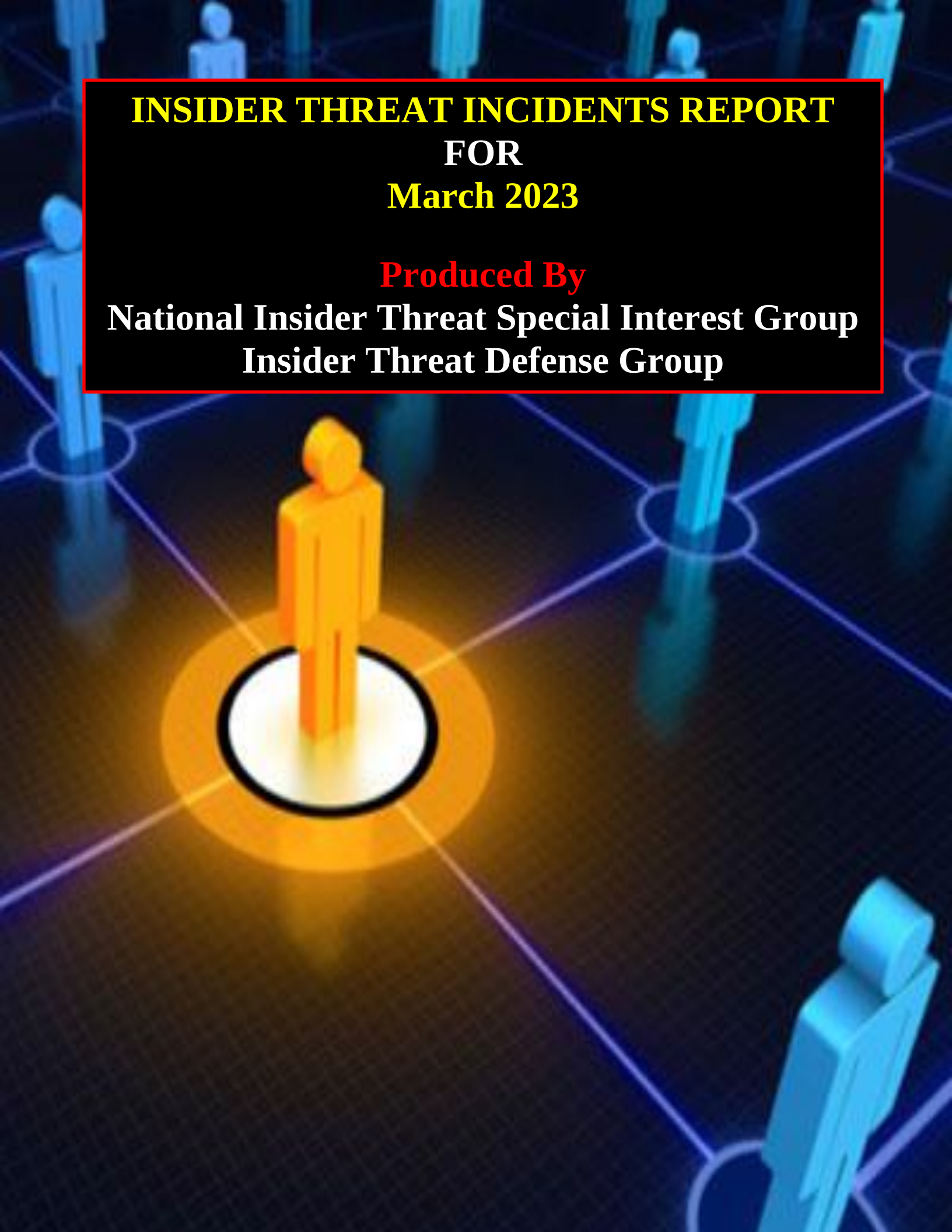

INSIDER THREAT INCIDENTS REPORT
FOR
March 2023

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **4,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

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

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

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

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

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

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 27 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

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

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

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees'

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR MARCH 2023

FOREIGN GOVERNMENT / COUNTIRES INSIDER THREAT INCIDENTS

INDIA

Former General Manager Accused Of Stealing Confidential Data To Start Rival Business - March 10, 2022

A company engaged in providing holistic care to children with special needs has accused one of its former executives of stealing confidential data and using the same to start a similar business with a rival firm.

In its complaint, the company officials alleged that they hired Pankaj Kumar as deputy general manager (DGM) in April 2019. By the virtue of his job profile, the accused was privy to confidential data and strategies of the company.

In June 2022, Pankaj resigned from the company and joined another firm as Senior Vice President and started a new vertical for providing holistic care to children with special needs.

The audit revealed that Pankaj, during his tenure in the company and even during his notice period, had transferred files and data from official email to his personal email in breach of a confidential agreement between the two parties. (Source)

MEXICO

Former Mexican Governor Sentenced To Prison For $3.5 Million Bribery / Money Laundering Scheme To Purchase Properties In U.S. - March 15, 2023

The former governor of Tamaulipas, Mexico, has been sentenced to nine years in prison for accepting over $3.5 Million in illegal bribe money.

