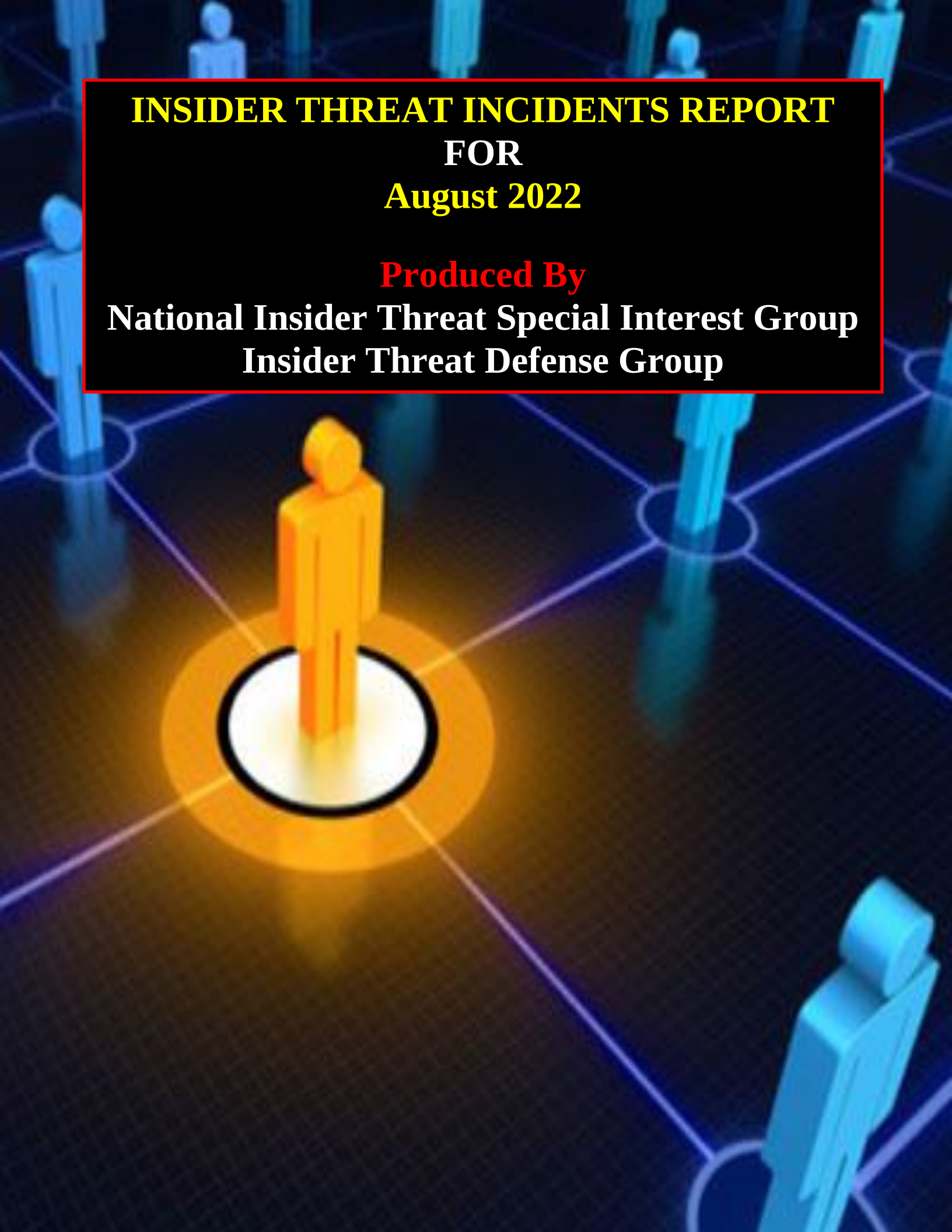

INSIDER THREAT INCIDENTS REPORT
FOR
August 2022

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 **3,900+** 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 AUGUST 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT
Former U.S. Postal Service Employee Pleads Guilty To Role Scheme To Deliver Drugs Through Mail - August 5, 2022

In 2014, Elliott Sheppard worked as a U.S Postal Service (USPS) mail carrier.

In exchange for bribes, he used his position to deliver five-pound packages of drugs through the U.S. mails to Dexter Frazier, a local drug trafficker who sold cocaine and marijuana.

In 2016, Frazier approached Sheppard about delivering additional drug packages. Sheppard was on disability leave from the USPS at that time and unable to intercept and deliver packages. So Sheppard offered to recruit other mail carriers to deliver drugs for Frazier, if Frazier paid Sheppard referral fees consisting of a mix of cash and marijuana. Frazier agreed.

Sheppard then contacted two coworkers, Tonie Harris and Clifton Lee. Sheppard explained to Harris and Lee that in exchange for payment, Frazier needed them to deliver packages of drugs. Sheppard instructed Harris and Lee how to arrange the deliveries to avoid detection. Harris and Lee agreed to participate in the scheme after which Sheppard gave their phone numbers to Frazier. Frazier then coordinated the illegal deliveries with Harris and Lee. Harris and Lee each delivered three packages for Frazier believing they contained two kilograms of cocaine or 10 pounds of marijuana. (Source)

U.S. Postal Service Mail Carrier Pleads Guilty To Theft Of Mail / Using Cocaine At Work - August 9, 2022

Between December 2020 and May 2021, Umberto Pignataro, while employed as a Mail Carrier for the U.S. Postal Service, stole hundreds of pieces of mail, including packages and greeting cards that contained cash, gift cards and other items of value. During the investigation, video surveillance captured Pignataro rifling through, destroying and pocketing pieces of mail while servicing his mail route.

