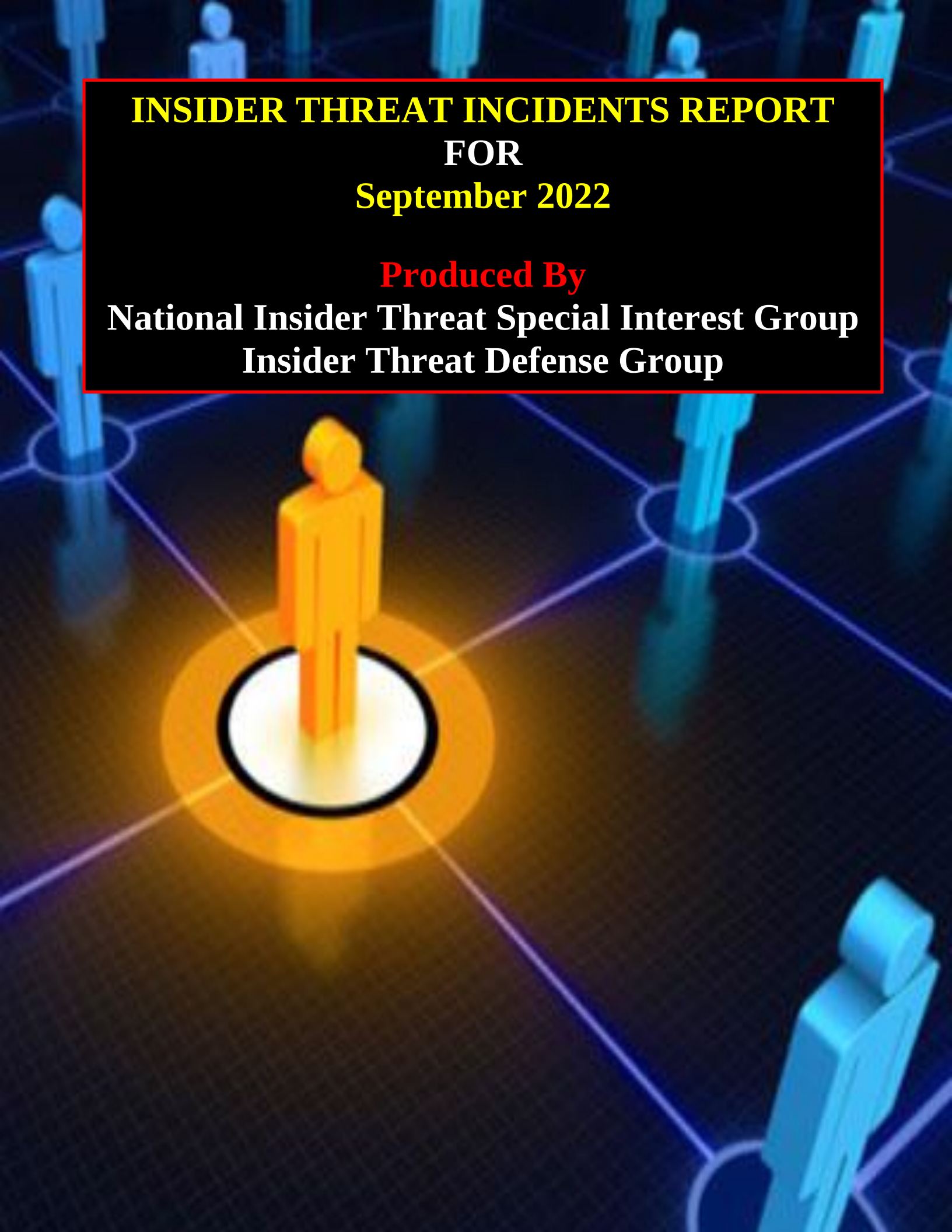


INSIDER THREAT INCIDENTS REPORT
FOR
September 2022

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 **4,000+** 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 21 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.

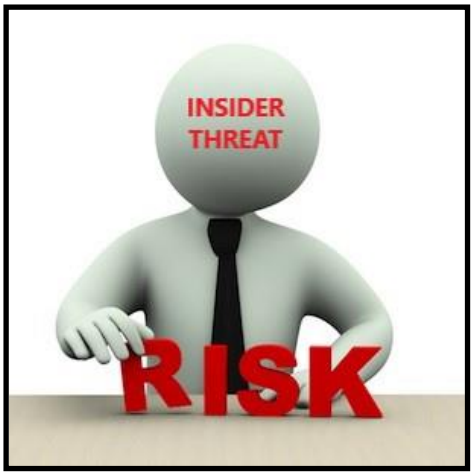
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees Transforming To Insider Threats
- ☐ Theft Of Organizations Assets
- ☐ 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 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 SEPTEMBER 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT
Multiple U.S. Postal Service Employees And Others Arrested For $1.3 Million Fraud And Identity Theft Scheme - September 29, 2022

Between in or around December 2018, up to and including the present, members of the conspiracy worked with U.S. Postal Service mail carriers, to steal credit cards from the mail stream before those cards were delivered to the assigned credit card customers.

After obtaining the stolen credit cards, members of the conspiracy activated the cards using stolen personally identifiable information (PII) of the intended recipients. Members of the conspiracy then used the stolen cards to purchase luxury goods, including items manufactured by, among others, Chanel, Fendi, Hermes, and Dior, from high-end retailers, including major department stores in and other places. (Source)

Former IRS Employee Pleads Guilty To Fraudulently Obtaining $62,000+ In CARES Act Funds While Working For IRS - September 28, 2022

In July 2020, Charles Clark fraudulently applied for a loan under the Economic Injury Disaster Loan (EIDL) program.

In his EIDL application, Clark falsely claimed to have been an independent contractor working in the "Hair & Nail Salon" industry when he was working as a full-time IRS employee. He obtained $62,300 in funds which he then misused by spending them on renovating an investment property he owned. (Source)

U.S. Postal Service Employee Admits To Role In Stealing $12,000 Worth Of Cell Phones From Mail / Then Selling - September 12, 2022

Nyasia Hutchinson was employed by the U.S. Postal Service as a postal service clerk at the Elizabeth Post Office (EPO).