Tomas Yarrington used the bribery money he received while governor to purchase properties in the United States. He had prestanombres - nominee buyers -purchase property in the United States to hide Yarrington's ownership of the properties and the illegal bribery money used to purchase them. Yarrington laundered his illegally obtained bribe money in the United States by purchasing beachfront condominiums, large estates, commercial developments, airplanes and luxury vehicles. (Source)

U.S. GOVERNMENT

GSA Construction Control Representative Official Sentenced To Prison For Accepting $400,000+ In Bribes - March 2, 2023

Charles Jones was employed as a Supervisory Construction Control Representative with the GSA in Richmond. He had responsibility for the management and oversight of construction and renovation projects at certain federal buildings throughout the Norfolk, Richmond, and Alexandria areas.

Beginning in approximately December of 2015 and continuing through August 2019, Jones received bribes totaling $411,192 from Daniel Crowe, in exchange for awarding them federal construction projects to his companies. In October of 2019, Jones received a cash payment from Jennifer Strickland, the President of SDC Contracting LLC, in exchange for awarding a contract valued at approximately $1,369,501. (Source)

Former Social Security Administration Employee Pleads Guilty To $320,000 Fraud And Money Laundering Scheme - March 8, 2023

Beginning around August 2019 and continuing through September 2021, Justin Skiff used his position as a Claims Specialist with the Social Security Administration (SSA), to fraudulently obtain money from the SSA.

Skiff used his knowledge and access to establish Social Security Numbers for ten fictitious children. He then established fictitious records of entitlements for surviving child benefits which he connected to the record of a real deceased individual whose children would receive benefits. These benefits were deposited into a bank account accessible to Skiff through debit cards he directed to be mailed to a P.O. Box to which he had access. Skiff withdrew money and made purchases from this account from October 2019 through September 2021 for a total amount of $324,201.44. (Source)

Department Of Labor Agent Pleads Guilty To $197,000+ Of Unemployment Fraud Schemes - March 22, 2023

Thomas Hartley was a Special Agent with the Department Of Labor.

Hartley admitted that he obtained a total of $197,366 through multiple fraud schemes. Between April 2020 and September 2021, Hartley applied for and collected Pennsylvania unemployment compensation benefits by claiming that he was unemployed, when in fact Hartley was employed on full time active duty with the New Jersey National Guard.

Further, in applying for unemployment benefits, the defendant failed to disclose that he was on military leave from his full-time federal civilian employment with the United States Department of Labor. Hartley thereby utilized the mail to collect approximately $60,284 in unemployment compensation funds to which he was not entitled.

Hartley also acknowledged that he fraudulently obtained $23,582 in Basic Allowance for Housing (BAH) funds paid by the Department of the Army, $50,000 in "lost wage" benefits paid by USAA insurance, and $63,500 from his Thrift Savings Plan.

Hartley was also charged with 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, resulting from an 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.

Hartley was also charged with fraudulently obtaining funds from his Thrift Savings Plan 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. (Source)

U.S. Fish & Wildlife Service Employee Charged With Embezzling $100,000+ - March 3, 2023

Kimberly Robinson was employed with the U.S. Fish and Wildlife Service (USFWS) since 2003, and in 2020 was promoted to the role of Budget Analyst in charge of reconciling the budgets for each USFWS regional office. To perform her duties the federal government issued Robinson multiple credit cards to pay for official government expenses and travel.

From at least 2018 through June 2021, Robinson engaged in a scheme to defraud the U.S. Fish and Wildlife Service by using her government issued credit cards for unauthorized personal purchases and expenses. She then deleted and altered the unauthorized transactions on the credit card statements submitted to her supervisor for reconciliation to conceal the scheme and to cause USFWS to disburse public funds to pay the credit card balances.

Robinson embezzled over $100,000 through this scheme. (Source)

Former U.S. Postal Worker Sentenced To Prison For Stealing $90,000+ Of Cash From Mail To Pay Off Debt / Give Money To Family - March 8, 2023

Roberta Feliz was employed as Lead Sales and Services Associate with the Gardner Post Office in Boston.

Between February and July 2020, Feliz stole over $90,000 in cash deposits that were mailed from a Tractor Supply Company to its bank. Feliz, who was scheduled to work on each day that a cash package was mailed, was observed on surveillance camera removing envelopes from the postal service floor into the employee locker area or the women's restroom.

In August 2020, Feliz was approached by law enforcement after she took a control package containing cash from the postal floor into an office, removed money from the envelope and hid it in an unused desk. Feliz admitted to stealing packages from the Tractor Supply Company and stated that she used the money to pay off debt and sent some to family overseas. (Source)

U.S. Postal Worker Charged With Embezzling $52,000+ - March 27, 2023

Anthony Fernandes was a Supervisor for the USPS in Buzzards Bay, Boston.