When confronted by investigators in May 2021, Pignataro admitted stealing mail, and also admitted that he possessed a firearm and used cocaine at work. He was then placed on unpaid leave. (Source)

U.S. Postal Service Mail Carrier Pleads Guilty To Her Role In $462,000 Mail Fraud Conspiracy - August 9, 2022

Kanisha Black pleaded guilty to her role in a conspiracy to commit mail fraud in connection to the illegal possession of unemployment benefit debit cards issued by the Nevada Department of Employment, Training and Rehabilitation (DETR) and Arizona's Department of Economic Security (DES). These agencies administer Nevada's and Arizona's unemployment insurance program, respectively.

Black who was employed as a U.S. Postal Service Mail Carrier, assisted co-conspirator Vincent Okoye to fraudulently obtain unemployment insurance benefits from DETR and DES using other people's personal identifying information, without their consent.

Black used her position to help Okoye find either vacant residences or rarely-checked mailboxes to which fraudulently obtained debit cards could be sent. Black then intercepted and delivered those cards to Okoye in person. In total, DETR and DES approved of at least $462,000 in benefits for these fraudulent claims submitted by Black and Okoye. (Source)

Former U.S. Postal Service Mail Carrier Charged With Bank Fraud & ID Theft For Stealing $215,000 Of Jobless Benefit Debit Cards - August 21, 2022

A former United States Postal Service (USPS) Mail Carrier (Toya Hunter) was charged for her role in a scheme that allegedly defrauded banks out of more than $200,000 via the theft of debit cards containing unemployment insurance benefits from her mail route and giving them to a co-schemer in exchange for cash payments and gifts. Her co-conspirator Michalea Barksdale were previously charged in December 2021.

From December 2014 to May 2020, Hunter used her position as a Mail Carrier with the USPS to steal Bank of America debit cards mailed by the California Employment Development Department (EDD) to jobless individuals. She then allegedly provided Barksdale the stolen debit cards in exchange for future payments and gifts.

Aiding and abetting each other, Hunter and Barksdale made fraudulent and unauthorized cash withdrawals and purchases from at least 193 separate EDD cards and thereby stole from Bank of America at least $215,641 to which they were not entitled. (Source)

Department Of Labor Agent Charged With Multiple Fraud Schemes - August 17, 2022

Thomas Hartley, a Special Agent from the U.S. Department of Labor, was charged with engaging in multiple schemes to commit fraud.

The first indictment alleges that Thomas Hartley, while on leave from his position with the Department of Labor and serving with the New Jersey National Guard, submitted false documents to the Department of the Army and thereby obtained approximately $23,580 in housing allowance funds to which he was not entitled.

The second superseding indictment charges Hartley with fraud in connection with the receipt of Pennsylvania unemployment compensation benefits. The indictment alleges that Hartley fraudulently applied for and collected unemployment benefits by claiming that he was unemployed, when in fact Hartley was employed on full time active duty with the New Jersey National Guard. Hartley thereby collected approximately $60,284 in unemployment compensation funds to which he was not entitled.

Also the second superseding indictment charges Hartley with fraudulently obtaining approximately $127,000 from his Thrift Savings Plan (TSP) by falsely claiming that he was not married, when in fact he was at all times married. Hartley thereby transferred the funds to himself personally, or to a bank account solely in his name, without the knowledge or consent of his wife.

Also the second superseding indictment charges Hartley with fraud in connection with the filing of a lost wage claim with USAA Insurance following an automobile accident. Hartley falsely claimed that he had lost wages as a result of the automobile accident, when in fact Hartley was suspended without pay from his employment with the Department of Labor as a result of an ongoing criminal investigation. Hartley thereby collected approximately $50,000 in lost wage benefits to which he was not entitled. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Senior U.S. Navy Employee Convicted For Bribery (Cash, Travel, Prostitutes, Etc.) - August 24, 2022

Fernando Monroy is the former Director of Operations of the U.S. Navy's Military Sealift Command Office in Busan, South Korea.

Monroy engaged in a conspiracy to commit bribery with the owner of DK Marine, a South Korea-based company that provided services to the U.S. Navy, and a former civilian U.S. Navy cargo ship captain. Evidence at trial proved that Monroy conspired to unlawfully provide services for the Navy ship, captained by one of Monroy's co-conspirators, during a December 2013 port visit in Chinhae, South Korea.

Monroy provided a co-conspirator with confidential and other proprietary, internal U.S. Navy information. In exchange for the steering of business and the provision of such information, the co-conspirator paid bribes to Monroy, including cash, personal travel expenses, meals and alcoholic beverages, and the services of prostitutes. Monroy also repeatedly lied to special agents of the Defense Criminal Investigative Service (DCIS) and Naval Criminal Investigative Service (NCIS) during a voluntary interview in July 2019. (Source)

Air Force Explosives Expert Charged With Aggravated Assault, Reckless Endangerment Of Fellow Soldier & Wrongfully Obtaining Classified Information - August 4, 2022

An Air Force explosives expert Tech. Sgt. David D. Dezwaan Jr., has been charged in connection with a suspected insider attack that wounded four other U.S. troops at an outpost in Syria earlier this year.

Dezwaan is accused of aggravated assault, reckless endangerment and wrongfully obtaining classified information, among other crimes. he charges stem from a military investigation into the April incident at Green Village, a base the Americans share with partner forces in eastern Syria.