From May 1, 2018, through Dec. 31, 2018, another EPO employee provided Hutchinson with 15 to 20 stolen cell phones that the employee had taken out of packages at the EPO that had been mailed to a Hillside, New Jersey, business. Hutchinson admitted that she taped up empty packages and placed them back in the mail stream after cell phones had been removed. Hutchinson later sold the stolen iPhones which had a total approximate value of $12,000, keeping the sales proceeds for herself. (Source)

Former Puerto Rico Legislator Sentenced To Prison For $190,000 Bribery & Kickback Scheme - September 7, 2022

Nelson Del Valle Colón pleaded guilty in the District of Puerto Rico to federal program bribery on March 31, 2022.

Del Valle Colón was elected to be a member of the Puerto Rico House of Representatives in 2016. He thereafter hired Mildred Estrada-Rojas and her daughter, Nickolle Santos-Estrada o, to work in his legislative office.

In exchange for their employment and their salaries, however, Estrada and Santos paid biweekly kickbacks to Del Valle Colón of between approximately $500 and $1,300 from early 2017 until approximately July 2020.

Del Valle Colón, Estrada, and Santos admitted that the biweekly kickbacks were paid in a variety of ways. Estrada and Santos generally paid their biweekly cash kickbacks in envelopes that they provided to Del Valle Colón in offices in the Capitol building in Old San Juan. Estrada sometimes paid her kickback to Del Valle Colón over ATH Móvil, a mobile phone cash transfer application.

Del Valle Colón was also ordered to pay $190,000 in restitution. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former NSA Employee Arrested On Espionage Related Charges - September 29, 2022

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

Between August and September 2022, Dalke used an encrypted email account to transmit excerpts of three classified documents he had obtained during his employment to an individual Dalke believed to be working for a foreign government. In actuality, that person was an undercover FBI agent. Dalke subsequently arranged to transfer additional classified information in his possession to the undercover FBI agent.

Dalke began communicating on or about July 29, 2022, via encrypted email with an individual he believed to be associated with a foreign government. Dalke told that individual that he had taken highly sensitive information relating to foreign targeting of U.S. systems and information on U.S. cyber operations, among other topics. Dalke represented to the undercover FBI agent that he was still employed by the U.S. government but said he was on a temporary assignment at a field location. Dalke requested compensation via a specific type of cryptocurrency in exchange for the information he possessed and stated that he was in financial need.

To prove he had access to sensitive information, Dalke transmitted excerpts of three classified documents to the undercover FBI agent. Each excerpt contained classification markings. One excerpt was classified at the Secret level, and two excerpts were classified at the Top Secret level. In return for this information, the FBI undercover agent provided the requested cryptocurrency to an address Dalke provided.

On or about Aug. 26, 2022, Dalke requested $85,000 in return for additional information in his possession. Dalke also told the FBI undercover agent that he would share additional information in the future, once he returned to the Washington, D.C., area. Although he was not employed by the NSA while communicating with the FBI, Dalke re-applied to the NSA in August 2022. (Source)

Former Army Major And Wife Tried To Leak Military Health Data To Help Russia Gain Insights Into The Medical Conditions Of U.S. Military - September 30, 2022

Jamie Lee Henry, the former U.S. Army Major who was also a doctor at Fort Bragg in North Carolina, and his wife, Dr Anna Gabrielian, were charged in an unsealed indictment in a federal court in Maryland with conspiracy and the wrongful disclosure of individually identifiable health information about patients at the Army base.

The indictment alleges that the plot started after Russian President Vladimir Putin invaded Ukraine.

Prosecutors said the pair wanted to try to help the Russian government by providing them with data to help the Putin regime gain insights into the medical conditions of individuals associated with the US government and military.

The two met with someone whom they believed was a Russian official, but in fact was actually an FBI undercover agent.

At a hotel in Baltimore on Aug 17, Dr. Gabrielian told the undercover agent she was motivated by patriotism toward Russia to provide any assistance she could to Russia, even if it meant being fired or going to jail.

In the meeting, she volunteered to bring her husband into the scheme, saying he had information about prior military training the United States provided to Ukraine, among other things.

At another meeting later that day, Henry told the undercover agent he too was committed to Russia, and claimed he had even contemplated volunteering to join the Russian army. (Source)

4 Army Depot Officials & Vendors Sentenced To Prison For Federal Bribery And Conspiracy Scheme - September 13, 202

Jimmy Scarbrough was the Equipment Mechanic Supervisor at the Red River Army Depot (RRAD) in Texarkana, Texas, a position he held from November 2001 until May 2019.

Scarbrough directed more than $7 million in purchases from RRAD to RRAD Vendor Jeffrey Harrison and Justin Bishop through the government purchase card (GPC) program. In order to manipulate the GPC program, which is designed to ensure a competitive bidding process, Scarbrough told the vendors what to bid, including the item, the quantity, and the price. By collecting fake bids from multiple vendors, Scarbrough was able to direct RRAD purchases to his select vendors, in this case Harrison and Bishop, while maintaining the appearance of a competitive bidding process. Scarbrough also defrauded the United States by falsely certifying that he had received the purchased items, therefore causing the RRAD to pay his select vendors. However, the reality was that Scarborough instructed the vendors not to deliver certain RRAD-purchased items.

Scarbrough demanded hundreds of thousands of dollars in bribes from his selected vendors. Scarbrough accepted bribes in various forms, including receiving at least $116,000.00 in U.S. Postal Service money orders from Harrison. Scarbrough also had Harrison and Bishop purchase at least $135,000.00 in car parts or services for his hot rod collection, which included a red and black 1936 Ford Tudor, an electric green 1932 Ford Coupe, a cherry red 1951 Ford F-1 truck, and more. Scarbrough received more than $27,000.00 worth of firearms from Bishop, including rare Colt handguns and Wurfflein dueling pistols. Finally, Scarbrough directed at least $32,000.00 in donations to the Hooks Volunteer Fire Department while he was the Capitan of Operations. In total, Scarbrough received more than $300,000.00 in bribe payments from Harrison and Bishop.

