested in January 2012. On June 8, 2012, Trapp was charged by Information and a petition to plead guilty was filed with the federal court on November 9, 2012. A change of plea and sentencing hearing was scheduled for March 7, 2013. Less than two weeks before the hearing, however, Trapp absconded from his residence, where he'd been ordered by the court to remain while on pretrial release.

Trapp's whereabouts remained unknown until 2021, when Deputy U.S. Marshals located him living under an assumed name in Utah. Trapp was arrested in October 2021 and transported back to Indiana to face the still-pending charges. Trapp formally pleaded guilty to the criminal charges on July 19, 2022. (Source)

5 Florida Home Owners Association Leaders Arrested For $2 Million Of Fraud - November 15, 2022

Current and former board members of the largest homeowners association (HOA) in Florida are being charged with plundering millions of dollars from the organization's finances.

Investigators arrested 5 members and vendors of the Hammocks Community Association, which oversees 40 communities and over 6,500 units in West Kendall. They are being accused of engaging in a complicated fraud, racketeering and money-laundering scheme that netted over $2 million in stolen funds.

The charges stem from a long-running probe that last year resulted in the arrest of the Hammocks homeowners association President Marglli Gallego. Since her arrest, the sprawling planned community of over 25,000 residents has been in turmoil, its coffers depleted, homeowners hit with 300% to 400% hikes in maintenance fees and the launching of a contentious recall effort against the board.

Gallego faces additional charges, and prosecutors charged her husband, Jose Antonio Gonzalez, 45. He's accused of running two companies that reaped at least $1.26 million in HOA funds.

Also charged: the current president, Monica Isabel Ghilardi, 52, board member Myriam Arango Rodgers, 76, and Yoleidis Lopez Garcia, 47, who served on the board between 2016 and 2022.

It was in April 2021 that prosecutors first charged Gallego on accusations she stole nearly $60,000 from the association – including money spent on a private investigator to spy on her perceived enemies in the neighborhood.

Prosecutors said that between November 2016 and March 2018, Gallego improperly used an HOA credit card for a wide array of personal purchases, including at supermarkets, bakeries and fast food restaurants such as Pollo Tropical, Panera Bread and Little Caesars. Her trial is pending.

An arrest warrant depicted her as using HOA resources to go after enemies, ordering the community's security to "harass" rival association members and filing lawsuits against people she felt were "targeting her unjustly."

Investigators say she and the board repeatedly ignored subpoenas, failing to turn over thousands of financial records while fighting with prosecutors over tens of thousands of dollars in reimbursement for the time and expense of gathering the records. At one point, she even filed lawsuits against a Miami-Dade economic crimes investigator who was leading the criminal probe that led to her arrest.

But as her criminal case wound through the legal system, the State Attorney's Office embarked on a wider fraud probe into the HOA – and again found itself stymied by the board while trying to subpoena financial documents.

Despite judges ordering the HOA to produce financial documents, the association refused to comply, even appealing one judge's ruling. An appeals court threw out the appeal. At one point earlier this year, an attorney for the board told a Miami-Dade judge the board voted to ignore the judge's order because "the board doesn't trust the state." (Source)

Former Office Manager For Small Family Owned Business Pleads Guilty To Embezzling $1.8 Million Over 15 Years - November 10, 2022

Edward Ziegler was employed as the Office Manager for a small family owned business, identified in court documents as Company A.

In approximately 2006, Ziegler opened a bank account in his name and with the qualifying language "Doing Business As Company A." Over the course of approximately 15 years, Ziegler diverted more than 400 checks, totaling approximately $1.8 million, from Company A's customers and deposited them into the secret bank account he had established. Ziegler also made fraudulent entries in Company A's books and record keeping system to cover up the fact that he had diverted the checks and used the funds for his own benefit. (Source)

Former Amtrak Employee And Her Husband Plead Guilty To Fraudulently Obtaining Nearly $1 Million In COVID Jobless Relief Funds / $63,000 In Fraudulent Sick Benefits From Amtrack - November 22, 2022

A former Amtrak employee (Lizette Lathon) pleaded guilty to criminal charges for conspiring with her husband (Kenneth Lathon) to steal nearly $1 million in COVID-19 pandemic-related unemployment insurance (UI) benefits and for fraudulently obtaining sickness benefits while she worked at Amtrak.