In first reporting the attack, U.S. military officials initially said the explosions, which occurred in areas of the base housing ammunition and shower facilities, were the result of indirect fire. They later clarified the blasts were believed to be a result of deliberate placement of explosive charges" and announced several weeks later that a U.S. service member had been detained. (Source)

CRITICAL INFRASTRUCTURE

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

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

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

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

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

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

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Police Chief Sentenced To Prison For Accepting $175,000+ In Bribes For $5.7 Million Contract Award - August 5, 2022

Tim Vasquez is the former San Angelo, Texas Chief of Police.

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

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

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

Special Deputy United States Marshal Facing Charges For $1.9 Million Money Laundering Related To Romance Scams Involving 20+ Victims - August 11, 2022

Isidore Iwuagwu is a Special Deputy United States Marshal and Department of Justice contractor providing security for critical Department of Justice facilities.

Between October 2015 and July 2021, Iwuagwu participated in a romance scam in which individuals contacted victims on social media platforms and dating sites, engaged in online relationships with the victims, then convinced victims to send large sums of money claiming the funds were needed for purported personal hardships or shipping costs for various imports.

Many victims reported sending funds at the request of individuals claiming to be deployed members of the U.S. Armed Forces who asked for money for various personal hardships. The alleged scam involved more than 20 victims, many of whom are senior citizens. The victims linked to Iwuagwu reported losing a combined $1.9 million to the scheme. (Source)

TSA Labor Union President Sentenced To Prison In Fraud Scheme To Misappropriate Union Funds - August 16, 2022

Marie LeClair was the president of the American Federation of Government Employees, Local 2617, which was based in Boston and represented TSA employees.

Beginning in or about March 2015, LeClair engaged in a scheme to defraud the union by misappropriating funds belonging to the union for her personal use. LeClair transferred funds from union accounts to a travel debit card issued in her own name without the knowledge or authorization of the union and used the misappropriated union funds for personal expenses. On May 22, 2018, LeClair made a wire transfer of $3,000 from a union account to her personal travel debit card. (Source)

STATE / CITY GOVERNMENTS

Former Employee Of Housing Authority Pleads Guilty To Embezzling $30,000+ Of Federal Program Funds - August 4, 2022

Lisa Cooper was employed by, and an agent of, the Cottonport Housing Authority (CHA), which is a local government agency that provides subsidized housing to low income individuals.

In 2019, a routine financial audit was conducted, and it revealed some accounting discrepancies at the CHA, specifically, that from 2017 through 2019, tenant payments were being diverted from the CHA. Further investigation revealed that Cooper had been embezzling funds from the CHA.

While acting as an agent of the CHA, Cooper had been collecting rental payments on behalf of the agency from the CHA's tenants in the form of money orders, with the payee and payor sections of the money orders left blank. Cooper would then enter her name as the payee and deposit the money orders into her personal bank accounts. The investigation revealed that approximately $30,079.05 in money orders was deposited into her personal bank accounts from 2017 through 2019. (Source)

2 Former St. Louis County Officials Accused Of Stealing $660,000 / Used Funds For Personal Expenses (Rent, Restaurants, IRS Taxes Owed) & Gambling - August 17, 2022

Maureen Woodson was the former City Clerk, and Donna Thompson was the former Assistant City Clerk.

The pair wrote about 614 city checks to themselves totaling more than $531,000 without the authority or knowledge of its mayor, treasurer or board of aldermen. About 368 checks worth $376,026 were written to Woodson and 246 checks worth $155,329 were written to Thompson. The signature of the mayor and / or the treasurer, which were needed to authorize payment were forged by the women.

The pair used the money to pay personal expenses and for gambling both online and at area casinos.

In the second scheme Woodson and Thompson used $132,249 in city funds to directly pay personal expenses including retail vendor charges, entertainment, restaurant bills, rent for their home and taxes they owed to the Internal Revenue Service. The women either used Flordell Hills bank checks to pay the bills or used wire transfers of city money. (Source)

Former Motor Vehicle Administration Employee Sentenced To Prison For Role In Scheme To Provide Fraudulent Driver's Licenses To Applicants Who Paid A Fee - August 18, 2022

From at least July 2015 through March 2016, Marion Payne and another co-conspirator were both employees of the Maryland Motor Vehicle Administration (MVA) and worked in the Largo, Maryland branch office. Payne's duties at the MVA included the issuance of Maryland driver's licenses.

The MVA co-conspirator conspired with Warner Portillo to produce and transfer Maryland driver's licenses without lawful authority. Specifically, Portillo and others met with prospective Maryland driver's license applicants who were willing to pay money to obtain a driver's license illegally, typically because the applicants were aliens without legal status in the United States, or were otherwise unable to obtain a lawfully issued driver's license. The applicants paid Portillo and others between $800 and $5,000 in cash for each fraudulently issued Maryland driver's license.

The conspiracy resulted in the unlawful production and transfer of at least 276 Maryland driver's licenses. In exchange for the improperly issued driver's licenses, Portillo paid Payne at least $25,000 in cash and gifts. (Source)

Former State Of Georgia Employee Charged For Role In Creating Fake Students With Non-Existent Disabilities To Steal $1.3 Million+ - August 25, 2022

Former Georgia Vocational Rehabilitation Agency Counselor Karen Lyke has been charged with forging educational records and creating fake students with non-existent disabilities and illnesses in an elaborate, multi-year scheme to steal more than $1.3 million.

From approximately May 2016 to November 2020, Lyke and a family Member allegedly conspired to steal money from the Georgia Vocational Rehabilitation Agency (GVRA) by claiming educational expenses for approximately 13 fake students.