Scarbrough is not the only official at RRAD who accepted bribes. Devin McEwin accepted more than $21,000.00 in bribes from Harrison, including hunting trips, donations directed to the Annona Volunteer Fire Department, and the refurbishment of his 1964 Ford truck. Additionally, Louis Singleton accepted more than $18,000 in bribes from Harrison and others, including tickets to the Hall of Fame section of AT&T Stadium for the Dallas Cowboys football game against the New England Patriots. Singleton was the supervisor of the GPC program at the RRAD and was responsible for approving purchases requested by Scarbrough. (Source)

2 Former Managers Working For Military's Private Housing Contractor Sentenced To Probation For Defrauding Air Force Out $3.5 Million - September 13, 2022

Stacy Cabrera, who managed Balfour Beatty Communities-owned housing at Lackland Air Force Base, Texas, and Rick Cunefare, who was a regional manager at Balfour Beatty, were both sentenced Thursday in the U.S. District Court for Washington, D.C., according to court records.

Both Cabrera and Cunefare pleaded guilty in 2021 to charges stemming from a scheme in which Balfour Beatty was accused of manipulating maintenance records to obtain performance bonuses from the military while covering up unsafe housing conditions from 2013 to 2019.

The company itself pleaded guilty last year to the scheme to defraud the Army, Air Force and Navy, and agreed to pay $65 million in fines and restitution.

Cunefare, who pleaded guilty to major fraud, was responsible for reviewing and approving the maintenance reports from Lackland, as well as Travis, Vandenberg, Tinker and Fairchild Air Force bases. according to the Justice Department. Cabrera, who pleaded guilty to conspiracy to commit wire fraud, was accused of personally falsifying maintenance reports.

Together, their actions made Balfour Beatty about $3.5 million the company didn't earn, the Justice Department said in a sentencing memo. Still, because they were both "low- and mid-level managers with minimal financial incentive to commit fraud," prosecutors sought lenient sentences.

Cabrera has said she was pressured by her superiors to fake the reports, but has also expressed regret for her actions. (Source)

Former Veterans Affairs Hospital Employee Sentenced To Prison For Stealing Almost $500,000 In Government Funds - September 22, 2022

Bruce Minor pleaded guilty to one count of theft of government funds. The charge arose from his theft of approximately $487,000 in Veterans Affairs travel reimbursement funds, which he helped administer as part of his official duties as a travel clerk.

In order to perpetrate the theft, Minor created fraudulent travel reimbursement claims in the names of at least three other VAMC employees and then diverted the fraudulently obtained funds into bank accounts he controlled. (Source)

CRITICAL INFRASTRUCTURE

Former Public Works Department Employee Charged With $150,000+ Of Identity Theft Using Employee Credit Cards For Car Repairs, Furniture, Etc. - September 8, 2022

Allison Donaldson was employed as an Administrative Manager for the City of Covington Public Works Department in Kentucky, from 2005 until 2022.

Donaldson had access to credit card information for the department. Starting in February 2020 and continuing until February 2022, Donaldson knowingly defrauded the City of Covington by using employee credit cards, making over $150,000 in purchases for herself and her home. The purchases listed in the indictment include repairs for a Mercedes Benz, Crate & Barrel furniture, and designer counter stools. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Lieutenant Colonel Of Kentucky State Police Convicted Of $40,000 Theft Of Ammunition - Government Property - August 31, 2022

Michael Crawford was a former Lieutenant Colonel of Kentucky State Police (KSP).

In 2016, Crawford conspired with John Goble, the former Coroner of Scott County, and KSP armorer, Mitch Harris, to unlawfully misappropriate 21 firearms belonging to Kentucky State Police, including 19 shotguns and 2 M1A rifles. Crawford's co-defendant, Goble, previously pleaded guilty to a related conspiracy between the same individuals to misappropriate 187 cases of KSP ammunition, valued at approximately $40,000, which was stored in the basement of Goble's office. (Source)

2 Former Volunteer Firefighters Face Fraud & Embezzlement Charges - September 22, 2022

2 West Virginia volunteer firefighters are facing charges of conspiracy, fraud, and embezzlement. A grand jury handed down an indictment accusing Cody Perry and Thomas Perry Jr. of overcompensating themselves and three others.

The payments were made for more than $1,000 coming out of the department's pocket. The two men used to be in charge of their finances, but haven't been for months now. The payments were made between January 2015 and September 2020, investigators say. (Source)

STATE / CITY GOVERNMENTS

Former City Of Atlanta Director Of Human Services Sentenced To Prison For Accepting $3 Million In Bribe Money - September 8, 2022

Mitzi Bickers has been sentenced to 14 years in prison for accepting approximately $3 million in bribe money to influence government contracts, money laundering, lying to the City of Atlanta to maintain her salary and cabinet-level position, and failing to disclose more than $600,000 in income on her federal tax return. (Source)

Former County Clerk Sentenced To Prison For $1.5 Million+ Wire Fraud Scheme To Fund His Business - September 21, 2022

Former Craighead County Clerk Jacob Holliday was sentenced to prison for taking more than $1.5 million in county money for his personal use.

In June 2020, Craighead County officials reported that a theft had occurred from the Craighead County Clerk's office. The bank that managed the Clerk's office account had flagged suspicious activity, and auditors concluded that approximately $1,579,057.03 was missing and had been moved to Holliday's personal banking accounts.

Law enforcement interviewed Holliday, who admitted to taking the money to fund his businesses: Holliday Development and Management, LLC, and Total Healthcare, LLC, both of which operated restaurants and coffee shops. Holliday told investigators he planned to pay the money back, but once the COVID-19 pandemic caused most of his businesses to close, he could not replace the money. (Source)

Former Town Finance Director Pleads Guilty To Embezzling $500,000+ For Personal Use - September 21, 2022

Cameron Tucker was the Finance Director and Accounting Technician for the Town of Spring Lake, in Raleigh, N.C. She pled guilty today to embezzling over $500,000 from the Town of Spring Lake between 2016 and 2021.

Tucker wrote checks from the Town's bank accounts for her personal use, forging the signatures of other town officials, including the mayor and town manager. These forged checks were made payable to herself, used to cover her personal expenses, and deposited into bank accounts she controlled. (Source)

Former County Attorney & Legal Secretary Sentenced To Prison For $365,000 Of Wire Fraud & Federal Program Theft For Personal Expenses - September 27, 2022

The former County Attorney for Lawrence County, Kentucky Michael Hogan, and his wife and legal secretary, Joy M. Hogan were sentenced to 42 months and 12 months and one day in prison.

The Hogans conspired with each other to commit wire fraud by issuing checks from a second delinquent tax account for the Lawrence County Attorney's Office, the statements for which went to their personal residence.