From 2014 until the present day, Lizette Lathon, in addition to her one-time duties as a service attendant for Amtrak, operated at least three tax preparation businesses: Miracle Tax Service, Hardcore Taxes and Lathon LLC.

Lizette Lathon and her husband took advantage of the expanded eligibility for unemployment insurance benefits made possible by the Coronavirus Aid, Relief, and Economic Security (CARES) Act signed into law in 2020.

In some instances, Lizette Lathon submitted fraudulent applications with the California Employment Development Department (EDD) for UI benefits using names, Social Security numbers and dates of birth that she obtained from former clients of her tax preparation businesses without the permission of those former clients. On the applications, she falsely asserted inflated income for the named claimants – many of whom had never lived in California – to receive the maximum benefit amount.

As a result of the fraudulent claims she filed, EDD authorized Bank of America to issue debit cards in the names of Lizette Lathon's former clients, but the cards were mailed to addresses she and her family controlled. She and her husband then used the debit cards to make cash withdrawals at ATMs and to make purchases at retail stores.

During the conspiracy, which lasted from the spring of 2020 until March 2021, Lizette Lathon and her husband caused at least 44 fraudulent unemployment claims to be filed, resulting in losses to EDD and the United States Treasury of approximately $998,630.

Lizette Lathon, who was employed at Amtrak from 2000 to 2021, also schemed to defraud the Railroad Retirement Board (RRB) out of sickness benefit payments by filing forged and false claims that stated she was being treated by a medical professional for pain and anxiety. Through this scheme, which lasted from September 2014 to January 2020, she fraudulently obtained approximately $63,047 in sickness benefit payments. (Source)

Company Credit Manager Pleads Guilty To Embezzling $850,000 To Pay For Personal Services & Expenses - November 1, 2022

From 2000 until 2020, Jeannie Valentin was the Credit Manager for the Oklahoma City branch of Dealers Electrical Supply (DES). Valentin was responsible for the management of the consolidated billing for DES's customers, which included processing checks made payable to DES and then forwarding the checks to DES's accounts payable department.

Valentin admitted that in 2003, she added DESCO as a DBA to her personal WEOKIE checking account without DES's knowledge or authorization. Valentin further admitted that between 2003 and 2017, she diverted approximately 144 checks sent from customers for payment to DES and deposited each of these checks into her personal WEOKIE checking account without DES's authorization. Valentin further admitted that used these funds to pay for various personal services and expenses. As a result of this scheme, Valentin defrauded DES out of approximately $854,449.06. (Source)

Former Union Benefit Plan Administrator Sentenced To Probation For Embezzling $140,000 - November 16, 2022

George Laufenberg is the former Administrative Manager for the Northeast Carpenters Pension Fund.

Laufenberg admitted stealing $140,000 that was paid to him under a deferred compensation agreement to which he was not entitled. (Source)

Former Accountant Sentenced To Prison For Embezzling $800,000+ From Employer For 7 Years - November 22, 2022

From 2012 until 2019, Renae Swanson embezzled $804,413 while working as an Accountant and Controller for Williams Plumbing & Heating. Swanson fraudulently altered the payroll process, resulting in her increasing the amount of money she received from the business. (Source)

Former Bookkeeper And Husband Sentenced To Prison For $340,000 Credit Card Fraud Scheme / Used Funds For Personal Items & Services - November 22, 2022

Desiree Madiedo was hired in 2004 by Company 1, a worldwide agribusiness, to work in the company's Tampa office. She initially worked as a Receptionist and was later assigned to work in the company's Accounting and Office Management Department where she handled the Tampa office's accounts receivable and accounts payable.

Around 2014, Desiree Madiedo's duties and responsibilities were expanded to include administration and reconciliation of Company 1's credit card account. Around the same time, she caused Company 1 to establish an automatic monthly payment to be made from its bank account to cover charges made by Company 1 employees against its credit cards. From then and until around January 2018, the Madiedo's utilized Desiree Madiedo's company credit card to purchase approximately $342,155 in personal items and services, which were not valid business-related expenditures.