Lyke and the family member allegedly used the names of friends and relatives to create fake medical records to make it appear that the approximately 13 fake students qualified for tuition assistance from the GVRA. Lyke and the Family Member claimed that these fake students suffered from disabilities or illnesses like AIDS, cancer, psychosocial impairments, or muscular dystrophy.

As proof of identification, Lyke and the family member provided the GVRA with manufactured images of fake driver's licenses that listed the names of their friends and relatives. In one instance, the Family Member created a fake driver's license in his cousin's name, by using a mug shot image of an unknown individual from the Internet as the driver's license photograph.

Based on false documentation, Lyke caused more than 230 checks to be mailed to approximately 13 friends and relatives for claimed educational expenses. In fact, none of the 13 fake students attended any colleges or universities. (Source)

Former State Employee Pleads Guilty For Role In $825,000+ Unemployment Insurance Fraud Case Involving Co-Conspirators - August 25, 2022

Former New York State Department of Labor (NYSDOL) employee Wendell Giles pled guilty to mail fraud and aggravated identity theft charges.

Giles admitted that he and another former NYSDOL employee, Carl DiVeglia, abused their state computer systems access to create and approve false unemployment insurance (UI) applications in 2020 and 2021, including applications for the federal Pandemic Unemployment Assistance (PUA) program.

Giles recruited relatives, friends and friends-of-friends to submit false benefits applications over the phone to DiVeglia after Giles had instructed them to lie in response to eligibility questions.

Giles and DiVeglia then took a share of the benefits paid by NYSDOL on the false claims. Giles used his share to enrich himself, including by purchasing a three-wheeled motorcycle.

Giles admitted responsibility for $826,530 in losses to pandemic-related UI benefits programs administered by the state. He has agreed to pay full restitution to NYSDOL. DiVeglia previously pled guilty to related charges and also agreed to pay restitution. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

City School Administrator Sentenced To Prison For Role In $10 Million Virtual Education Fraud Scheme Involving Co-Conspirators - August 3, 2022

A Montgomery, Alabama Athens City Schools administrator, William Carter, was sentenced to prison for his role in a scheme to defraud the Alabama State Department of Education (ALSDE).

Carter conspired with other school officials to fraudulently enroll students in public virtual schools and then falsely reported those students to the ALSDE in order to illegally receive additional education funding. Carter's co-conspirators include former superintendent of the Athens City Schools district Dr. William Holladay, David Tutt, Gregory Corkren, and former superintendent of the Limestone County School district Thomas Michael Sisk.

The submission of this false documentation allowed payments to continue from Alabama's Education Trust Fund to the Athens City Schools district and the Limestone County Schools district. Carter and his co-conspirators then received, for their own personal use, portions of the state funding. They skimmed the state money through direct cash payments and payments to third-party contractors owned by the various co-conspirators. During the course of the scheme, the total potential loss was approximately $10 million. (Source)

Former College Vice Chancellor Sentenced To Prison For $350,000 Of Procurement Fraud / Kickbacks - August 4, 2022

Sharod Gordon was employed by City Colleges of Chicago in a variety of leadership roles, most recently as the Vice Chancellor of Legislative and Community Affairs.

From 2013 to 2017, Gordon obtained kickbacks from vendor companies in exchange for steering them City Colleges contracts for community canvassing and flyer distribution services.

Some of the companies were formed by Gordon's City Colleges colleagues and other friends for the sole purpose of applying for the contracts. In some instances, the work was never performed, even though the companies submitted invoices that caused City Colleges to pay out nearly $350,000. Upon receipt of the payments, Gordon directed representatives of the companies to give him a portion of the money. (Source)

Former Catholic School Principal Pleads Guilty To Embezzling $175,000 From Fund For Student Activities And Services / Used Funds To Qualify For Home Mortgage Loan - August 3, 2022

Bridget Coates was the principal of St. Thomas More Catholic School in Southeast Washington at the time her criminal activity began, in 2012, until she resigned in 2018.

From June 2012 through December 2017, Coates devised a scheme to steal from the school's Home School Association, an organization affiliated with the school that supported student services and activities.

As the school principal, Coates had access to the Home School Association's checks and could use her discretion to pay expenditures for only school-related purposes. Coates, however, engaged in a pattern of purchasing personal goods and services with the funds. Over the time period, she wrote approximately 66 unauthorized checks and deposited at least $175,000 into her personal bank account. Among other things, she used the funds to help her qualify for a home-mortgage loan. (Source)

Former Assistant Vice President Of Finance For College Pleads Guilty To Stealing $66,000+ Using Fake Shell Company Scheme - August 1, 2022

Renee Crawford was employed as the Assistant Vice President of Finance for the College. In her role, Crawford had authority to manage invoice approvals, enter vendor information, and had oversight of the Finance Office's credit card program.

Crawford used her access to submit fraudulent invoices for a company that she created, receiving more than $44,000 from the College which she used for personal purchases. In addition, Crawford used two College issued credit cards to make personal purchases, such as family vacations and theme park tickets, totaling nearly $22,000. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee Sentenced To Prison For $38,000+ Of Embezzlement - August 11, 2022

Angelica Gebur was employed as the Lead Customer Service Representative for CorTrust Bank branch located in Webster, South Dakota.

The conviction stemmed from incidents beginning on or about March 22, 2018, and continuing through June 18, 2021, when Gebur was an employee of the bank. .

Needs Anonymous Thrift Store is a volunteer-run thrift store ministry located in Webster, and they banked with CorTrust Bank. The thrift store usually dropped off its weekly deposit bag at the bank's drive-up window. The bag typically contained mostly cash. The bag did not include a completed deposit form, but rather a handwritten note of the total deposit amount.