Michael Hogan and Joy Hogan would routinely prepare bonus checks issued to Joy, and signed by Michael, paid with delinquent tax funds that should have been used on operating expenses for the Lawrence County Attorney's Office.

The Hogans deposited these checks in Joy's personal account and the couple's joint accounts and spent the funds on personal expenses. Michael Hogan admitted he personally benefitted from these payments and knew some of these payments were not reasonable in amount, nor beneficial to the public. According to the indictment, between March 8, 2013, and April 30, 2020, Michael Hogan paid Joy Hogan more than $365,000 from the Lawrence County Delinquent Tax Account. (Source)

Former Secretary / Treasurer Of County Township Pleads Guilty To Embezzling $150,000 - September 13, 2022

Linda Baun was formerly employed as the Secretary / Treasurer for Jackson Township, in Mercer County, Pennsylvania.

Between 2011 and 2019, she embezzled at least $150,000 from the Township by making unauthorized ATM withdrawals and by charging personal purchases on Amazon to the Township's debit card. She has agreed to a restitution amount of $150,000. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former School Business Manager Charged With $1 Million+ Wire And Bank Fraud Offenses / Used Funds For Travel & Luxury Items - September 13, 2022

James Melis abused his position as Business Manager at a private school in Tampa by attaching his personal bank account to the school's PayPal account without authorization. When parents made tuition payments to the school's account, Melis initiated fraudulent electronic funds transfers to his personal account. He then spent the stolen funds on travel and luxury items, such as jewelry.

The indictment also notifies Melis that the United States is seeking an order of forfeiture in the amount of $1.1 million, the proceeds of the charged criminal conduct. (Source)

Former University Accounting Manager Sentenced To Prison For Making $12,000+ Of Unauthorized Credit Card Charges For Personal Benefit - September 26, 2022

Ralph Puglisi was employed as an Accounting Manager for the University of South Florida's University Medical Services Association (UMSA). In this position, he was involved in overseeing the administration of UMSA's credit cards.

Beginning in or around June 2014, and continuing through November 2019, Puglisi defrauded UMSA by using several of that entity's credit cards to make $12,860,744.07 in unauthorized charges for his own benefit, including rent payments, extensive home renovations, travel, chartered yachts, and contributions to women affiliated with an interactive adult website. Puglisi exploited his position as accounting manager to make false journal entries in records that created the illusion that his charges were related to UMSA's business operations. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Bank Manager Accused Of Defrauding Elderly Customers Of $328,000+ - September 15,, 2022

Andrea Hopkins' indictment alleges that from Feb. 20, 2020 to May 25, 2021, while manager of the Commerce Bank, she devised a scheme to divert money from numerous customer accounts for her own use.

Hopkins targeted elderly customers, including two 80-year-olds, one 95-year-old and one 82-year-old. She logged into customer accounts and transferred funds out, sometimes obtaining cashier's checks or prepaid cards. She changed the address on some account statements, forged customer signatures and transferred funds among customers to try and hide the thefts.

Hopkins fraudulently diverted $328,273 from customer accounts, but $152,431 of that she transferred internally among customers to hide her theft. (Source)

Former Credit Union Manager Charged With Embezzling $268,000 For Personal Expenses - September 9, 2022

Between August 2016 and August 2021, Phillip Topping while employed at New Pilgrim Federal Credit Union as a Manager, embezzled approximately $268,000 from an on-site ATM and from a teller cash drawer at New Pilgrim Federal Credit Union. Topping used the unauthorized funds for personal expenses. (Source)

Former Credit Union Manager Charged With Embezzling $210,000+ Over 10 Years - September 21, 2022

Gloria Hall was the Manager at Prairie View Federal Credit Union in Houston Texas, from February 2000 to August 2020.

Beginning in 2010, she allegedly embezzled approximately $211,563 from elderly account holder funds. She created loans totaling nearly $791,000, withdrew the loans and cashed $76,772 in numerous unauthorized checks from accounts at the credit union for her own personal use and benefit.

Hall allegedly fraudulently formed 58 nominee loans by creating fake share loans in the names of relatives and friends. She transferred money across the loans to make payments among them.

She also allegedly created fake monthly loan statements and moved funds mainly from elderly credit union members into the accounts of her relatives and friends. (Source)

Former Bank Financial Advisor Pleads Guilty To Stealing $158,000+ - September 28, 2022
From 2016 to 2021, Tyler Rigsbee worked as a financial advisor at a major bank in Sacramento.

During his employment, Rigsbee stole over $158,000 from the accounts of two bank customers. Rigsbee stole this money by transferring it from customer accounts to brokerage accounts he created at E-Trade, a third-party financial institution. He then transferred the money from these brokerage accounts to his own personal bank account. Rigsbee also attempted to conceal his scheme by partially replacing some of what he stole from one of these bank customers with money he took from the account of a third bank customer.

After the death of one bank customer in August 2018, Rigsbee created a fraudulent request for distribution of eligible assets from a transfer-on-death account by falsely pretending that he was the deceased customer's beneficiary. On March 15, 2019, Rigsbee submitted this request for distribution of eligible assets to the bank's estate processing department, which caused the liquidation of the customer's account and transfer of these funds to a brokerage account Rigsbee created and controlled. (Source)

TRADE UNIONS

Former Union Financial Secretary Pleads Guilty To Embezzling $38,000+ - September 29, 2022
From about late 2015, until December 2019, Jay Garnsey was employed by Remington Arms in Ilion, NY and the Financial Secretary of the union that represented its employees.

Garnsey admitted that, while he was Financial Secretary, he embezzled money from the union by, among other things, submitting fraudulent reimbursement vouchers. Garnsey admitted embezzling over $38,000 in union funds. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Broadcom Engineer Sentenced To Prison For Theft Of Trade Secrets - September 20, 2022
Engineer Stole Trade Secrets Before His Departure from Broadcom, Then Accessed and Referenced Trade Secrets While Working For China Based Startup Company

Peter Kim resigned from Broadcom effective July 17, 2020, and in the days before he left Broadcom, Kim copied more than 500 Broadcom files from its document repository system. In pleading to trade secret theft, he admitted to possessing Broadcom trade secrets related to the Trident family of chips, including those contained in test plans, design verification environment files, and design specifications. He admitted that he knowingly possessed the Broadcom trade secrets knowing that he took them from Broadcom. He also acknowledged that Broadcom took reasonable measures to keep the Broadcom trade secrets secret, including by storing the trade secrets on non-public document repositories in which the access permissions were restricted, requiring appropriate nondisclosure agreements to be executed before the trade secrets could be shared outside Broadcom, and in view of the confidentiality agreements Kim signed with Broadcom and the annual trainings he received, among other things.