In an effort to conceal the purchases of personal items and services by herself and her husband, Desiree Madiedo continued to collect and reconcile all of the other Company 1 employees' expense account reports, enter appropriate business expenditures made by the employees into Company 1's books and records, and ensure that the entire outstanding balance due the credit card company—which included charges made by the Madiedos against the company's credit card account for personal items and services—was paid in full.

Desiree Madiedo's husband, Christopher Madiedo was sentenced to 30 months in federal prison for his role in the wire fraud scheme. (Source)

Former Home Depot Employee Pleads Guilty In Credit Card Refund Fraud Scheme - November 1, 2022

Kimyada Knight worked in a specialized area of Home Depot (HD) business operations that primarily handled business and customer credit card accounts. Her area of responsibility included resolving charge disputes and requests for refunds from customers with credit card accounts and other accounts at HD.

An initial review by HD, with a follow up investigation by the United States Secret Service, determined that Knight had initiated a large number of fraudulent customer and business refunds between approximately January and August 2019 involving credit card accounts and other accounts at HD. After processing the fraudulent transactions, Knight then transferred the payments to accounts that she controlled and subsequently used the proceeds. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

2 Former Executives Of Non-Profit Organization Charged For $10.7 Million Fraud Scheme Using False Invoices / Unauthorized Use Of Credit Cards - November 11, 2022

Two former executives for Saint Francis Ministries (SFM) have been indicted by a Grand Jury of allegedly defrauding the nonprofit.

Robert Smith is the former CEO and President of SFM. Smith conspired and engaged in a scheme to defraud SFM of money and property, along with a second individual, William Whymark. Whymark was the CEO of WMK Research, Inc. and SFM says he previously served as Chief Information Officer.

Smith and Whymark defrauded SFM by the submission and approval of materially false invoices to SFM resulting in payments to Whymark totaling over $10 million. It also claims Smith used Saint Francis credit cards for personal expenses, causing Saint Francis to improperly pay for those expenses.

The scheme allegedly began in Jan. 2018 and continued until July 2021.

Around February 2018, the Saint Francis Ministries Board agreed to improve its IT systems, hardware, and software programs.

Roughly a month prior, in Jan. 2018, Saint Francis and Whymark entered into a contract for Whymark to work on the project. Smith and Whymark were signatories, according to the documents.

There was no competitive bid for the project, and the SFM Board of Directors' meeting minutes for 2018 did not reflect any record of Smith seeking authorization or informing the board of his decision to award the SFM Project to WMK.

Smith approved all WMK invoices even when the dollar amount exceeded his approval authority. Allegedly, he did not bring the invoices to the attention of the board for their approval, which is required by SFM policy.

The invoices were fraudulently inflated by approximately $4.7 million. During the course of the contract, Whymark submitted invoices to Saint Francis, resulting in 65 payments to WMK totaling approximately $10.7 million.

Smith failed to report his personal purchases on Saint Francis corporate credit cards and failed to reimburse Saint Francis for personal purchases. These purchases included: Cash withdrawals, clothing and jewelry, personal travel expenses. (Source)

Former Employee For Commercial Real Estate Agency Arrested For Embezzling $2.6 Million From Employer By Submitting Fictitious Invoices - November 14, 2022

Varun Aggarwal is a former executive at a commercial real estate agency. He was arrested on a federal criminal complaint alleging a decade-long scheme in which he stole $2.5 million by submitting fictitious invoices for companies controlled by his family and friends whose services were never performed.

Beginning at least in 2012 and continuing through January 2022, Aggarwal used his position at the Newport Beach-based KBS Realty Advisors to embezzle his employer's money.

Aggarwal worked in the company's Internal Auditing Department, rising to the level of the Department's Director. As a member of the company's accounting group, Aggarwal was intimately familiar with KBS's policies and procedures for payments to vendors. Aggarwal used his knowledge of KBS's policies and procedures to have his friends and family perform contracting work for his groups at KBS.

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

A review of company, bank and tax records show that Aggarwal, using approximately six vendors, stole approximately $2,601,246 from KBS between approximately January 1, 2012, and January 13, 2022. (Source)

Company Branch Manager Sentenced To Prison $549,000+ For Fake / Fraudulent Invoice Billing Scheme - November 4, 2022

Michael Goll was the Branch Manager of a company that provides material handling equipment to businesses.