Gebur often received the deposits from the thrift store that were meant to be deposited into the thrift store's accounts at the bank. On multiple occasions, Gebur stole some of the cash from the thrift store's intended deposits, kept it for herself, and used it for her own purposes.

Gebur was ordered to pay restitution to the Needs Anonymous Thrift Store in the amount of $38,986. (Source)

Former Bank Assistant Manager Sentenced To Prison For Stealing $284,000 - August 16, 2022
Capri Duvall was rhe former Assistant Manager of a bank in Wellston, Missouri.

Duvall pretended to be filling the ATM with cash on July 19, 2021, but hid $284,000 in a brown box and carried it out to her car. After work, Duvall met with teller Chloe Anderson and security guard Mariah Barnes and split up the money. Anderson and Barnes each got $30,000. (Source)

Former Bank Branch Manager Sentenced To Prison For Embezzling $184,000 - August 25, 2022
Dorinda Lumpkin was employed as a Branch Manager at a BBVA Bank in Gadsden, Ala.

Between January 2017 and June 2020, Lumpkin stole at least $184,250.00 from BBVA accounts associated with a deceased customer and her daughter. To do so, she prepared and approved debit tickets authorizing the transactions, which were purportedly signed by the deceased customer's daughter. The defendant then withdrew the funds from those accounts and converted them to her own use. (Source)

TRADE UNIONS

No Incidents To Report

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Twitter Employee Found Guilty Of Acting As An Agent Of A Foreign Government & Unlawfully Sharing Twitter User Information / Taking Bribes - August 10, 2022
Ahmad Abouammo was employed at Twitter as Media Partnerships Manager for the Middle East / North Africa region.

The evidence at trial demonstrated that Abouammo took bribes in exchange for accessing, monitoring, and conveying the private information of Twitter users to officials of the Kingdom of Saudi Arabia and the Saudi Royal family.

Abouammo began receiving bribes from an official of the Kingdom of Saudi Arabia as early as December 2014. The foreign official met with Abouammo in London and provided Abouammo with a luxury Hublot watch. Abouammo later acknowledged the value of the watch was $42,000 when he offered it for sale on Craigslist.

After the meeting in London, Abouammo began repeatedly accessing private information about several Twitter accounts, at least one of which was an influential account who was critical of members of the Saudi Royal Family and the government of the Kingdom of Saudi Arabia. Abouammo also continued to communicate with the official of the Kingdom of Saudi Arabia, including regarding the influential critical account.

Evidence at trial further showed that after Abouammo traveled to Lebanon in February 2015. A bank account was opened in the name of his father in Lebanon and Abouammo obtained access to that bank account. The account then received $100,000 from the official of the Kingdom of Saudi Arabia and Abouammo laundered the money by sending it into the United States in small wire transfers with false descriptions. Abouammo left his job at Twitter in May 2021 and, shortly thereafter, received another $100,000 into the bank account in Lebanon accompanied by a note from the official apologizing for the delayed payment. Abouammo responded, in part, by asking whether the official wanted any additional information from Twitter. (Source)

Automotive Car Dealership Salesman Is Accused Of Stealing Personal / Financial Tnformation From A Customer To Buy 2 Vehicles - August 24, 2022

Etni Carrizales was arrested on for fraudulent use or possession of identifying information, theft between $30,000 and $150,000, and false statement to obtain property or credit.

A customer went to a car dealership where Carrizales worked as a salesman, and filled out the required paperwork as an interested buyer. The man left and chose to not purchase a vehicle, but he noticed that his credit was being run several times through different banks and financial companies.

The customer told police that Carrizales messaged him weeks later and asked for a copy of his driver's license "for their records". He later realized that Carrizales circumvented the credit bureaus, unblocked his credit, and purchased vehicles using the stolen identity.

Carrizales bought a 2019 Chevrolet Traverse from a local dealership for $36,018 using a fake driver's license that contained the victim's information. The vehicle was delivered to Carrizales' apartment complex. He also bought a vehicle in using the victim's name, but he provided his real name for the insurance.

Carrizales was fired from the car dealership in January following a separate incident where he stole checks and deposited them. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE & STAFF

Former Pharmacy Vice President & Executive Assistant Sentenced To Prison For Their Roles In $88 Million Health Care Fraud Scheme Targeting U.S. Military - August 19, 2022

A former South Florida pharmacy executive (Matthew Smith) was sentenced today to seven and a half years in prison for defrauding Tricare and CHAMPVA of approximately $88 million through a compounding pharmacy fraud scheme. His executive assistant (Alisa Catoggio) received a sentence of five years imprisonment for her role in the conspiracy.

Smith admitted his role in submitting fraudulent claims to Tricare and CHAMPVA for expensive, medically unnecessary compound drugs through a pharmacy. Tricare and CHAMPVA are the health care benefit programs for the United States Department of Defense and Department of Veterans Affairs.

Smith paid kickbacks to patient recruiters in exchange for their recruiting beneficiaries and referring prescriptions for the medical unnecessary drugs. Catoggio calculated and tracked the kickbacks and sham co-pay assistance programs used to further the scheme. The fraudulent referrals caused an actual loss to the government programs of approximately $88 million. (Source)

Pharmaceutical Sales Representative Sentenced To Prison For Role In Defrauding University Of $1.2 Million For Unnecessary Drug Prescriptions - August 15, 2022

Daniel Brown's conviction stemmed from an agreement to have expensive and medically unnecessary compounded pain creams and patches prescribed to Michigan State University (MSU) employees that were filled by pharmacies in Mississippi.