Less than two weeks after he left Broadcom, Kim began working as IC Design Verification Director for a startup company based in the People's Republic of China (PRC).

Kim acknowledged that the company was seeking to become a leading chip designer focused on the PRC's domestic market for networking chips at the time. During Kim's employment at his new company, Kim repeatedly accessed and referenced the Broadcom trade secrets on his personal electronic devices as well as the laptop issued by his new employer.

Kim admitted in his plea agreement that, having taken the Broadcom trade secrets for reference purposes, he knew that having them could advance the quality of his work as an employee for his new employer and therefore economically benefit the company. Kim also admitted that he knew that his actions could injure Broadcom, including because his new employer was seeking to become a competitor to Broadcom by developing competing products abroad. (Source)

Former Walgreens Health Care Worker Photographed Patient Credit Cards And Went On Shopping Spree - September 28, 2022

A Maryland woman accused of using stolen credit and debit card information, then using it to shop online has been charged with 120 counts of theft and fraud.

The woman was employed at a Walgreens in Cambridge, Maryland, before starting a job at Your Doc's Inn, an urgent care clinic in the same city. The woman is accused of taking pictures of credit and debit cards belonging to patients and customers at both locations, according to the release. The cards were then used to purchase a variety of items online, from November 2021 to Sept. 7, police stated. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS /

2 Health Services Clinic Employees Found Guilty Of Embezzling $30,000+ From Employer - September 30, 2022

In June 2013 Jerome Kangas was hired as a Clinician in the Park Nicollet CPAP clinic, where David Koch was the supervisor and later manager. CPAP machines are devices commonly used to treat sleep apnea.

Between June 2013 and June 2018, Koch and Kangas defrauded Park Nicollet out of hundreds of thousands of dollars in compensation. Although Kangas worked only afterhours and weekends responding to CPAP patient calls, Koch entered more than 8,500 weekday hours in the Park Nicollet records to cause Kangas to be paid for work he did not perform. On most of the days for which Kangas was paid, the evidence showed that he was either working for another employer or out of town. The evidence at trial also showed that Koch logged into the company network for Kangas and helped Kangas reset his computer password to conceal that Kangas was not working as his job description required. The scheme was discovered when Koch was laid off in 2018 as a result of the acquisition of Park Nicollet by HealthPartners.

The currency transaction structuring related to a 12-day period in July and August 2017 when Kangas made six withdrawals between $5,000 and $5,500 from four different Wells Fargo Bank branches, for a total of $30,500. Federal law requires banks to report currency transactions over $10,000, as a means of detecting financial crimes. Four days after the last $5,500 withdrawal by Kangas, Koch made a $29,300 cash deposit into his own US Bank account. (Source)

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

Former Chief Financial Officer Admits To Embezzling $3.7 Million+ - September 6, 2022

From January 2018 through December 2020, Any Aldi abused her position as Chief Financial Officer and Director of Operations for a New Jersey company.

She embezzled millions of dollars by withdrawing cash from the company's operating account and then using the cash for her own personal benefit. Aldi, without authorization, made over 200 cash withdrawals, in amounts ranging from $5,000 to $25,000 per withdrawal, totaling more than $3.7 million. Aldi concealed the theft by falsifying company accounting and financial records, including making false journal entries and altering bank statements issued to the company for the company's operating account. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $3.6+ Million Over 6 Years To Purchase Properties, Vehicles, Travel, Pay Credit Cards - September 19, 2022

Trina Welch was employed by Kasco of Idaho, LLC as a bookkeeper from 2012 until 2019. Kasco is a construction and telecommunication company that does work in Washington, Idaho, Oregon, Montana, and Alaska.

Beginning in at least 2013 and continuing until the day she was terminated on July 3, 2019, Welch used her position as a bookkeeper to engage in a scheme and plan to defraud Kasco and obtain money and property for herself. Welch conducted the scheme by issuing 341 fraudulent checks to purchase properties, vehicles, and travel for herself, her family, and her friends.

In January of 2022, Welch pleaded guilty to the charge of wire fraud, admitting that in 2017 alone she took over $930,000 just to pay her Bank of America credit cards. As part of the plea agreement, Welch admitted writing the 341 fraudulent checks, and agreed to pay restitution and forfeit her interest in any of the properties she bought with the money. However, she contested that the entire amount of the checks represented a loss to Kasco. Welch's scheme caused a $3,673,934.00 loss to Kasco. (Source)

Former Director Of Accounting Services Charged With Embezzling $2 Million Using Corporate Credit Cards For Vacations, Tuition & To Fund Family Business - September 30, 2022

Catherine Latoski was the Director of Accounting Services for a Scranton-based for-profit educational institution.

Beginning in November 2016, through her termination in June 2021, Latoski allegedly charged approximately $2,000,000 in personal expenses on corporate credit cards issued by her former employer, spending the funds on vacations, Disney timeshares and cruises, personal utility bills and shopping expenses, her child's college tuition, and to fund her and her family members' personal businesses selling health and beauty products. Latoski then used her accounting position to facilitate having her former employer pay off the credit card charges, including by creating false entries in the company's books and records to conceal the expenses. (Source)

Former Bookkeeper Pleads Guilty To $2 Million+ Wire Fraud Scheme Over 7 Years - September 6, 2022
Christina Joyner worked for 25 years as a Bookkeeper for Quanz Motor Car Company, doing business as Quanz Auto Body.

From approximately July 2014 through September 2021, Joyner defrauded the company of over $2 million. Joyner was responsible for maintaining the integrity and accuracy of these accounts as well as the accounting system, and was authorized to sign company checks on behalf of Quanz. However, she was not authorized to sign checks issued to herself, apart from normal payroll.

Joyner admitted to issuing checks to herself and coded them to give the appearance they were for legitimate business expenses. Joyner then would deposit the checks electronically through a mobile banking app and immediately withdraw the funds the same day.