From January 2013 through September 2017, Goll defrauded his company of approximately $549,667.39. Goll is alleged to have executed the scheme by sending his company false invoices from shell companies that he had created, when in fact the work was either done by the company's own employees or the work was not done at all.

Golll had a contractor who did personal work for inflate his bills to the company to cover the work done for Goll. Goll justified the over billing by telling the contractor that he planned on buying company in the future, although Golll never did purchase the company. (Source)

THEFT OF COMPANY PROPERTY

No Incidents To Report

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

Deloitte Consulting In India Fires Employee After Discovering He Was Running Hacking Side Business - November 8, 2022

Deloitte India said it has fired the person who was reportedly running a hacking firm on the side. The Sunday Times and the Bureau of Investigative Journalism conducted a sting operation that's said to have exposed India-based hacking groups targeting VIPs globally.

Aditya Jain, an associate director with Deloitte's cyber unit, was running hacking firm WhiteInt, according to the report. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

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

A California announced the prosecutions of 20 defendants in a series of DMV corruption cases charged in the Eastern District of California. Charges against the defendants included bribery of public officials, identity fraud, unauthorized access of computers, and conspiracies to commit those offenses. The defendants included corrupt DMV employees who took bribes, trucking school owners and affiliates who bribed them, and others who participated in the conspiracies. The criminal activities charged in these cases took place throughout California, including the Central Valley, Los Angeles Basin, and as far north as Eureka.

Defendants 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)

EMPLOYEE DRUG RELATED INCIDENTS

Nurse Pleads Guilty To Stealing Fentanyl From Elderly Patients For Her Own Use - November 22, 2022

Ryan Thornton admitted that he diverted and stole liquid fentanyl from elderly patients that was supposed to be dispensed to patients, for his own personal use, by removing fentanyl from the patients' IV pumps with a syringe. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE

Chesapeake, Virginia Walmart Employee Kills 6 Co-Workers / 4 Wounded - November 23, 2022

The City of Chesapeake, Virginia, has identified Andre Bing as the alleged Walmart employee who opened fire on November 22, 2022 night at one of the company's stores there, killing 6 people before police say he turned his pistol on himself.

Bing was an overnight team lead and he's been employed with Walmart since 2010. Bing was armed with one handgun and had multiple magazines.

Employee Briana Tyler said the overnight stocking team of about 15 or 20 people had just gathered in the break room to go over the morning plan. She said the meeting was about to start, and her Bing saying "All right, guys, we have a light night ahead of us," when her manager turned around and opened fire on the staff.

"It is by the grace of God that a bullet missed me," Tyler said. "I saw the smoke leaving the gun, and I literally watched bodies drop. It was crazy."

At first, Tyler didn't think the shooting was real. "It was all happening so fast. I thought it was like a test type of thing. Like, if you do have an active shooter, this is how you respond."

Tyler, who worked with the manager just the night before, said the assailant did not aim at anyone specific.

"He was just shooting all throughout the room. It didn't matter who he hit. He didn't say anything. He didn't look at anybody in any specific type of way." (Source 1)

Bing legally purchased the 9mm handgun from a local store on the morning of the shooting. He had no criminal history. Police found a box of ammunition and various items in reference to the 9mm handgun at Bing's home.

UPDATE

Virginia Walmart Gunman's Manifesto Claims He Was Betrayed By Coworkers He Killed, Felt Led By' Satan - November 25, 2022

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

"Sorry God, I've failed you, this was not your fault but my own. I failed to listen to the groans of the holy spirit which made me a poor representation of you," Bing wrote in a note released Friday by the Chesapeake Police.

Bing wrote that he "Was harassed by idiots with low intelligence and a lack of wisdom," specifically mentioning an incident in which his "Dignity was completely taken away beyond repair by my phone getting hacked."

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.

"My true intent was never to murder anyone believe it or not, I was actually one of the most loving people in the world if you would get to know me. I just wanted a wife that was equally yoked as I and obsessed over the thought; however, I didn't deserve a wife," Bing wrote.