Brown admitted soliciting a local physician to sign the prescriptions and splitting commission payments that the Mississippi pharmacies paid Brown for directing the prescription to their pharmacies. The pharmacies then charged MSU's health plan $2,000 - $3,000 for each prescription. Brown was ordered to pay restitution totaling $1,267,418.00.

Brown subsequently cooperated in the investigation and prosecution of the persons operating the pharmacies who were held criminally responsible in related federal cases in Mississippi for more than $200,000,000 in total claims paid for medically unnecessary compounded medications resulting from illegal kickbacks paid to sales representative and physicians around the country. (Source)

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

Former Owner Of T-Mobile Retail Store Found Guilty Of Committing $25 Million Scheme To Illegally Unlock Cell Phones Over 5 Years - August 1, 2022

Argishti Khudaverdyan, a former owner of a T-Mobile retail store, has been found guilty for his $25-million scheme to enrich himself by stealing T-Mobile employee credentials and illegally accessing the company's internal computer systems to illicitly unlock and unblock cell phones.

To gain unauthorized access to T-Mobile's protected internal computers, Khudaverdyan obtained T-Mobile employees' credentials through various dishonest means, including sending phishing emails that appeared to be legitimate T-Mobile correspondence, and socially engineering the T-Mobile IT Help Desk. Khudaverdyan used the fraudulent emails to trick T-Mobile employees to log in with their employee credentials so he could harvest the employees' information and fraudulently unlock the phones.

From August 2014 to June 2019, Khudaverdyan fraudulently unlocked and unblocked cellphones on T-Mobile's network, as well as the networks of Sprint, AT&T and other carriers. Removing the unlock allowed the phones to be sold on the black market and enabled T-Mobile customers to stop using T-Mobile's services and thereby deprive T-Mobile of revenue generated from customers' service contracts and equipment installment plans.

Khudaverdyan advertised his fraudulent unlocking services through brokers, email solicitations, and websites such as unlocks247.com. He falsely claimed the fraudulent unlocks that he provided were "official" T-Mobile unlocks. (Source)

Former Accountant Pleads Guilty To Role In Embezzling $6.8 Million / Money Laundering Over 14 Years To Purchase Collectible Cars & Real Estate - August 26, 2022

From October 2005 to January 2019, Jonathan Weston, a former Accountant for Hillandale Farms Co. located in Greensburg, Pennsylvania, engaged in a scheme with his personal secretary and company bookkeeper known as VP, to embezzle approximately $6.8 million dollars from Hillandale Farms, and then launder the stolen money businesses they both controlled, to purchase collectible cars and real estate and pay for personal expenditures.

Both Weston and VP laundered millions of stolen funds for themselves. Weston purchased, personally or through a Cougar Holdings, a company he owned, a 2013 Honda Pilot SUV, 2003 Lexus SC convertible, a 2010 Lexus LX5 SUV, a 2008 Aston Martin Vantage convertible, a 2013 Lexus GX6 SUV, a condominium in Gateway Towers in downtown Pittsburgh, in addition to hundreds of thousands of dollars used for the operation of several car washes and Katie's Kandy stores, which he owned.

VP used the stolen funds to purchase a custom 1933 Ford Model 40 coupe, a 2013 Morgan 3-wheeler, a 2010 Bennington pontoon boat and a 2014 Yamaha wave runner with trailers, and thousands of dollars in credit card expenses. In 2019, VP died.
(Source)

Former Accounting Manager Charged With Embezzling $4 Million From Company & Clients / Used Funds To Pay For Her Wedding, Anniversary Party, Cosmetic Surgery, Tuition - August 18, 2022

Millie Miranda was an account manager at a small business management firm that primarily serviced clients in the entertainment industry.

From at least in or about December 2014, up to and including at least January 2022, while serving as an Account Manager for the company, MIRANDA embezzled funds from the company and some of the company's clients.

She added herself as an authorized user on two credit cards belonging to a Client, used two other credit cards issued to a client's employees, and wrote checks and sent electronic funds transfers out of the clients' accounts. Miranda used the credit cards, the checks, and electronic funds transfers to make payments to a cosmetic surgeon, her children, and others, and to pay for expenses such as tuition, travel, her wedding, an anniversary party, and luxury items from Jimmy Choo. To conceal the Client funds that she had stolen and spent, Miranda transferred funds between accounts belonging to different clients. (Source)

Chief Financial Officer Admits To Embezzling $1.5 Million+ To Pay Credit Cards & Home Equity Line Of Credit - August 30, 2022

Carolina Guerreno served as the Chief Financial Officer of a financial services company. As part of her job responsibilities, she had access to her employer's bank accounts and was allowed to initiate financial transactions, including wiring company funds to other bank accounts.

From January 2019 and continuing until her fraud was detected by the company in February 2021, Guerreno stole $1,532,207.24 by altering company financial transactions and directing electronic payments from her employer's bank account to her credit card accounts, her personal bank accounts, and to pay her home equity line of credit. (Source)

Former Home Owners Association (HOA) Manager Sentenced To Prison For Stealing $1.4 Million From HOA's & Employer For Gambling Addiction- August 24, 2022

Between January 2018 and August 2021, Aimee Statham embezzled from her employer, Rouland Management Services (RMS), and the homeowners' associations that RMS managed.

Statham issued hundreds of unauthorized checks made payable to herself from the bank accounts of various HOAs, and she made unauthorized interbank electronic money transfers of funds between HOA bank accounts and RMS' bank account, which she would then transfer to herself. To perpetuate and conceal her scheme, Statham altered the HOAs' monthly bank statements by removing the unauthorized transactions. Statham used the stolen funds to feed her gambling addiction. The total loss exceeded $1.4 million. (Source)

Former Accountant For Construction Company Charged With Embezzling $1.5 Million+ In Company Funds - August 12, 2022

Richard Mandarino was a former Senior Accountant for a Chicago construction company.