Joyner also admitted to using company credit cards to make personal, online purchases without the knowledge or authorization of Quanz. Joyner sometimes kept money from cash transactions for her personal use.

Joyner used her position to create fraudulent pay stubs for her husband that were used as proof of income to obtain loans. Joyner emailed reminders to herself to modify entries in the accounting software, and used her position to manipulate the software to conceal her personal use of Quanz funds. (Source)

Former Financial Manager Charged With Embezzling $1 Million+ from Employer - September 26, 2022
Mai Houa Xiong was employed as a Financial Manager for a property management company that provided financial services to homeowners' associations. Xiong's duties included bookkeeping, and as manager she had nearly unfettered access to the victim homeowner's associations' financials, bank accounts, vendor and contractor payments, and bookkeeping systems.

Between February 2015 and February 2022, Xiong devised and executed a fraud scheme to embezzle funds directly from the accounts to which she had access. These funds were HOA fees collected from residents, intended to pay for maintenance, construction, and other costs incurred by the victim associations.

Xiong repeatedly accessed the HOAs' bank accounts and conducted electronic transfers of funds directly into her personal bank accounts. Xiong disguised these transfers by mis-labeling them to make it appear as if they were legitimate HOA expenses. Xiong also used her authority as a signatory to make cash withdrawals directly from the HOAs' accounts, including making withdrawals after she was fired from her position in July 2021. After her termination, Xiong began collecting Unemployment Insurance (UI) funds. However, even after Xiong found new employment, she continued to wrongfully obtain public UI benefits. (Source)

RV Resort Manager Charged For $1 Million Fraud Scheme - September 20, 2022
Troy Bittner, in his role as Manager for Carolina Pines RV Resort, used his access to the company's credit card reservation system to commit wire fraud.

Bittner would use the electronic payment system to initiate a refund as if guests had cancelled their reservations. During the Coronavirus pandemic it was not uncommon for guests to cancel reservations. However, rather than direct the refunds to the credit cards on file, Bittner instead issued the refunds to his own various personal credit cards. Over the 26-month window of Bittner's alleged scheme, he received more than $800,000 in fraudulent refunds at the expense of Carolina Pines. (Source)

Financial Officer Sentenced To Prison For Defrauding County Non-Profit Organization Out Of $800,000+ - September 23, 2022

Evidence presented to the Court showed that while serving as the Financial Officer for Sumter Behavioral Health Services (SBHS), a 501c3 non-profit, Rodney Ellis defrauded the non-profit out of more than $800,000 over eight years. His scheme was to divert funds from SBHS banking accounts to his own personal banking accounts. (Source)

Former Accountant Sentenced To Prison For Embezzling $362,000+ From Employer / Previously Convicted For Embezzling From Another Company - September 13, 2022

Carrie Long was employed by Executive Coach Builders, Inc. to provide in-house accounting services to the company and to Executive Bus Builders, Inc. The companies are headquartered in Springfield but do business worldwide with factories and sales offices in Missouri and California. The companies build luxury buses, coaches, and limousines. Long was hired in April 2014.

Long admitted that she stole at least $362,175 from the companies from February 2016 to September 2020. Long also admitted that she failed to pay approximately $902,226 of employment taxes the companies owed to the IRS. By not making these payments, Long created a pool of funds in the companies' bank accounts from which she continued her embezzlement scheme.

Long used her position as an in-house accountant for the companies, and her access to the companies' check stock, to regularly write checks against the companies' bank accounts for unauthorized payments to herself. Long stole money from the companies by filling in unauthorized amounts on some pre-signed checks and making such checks payable to herself. Long also stole money from the companies by forging signatures on the companies' checks, filling in unauthorized amounts on the checks, and making such checks payable to herself.

Long stole from the companies at least 198 times. When the companies' owner confronted her with evidence that she had stolen from the companies and that she had not paid over the companies' employment taxes, she continued to lie to him, forcing him to hire an accounting firm to investigate.

Beginning in April 2019, Long ceased to make regular payments to the IRS for the employment taxes the companies owed the IRS. Long concealed her actions from company officials by altering the companies' bank account statements and misrepresenting on her financial reports that the payments had been made. Long caused the companies to fail to pay over to the IRS approximately $902,226 of taxes (including both the employer portion and the funds withheld from the companies' employees' paychecks) owed to the IRS for two quarters of 2019 and one quarter of 2020.

Long was convicted in state court of similar conduct with a previous employer and was still on probation for that crime at the time of this federal offense. On Oct. 21, 2013, she pleaded guilty in the Circuit Court of Laclede County, Mo., to stealing more than $88,000 from a client of her then-accounting firm employer. As in this federal case, she stole by forging checks made payable to herself and endorsed in her own name against the victim's bank account. Long received a suspended five-year sentence, was ordered to serve 90 days shock time, placed on probation for five years, and ordered to pay restitution to her victim within 30 days of her sentencing.

Long's mother actually paid her court-ordered restitution on her behalf in the state case. Long used the money she stole from the companies in this scheme to pay her mother back for the prior victims' restitution payment. (Source)

Former Director Of Finance Sentenced To Prison For Embezzling $600,000 From Credit Union / Used $$$ To Buy Stocks, Fund Retirement Account, Pay Off Car - September 19, 2022

Salusthian Lutamila is the former Director of Finance of the Inter-American Development Bank / Federal Credit Union.

From November 2016 through April 2019, Lutamila worked at the credit union, first as the Controller and then as the Acting Chief Financial Officer. Shortly after finding out that he was not being promoted to the role of Chief Financial Officer, Lutamila began embezzling money from the credit union. Specifically, beginning in November 2018 through January 2019, Lutamila stole $610,000.

Throughout the scheme, Lutamila abused and misused his position and employment at the credit union in order to illegally transfer money from internal operating accounts to a previously dormant checking account. Lutamila then abused the authority granted to him as Acting CFO to secretly move that money to an E-Trade account he had opened at the beginning of the scheme.

Lutamila then used the stolen money to pay off his car, increase the balance on his retirement account, and buy stocks. Lutamila's scheme was discovered only a few weeks before he was set to resign from the credit union when the newly hired CFO identified the fraudulent transfers. Due to the quick actions by the newly hired CFO, the credit union was able to flag the fraud and get back most of the embezzled money. (Source)

Former Mortgage Company Employee Sentenced To Prison For $500,000+ Of Wire Fraud - September 27, 2022

In 2016, Victory Mortgage hired Hachelle Alsip as a Loan Funding Representative to assist, in part, with distribution of funds with loans provided by the lending company to its borrowers.