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)

EMPLOYEES INVOLVED IN TERRORISM

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE

This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

View On The Link Below Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

WORKPLACE VIOLENCE TODAY E-MAGAZINE

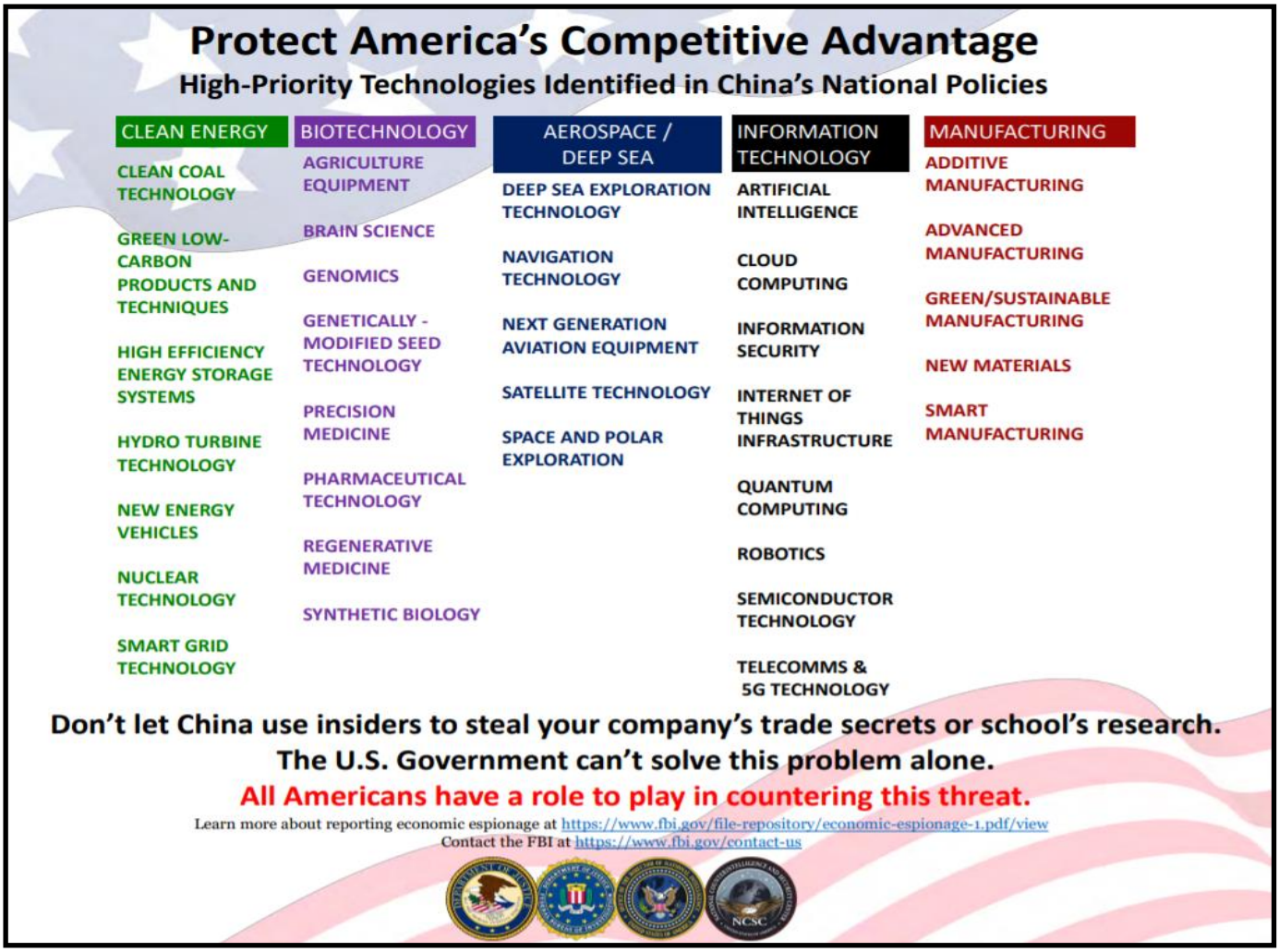
https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,200+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

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 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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