Mandarino entered false payment requests in the construction company's accounting system, causing checks to be issued to vendor companies for goods and services that Mandarino knew were never provided. Mandarino then converted those payments to his and others' personal use. Mandarino allegedly concealed the thefts by creating fictitious credits and offsets in the construction company's accounting system.

Mandarino committed the alleged fraud from 2015 to 2017 while he resided in Canada and worked on the construction company's Canadian business projects. The charges allege that Mandarino fraudulently embezzled and obtained more than $2 Million Canadian Dollars / $1.5 Million+ U.S. Dollars. (Source)

Company To Pay $1 Million In Forfeiture Related To Federal Embezzlement & Bribery By 2 Former Executives - August 11, 2022

A Springfield company (Pro1) will pay more than $1 million in forfeiture to the federal government under the terms of a non-prosecution agreement, which acknowledges the criminal conduct of two former executives who are involved in a related criminal investigation.

Pro1 IAQ, Inc., a Missouri corporation with operations in Springfield and Boulder, Colorado, designs and sells indoor thermostats nationwide.

The company owners and executives abused their leadership positions in an unrelated charity to illegally enrich themselves and their for-profit company. More than $1 million from the health care charity, primarily funded by Medicaid reimbursements, was siphoned to Pro1 through a series of illicit payments over several years. Pro1 has accepted responsibility for the criminal conduct of its former executives and cooperated with the federal investigation.

The investigation uncovered a scheme spanning several years to siphon money from a community-based health center to a for-profit company. (Source)

Former Bookkeeper Sentenced To Prison For Stealing $650,000+ From 2 Employers To Pay For Living Expenses, Shopping, Jewelry, Credit Bills - August 19, 2022

Suzanne Brooks was a Bookkeeper from 2013 to 2018 for 2 individuals who owned real estate companies in Georgia. Brooks had access to paper checks and online banking logon credentials for their businesses at multiple FDIC-insured institutions.

Brooks used business bank accounts to make multiple payments towards personal credit card balances for her and her husband with various credit card companies, without authorization from the victims.

Brooks used the money to pay for her living expenses, including utilities for her home, insurance payments, restaurants, first-class travel, online shopping, retail purchases, fine jewelry and to purchase inventory for her side business selling clothing with a multi-level marketing company.

When her personal credit cards developed balances, Brooks repeatedly used the victims' funds to pay off those balances at her discretion and without their authorization. Brooks concealed her theft by falsifying Profit & Loss statements and other files in the accounting software used by the businesses, resulting in both victims believing their businesses to be less profitable than they actually were. Brooks also altered bank statement records and wrote dozens of unauthorized checks to herself. In total, Brooks caused at least $659,106.38 of intended losses to the victims. (Source)

Former Director Of Finance Sentenced To Prison For Embezzling $650,000 For 10+ Years - August 4, 2022

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

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

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

Former Office Manager / Bookkeeper Sentenced To Prison For Embezzling $291,000+ - August 5, 2022

Alicia Henderson was the Office Manager and Bookkeeper for a non-profit corporation that provided services for the San Antonio Downtown Public Improvement District. Her responsibilities included oversight of the accounting and financial reporting functions for the non-profit corporation.

Between July 2014 and November 2017, Henderson forged or wrote to herself 118 checks drawn on the non-profit's bank account and deposited the funds into her personal bank account. Henderson used the stolen money, totaling $291,385.23, for her own personal benefit. (Source)

Office Manager Sentenced To Prison For Embezzling $260,000+ From Employer - August 30, 2022

Kimberly Jones was employed as an Office Manager at Guardian Retention Systems, LLC in Bullitt County, Kentucky.

As office manager, she handled accounts payable and receivable, petty cash, payroll, and taxes. She also had electronic access to the bank accounts to pay bills.

During her time as Officer Manger, Jones took several actions to embezzle from her employer. She used company credit cards in her name and the names of other employees to make unauthorized personal purchases. She directed unauthorized transfers from the company bank account and diverted customer revenue received by the company's electronic payment account. Jones also set up a business called KAB Enterprises, LLC to issue false invoices to Guardian Retention Systems. Jones would use the company credit cards and bank account to pay the fraudulent invoices from KAB Enterprises, LLC.

Jones was ordered her to pay $260,034 in restitution. (Source)

SHELL COMPANIES / FAKE INVOICE BILLING SCHEMES

Former Employee Sentenced To Prison For Using His Accounting Position To Embezzle $87,000+ His Employer Using Fake Invoice Scheme To Buy A Car & 5 Motorcycles - August 15, 2022

Patrick Garrett was employed as a Sales Specialist for a business located in Gibson County, Indiana. Garrett was responsible for handling accounts payable and accounts receivable.

From April 9, 2021, to July 16, 2021, Garrett devised and executed a direct bill and fake invoice scheme to steal $87,192.26 from his employer.

Garrett purchased approximately 62 items for himself from Amazon and other retailers by charging the purchases to his employer without authorization. Garrett's fraudulent purchases included a car, five gas motorcycles, three electric scooters, an Apple iPad Pro, an Apple iMac Pro desktop computer, an Apple MacBook Pro laptop computer, and two drones. Garrett entered false or altered information about these purchases into his employer's accounting system to conceal the fraud.