In 2021, Alsip caused two wire transfers totaling $507,000 to be made from one of Victory Mortgage's business checking accounts, into a personal bank account belonging to her and her husband. (Source)

Former Employee Admits To Embezzling $339,000+ - September 15,, 2022

Ronald Miller was the warehouse and labor supervisor for a small floor covering business. He was responsible for supervising the company's installers, scheduling their weekly shifts and drafting their timesheets. He also had the authority to hire flooring installers.

Miller submitted false timesheets for himself, his partner and his son. His partner did not work for the company, but Miller submitted timesheets anyway, then collected the paycheck and forged his partner's signature to deposit it in his own account.

Miller falsely inflated the hours worked by his son without his son's knowledge and did the same for himself by claiming he was working on installation projects when he was not.

Miller also submitted fraudulent invoices in the name of two fake companies, claiming he had made purchases there. Miller created accounts with Square Inc. in the names of those companies so he could pay himself with company credit cards or caused the company to issue checks to pay the fake invoices.

Finally, Miller altered and inflated receipts for legitimate purchases that he made and then sought reimbursement from his company. (Source)

Former FIFA Soccer Federation President Sentenced To Prison for Accepting $350,000+ In Bribes - September 29, 2022

Reynaldo Vasquez, is the the former President of the El Salvadorean Soccer Federation.

Vasquez accepted over $350,000 in bribes that he and other soccer officials from El Salvador received from an American company in exchange for the sale of broadcast rights to the El Salvador soccer team's World Cup qualifier and friendly matches. (Source)

Former Chief Financial Officer Sentenced To Prison For Embezzling $200,000+ Over 6 Years - September 22, 2022

Angela Clifton was the Chief Financial Officer for a manufacturing company in Alabama. Clifton had authorization to use multiple corporate credit cards for legitimate business expenses, and she was also in charge of the company's payroll and 401k plan.

In 2018, the company discovered that Clifton, then the company's Controller, had made over $25,000 worth of Amazon purchases for personal using corporate credit cards. Prior to her resignation, Clifton paid some of this money back to the company.

However, after her resignation, an audit was conducted and the company discovered that Clifton was not only making personal purchases with the corporate credit cards, but also fraudulently receiving 401k matches from the company when she was not contributing to her plan, and was issuing to herself unauthorized paychecks and bonuses. In total, the company discovered that Clifton abused her role as Controller and fraudulently obtained over $200,000 in money and personal items between 2012 and 2018. (Source)

Former Employee Pleads Guilty To Role In $46,000+ Bank Fraud Scheme - September 19, 2022

Between 2018 and October 2021, Katie Ricker was employed in various positions by a company in Sugar Hill, New Hampshire.

In or about October 2021, Ricker stole blank checks belonging to the company. She wrote fraudulent checks addressed to herself, her co-defendant William Hill, and others to transfer funds from the company's account to her joint bank account with Hill.

Ricker forged the signature of the employee authorized to sign on the company's account. The defendants were caught on camera cashing some of the fraudulent checks. In total, Ricker stole $46,055.35 from the company. (Source)

SHELL COMPANIES / FAKE INVOICE BILLING SCHEMES

No Incidents To Report

THEFT OF COMPANY PROPERTY

Former Director Of Information Technology Sentenced To Prison For Embezzling $590,000+ Worth of Electronic Devices Over 8 Years - September 28, 2022

Venancio Diaz was the Newark, New Jersey Housing Authority (NHA)'s Former Director Of Information Technology.

From December 2013 to Aug. 10, 2021, Diaz bought, on behalf of NHA and using NHA funds, 1,509 electronic devices, primarily cellular telephones and tablets, from a telecommunications company. Diaz then caused those devices to be activated on NHA's account on the company's network for a short period of time, often only days or weeks. After the brief period of activation ended, Diaz posed as the owner of the devices and sold them to two different online electronics resale marketplaces. Diaz directed all the proceeds of the sales – a total of $594,425 – to his own bank accounts and kept the money for his own personal use. (Source)

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE

Information Technology Professional Pleads Guilty To Sabotaging Employer's Computer Network After Quiting 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)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

3 Airline Employees Charged For $283,000+ Reservation Skimming Fraud Scheme - September 20, 2022

The 3 employees were charged with wire fraud in connection with their scheme to defraud their employer, a national airline carrier, out of ticket fare revenue by recruiting customers to book inexpensive flights which they didn't intend to use, upgrading those customers to more expensive flights which the customers actually wanted by using supervisors' computer access codes, and then charging the customers a 'commission' and pocketing that money rather than charging the customer the full price of the upgraded flight.

In 2017 and 2018, Tiana Thompson was an employee in a supervisory role with a major U.S. airline headquartered in Florida, and Tiana Fairfax and Theodore Robinson worked as customer service agents with the same airline. In those jobs, the defendants had access to the airline's computerized reservation system and were able to book flight reservations; supervisors like Thompson had the ability to use a special code at their discretion to make changes in the reservation system without charging customers the additional costs associated with modified reservations. In general, if a passenger changed their itinerary, airline policy required that the passenger pay the full price of the modified itinerary, which was often more expensive than the itinerary that the passenger originally booked. Although supervisors had the ability to modify a reservation without assessing those charges, under Airline policy, those charges were only to be waived under extenuating circumstances, such as a death in the passenger's family.

Between December 2017 and August 2018, all three defendants along with the two co-schemers modified more than 1,700 flight reservations without compensating the airline for the increased cost of those modified reservations, for a total loss to the airline of more than $283,000. (Source)

Employees Of Engineering Firm Contributed $50,000 To A Former City Prosecutor's Re-Election Campaign So He Would Prosecute Former Employee Of Firm For A Crime She Didn't Commit - September 13, 2022

There's been another arrest in the high-profile federal case against former city Prosecutor Keith Kaneshiro.

The FBI moved in on attorney Sheri Tanaka's California home, taking her into custody in connection with the alleged conspiracy.

Tanaka represents Mitsunaga & Associates, the engineering and architectural firm caught up in the public corruption scandal. Tanaka was indicted by a federal grand jury.

Kaneshiro and Dennis Mitsunaga, along with employees of Mitsunaga's company Terri Otani, Chad McDonald, and Aaron Fujii were charged with conspiracy and bribery.

The employees contributed nearly $50,000 to Kaneshiro's re-election campaigns between 2012 and 2016. In exchange, Kaneshiro allegedly prosecuted a former employee of Mitsunaga's firm for a crime she didn't commit. The employee had sued the firm for discrimination.

Records show that Tanaka wrote three letters to Kaneshiro's office in 2013, one in January, February and then July accusing the former employee of theft. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Jail Sergeant Pleads Guilty To Role In Cocaine Distribution Conspiracy - September 26, 2022

In 2020 the Federal Bureau of Investigation began investigating a drug trafficking organization that operated throughout the greater Washington County, Pittsburg area.

Beginning in April of 2020 and continuing through October of 2020, the FBI received authorization to conduct a Title III wiretap investigation into the organization. The organization was responsible for orchestrating and directing the movement of drugs from New Jersey to the Western District of Pennsylvania for distribution throughout Washington County.

Mr. Molinaro, who was a sergeant in the intake department of the Washington County Jail during this investigation, utilized his law enforcement position to provide a member of the drug trafficking organization with law enforcement sensitive information to aid that individual in evading law enforcement detection.

Mr. Molinaro is one of 20 defendants charged in the Superseding Indictment returned in this case. (Source)

MASS LAYOFF OF EMPLOYEES INCIDENTS

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

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)

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)

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)

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

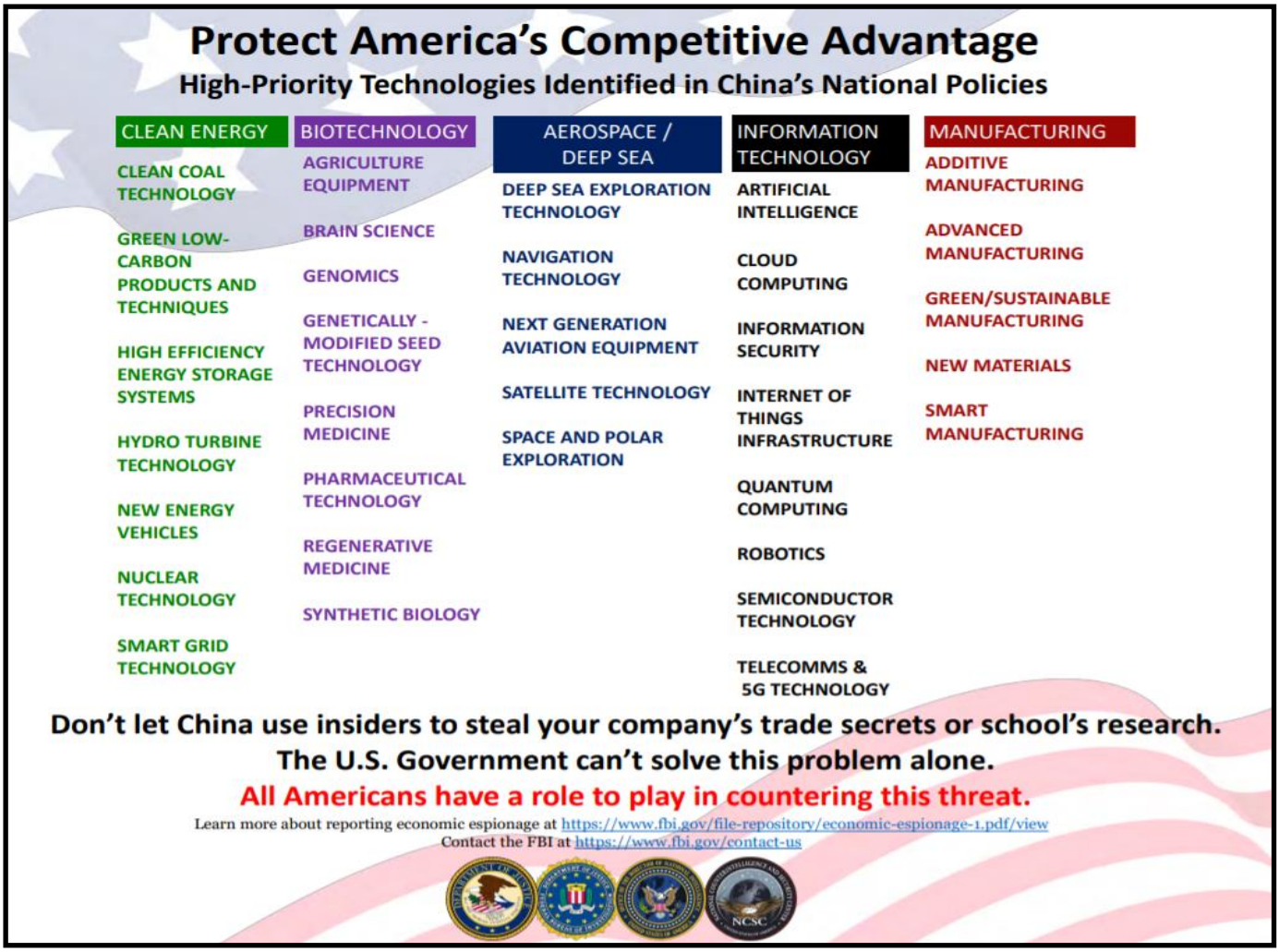
https://www.workplaceviolence911.com/node/994

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 (**4,000+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS 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

FTK ENTERPRISE

FOR NETWORK INVESTIGATIONS AND POST-BREACH ANALYSIS

When investigating insider threats, you need to make sure your investigation is quick, covert and able to be completed remotely without alerting the insider. FTK Enterprise enables access to multiple office locations and remote workers across the network, providing deep visibility into data at the endpoint. FTK Enterprise is a quadruple threat as it collects data from Macs, in-network collection, remote endpoints outside of the corporate network and from data sources in the cloud.

Find out more about FTK Enterprise in this recent review from Forensic Focus.

DOWNLOAD

If you'd like to schedule a meeting with an Exterro representative, click here:

GET A DEMO

exterro®

[Download FTK Review]
[Get A Demo]
[Exterro Insider Threat Program Checklist]