Garrett also submitted false invoices into his employer's accounting system for services he claimed were provided by Garrett Ventures. Garrett created the company in 2018 and served as its Chief Financial Officer. No services were ever provided by Garrett Ventures to Garrett's employer. (Source)

THEFT OF COMPANY PROPERTY

Former Maui Jim / Sunglass Manufacture Employee Charged With $100,000+ Of Mail / Wire Fraud - August 19, 2022

Maui Jim is a sunglass manufacturer and maintains its world headquarters in Peoria.

Erica Hornof had access to Maui Jim's computer systems, inventory parts, and mailroom.

Hornof stole sunglass parts 2021 until summer 2022, and used the parts to assemble sunglasses. After assembling the sunglasses, Hornof shipped the sunglasses to two individuals who sold them on the internet. The individuals then paid Hornof through a PayPal account. The indictment also alleges that Hornof defrauded Maui Jim of over $100,000. (Source)

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE

Former CEO Charged For Fraudulently Entering Competitor Laboratory And Destroying / Stealing Equipment - August 11, 2022

Eric Leykin was the CEO of a clinical reference laboratory based in New Jersey.

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

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

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

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Former Nurse Working At Health Clinic Sentenced To Prison For Removing Morphine From Vials And Injecting Herself Due To Opioid Addiction - August 1, 2022

Between August 2019 and April 2020, Esther Tuller was a Washington licensed registered nurse employed at the Confluence Health Clinic in Moses Lake, in Spokane, Washington. Her position as a nurse provided her with access to medications, including opioid narcotics such as morphine, an opioid derivative commonly prescribed by hospitals and health care facilities to relieve pain.

While working at Confluence Health, Tuller used syringes to remove morphine from at least 17 vials, and then ingested that morphine as part of her own opioid addiction. She then replaced the morphine with a saline solution that was essentially salt dissolved in water, and attempted to glue the caps back onto the vials to make them appear intact.

Before Tuller was apprehended by law enforcement, at least one Confluence Health patient who was prescribed morphine had to be rushed to the emergency room; that patient continued to be in excruciating pain after receiving only saline from what was supposed to be morphine vials. In sentencing Ms. Tuller, Chief Judge Bastian noted that Tuller's conduct did not simply involve stealing medications, but putting patients at risk. (Source)

Registered Nurse Working In Critical Care Unit In Hospital Pleads Guilty To Removing Vials From Medication Dispensing Machines - August 30, 2022

Mary Cheatham was registered nurse who previously was employed in the critical care unit at a hospital in Detroit, Michigan.

She removed vials and syringes of injectable hydromorphone from the medication dispensing machines, by extracting the hydromorphone using syringes, and then replaced the saline filled vials and syringes into the unit's medication dispensing machines. Cheatham's tampering took place between March 2020 and August 2020. Cheatham knew the vials and syringes of hydromorphone were intended to be administered to patients for the purpose of pain relief in the critical care unit of the hospital. (Source)

MASS LAYOFF OF EMPLOYEES INCIDENTS

No Incidents To Report

WORKPLACE VIOLENCE

Terminated Bank Employee Arrested For Making Threats Of Injury & Death To Employees - August 24, 2022

From April 2020 to November 2021, George Shind engaged in a pattern of harassment directed towards at least four employee, by employing means of electronic communications, including text messages and computing services platforms, to threaten grievous bodily injury and death.

Shind began a campaign of cyberstalking multiple victims after his termination from a bank where he and the victims were employed. Shind sent messages stating his intention to kill the victims and their families and referred to himself as a "predator." (Source)

Hospital Marketing Director Arrested After 39 Guns, Ammo Found In Unlocked Office Closet - August 9, 2022

Reuven Alonalayoff was the Marketing Director for Hudson Regional Hospital, In New Jersey.

He was arrested after police found a large cache of firearms and ammunition inside an office closet at the the medical facility,.

Secaucus police officers arrested Alonalayoff at Newark Liberty International Airport over the weekend, with help from the U.S. Department of Homeland Security Investigations, according to police. His arrest came several weeks after local law enforcement in Secaucus initially discovered the weapons at Hudson Regional Hospital.

Police were dispatched to the medical center on the afternoon of July 18 in response to a reported bomb threat. Officers searched the hospital using trained bomb dogs and ultimately discovering the cache of weapons inside an unlocked closet within an office.

Police said they recovered 11 handguns, 27 rifles or shotguns, and a .45 caliber semi-automatic rifle with a high-capacity magazine, which is an assault rifle, inside the closet. Officers also found another high-capacity handgun magazine with 14 rounds. (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

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 To Pay $7 BILLION+ In Damages For Employee Who Murdered Customer Because Of Systemic Spectrums Failures In The Pre-employee Screening, Hiring & Supervision Practices - July 29, 2022

The Spectrum cable company has been ordered to pay over $7 billion in damages to the family of 83 -year old Texas grandmother (Betty Thomas) who was brutally stabbed to death in her home by a Spectrum employee in 2019.

Roy James Holden, an installer for Spectrum, owned by Charter Communications, had performed work at Thomas' home in Irving in December 2019, police said at the time.

Holden returned the next day in uniform and using the company's van while he was off, posing as if he was on the job, and killed her, then used her cards for a shopping spree after her murder.

The jury previosly found Charter Communications negligent and grossly negligent in Thomas' death.

The jury awarded a verdict of $375 million in compensatory damages and said the company was responsible for paying 90% of it after the trial revealed "systemic failures" in the company's pre-employee screening, hiring and supervision practices.

Recently the verdict for punitive damages was announced, bringing the total to $7.37 billion. (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 (**3,900+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

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]