Fernandes fraudulently used his USPS supervisor's travel authorization account to approve approximately $52,987 in bogus travel reimbursement requests for the period of April through November 2022. (Source)

U.S. Postal Employee Sentenced To Prison For Mail Theft - March 15, 2023

Diamante Williams was indicted by a federal grand jury on three counts of mail theft by a U.S. Postal employee in March 2022 for events which occurred in March and April 2018.

In September, 2022 as stated in William's plea agreement, on or about March 28, he stole mail and contents of mail from individuals residing on his route, including financial instruments. Williams admitted to stealing a check intended for company in the amount of $1,274. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former U.S. Navy Assistant Chief Of Staff Sentenced To Prison In Massive Corruption Scandal - February 23, 2023

U.S. Navy Captain (Retired) Jesus Vasquez Cantu was sentenced today to 30 months in prison on charges that he received lavish bribes from foreign defense contractor Leonard Francis

Cantu acknowledged that Francis took him and others out for drinks and dinners at posh restaurants, nightclubs and karaoke bars and paid for lavish hotel rooms and the services of prostitutes on numerous occasions in 2012 and 2013, during which time Cantu was the Deputy Commander in the Far East in Singapore.

Cantu was in charge of logistical sustainment to Navy ships operating in the Seventh Fleet.

Cantu admitted that in return for these luxuries, he provided proprietary U.S. Navy information to Francis, and that he used his power and influence to help Francis and his company, Glenn Defense Marine Asia, known as GDMA, in its ship husbanding business. (Source)

Navy Doctor Pleads Guilty To Role In Defrauding The Navy Of $2 Million / Received $180,00 In Kickbacks - March 28, 2023

Dr. Michael Villarroel, a U.S. Navy Doctor, pleaded guilty in federal court, admitting that he and others conspired to defraud the Navy by faking or exaggerating injuries to obtain insurance payments intended to help service members recovering from traumatic injuries. Villarroel acknowledged he knew the claimed injuries were false or exaggerated but signed off on applications for a share of the insurance payments.

Villarroel admitted that from 2012 to at least December 2015, he conspired to commit wire fraud with Christopher Toups, a Chief Petty Officer Construction Mechanic in the Navy; Kelene Meyer, Toups' spouse and a nurse; and others. Toups prodded other service members to submit claims, told them to provide medical records to Meyer, requested part of the insurance payment in return, and distributed shares to Meyer and Villarroel. Meyer used her medical background to falsify or doctor supporting records to reflect fake or exaggerated injuries.

Participants in the scheme obtained about $2 Million in payments from the Traumatic Service Members Groups Life Insurance (TSGLI) program which is funded by service members and the Navy. Villarroel personally obtained more than $180,000 in kickbacks. (Source)

Former U.S. Army Soldier Sentenced To Prison For Attempting To Murder Fellow Service Members In Deadly Ambush - March 3, 2023

Ethan Melzer planned a jihadist attack on his U.S. Army unit in the days leading up to a deployment to Turkey, and sent sensitive details about the unit including information about its location, movements, and security to members of the extremist organization Order of the Nine Angles (O9A), a white supremacist, neo-Nazi and pro-jihadist group.

Melzer joined the U.S. Army in approximately 2018 and infiltrated its ranks as part of an insight role to further his goals as an O9A adherent. In approximately October 2019, Melzer deployed abroad with the Army to Italy as a member of the 173rd Airborne Brigade Combat Team.

While stationed abroad, Melzer consumed propaganda from multiple extremist groups, including O9A and the Islamic State of Iraq and al-Sham, which is also known as ISIS. For example, Melzer subscribed to encrypted online forums where he downloaded and accessed videos of jihadist attacks on U.S. troops and facilities and jihadist executions of civilians and soldiers, in addition to far-right, neo-Nazi, and other white supremacist propaganda. (Source)

U.S. Army Reservist Pleads Guilty To The Theft Of $8,300+ Of Government Funds - March 3, 2023

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

The National Defense Authorization Act of 2000 authorizes military funeral honors for active-duty soldiers, retirees, and veterans. At a family's request, eligible persons can receive military funeral honors, including the folding and presenting of the United States flag and the playing of "Taps." (Source)

Army Service Member Charged In Connection With Romance Scams And COVID-19 Assistance Fraud - March 3, 2023

Sanda Frimpong, an active duty service member stationed at Fort Bragg.

Frimpong was arrested after the unsealing of a 19-count indictment that included charges of Money Laundering,Fraud, Conspiracy, Aggravated Identity Theft, and Access Device Fraud in connection with multiple interstate and international fraud and money-laundering scams.

Frimpong and other conspirators, engaged in elaborate scams, impersonating romantic love interests, diplomats, customs personnel, military personnel, and other fictitious personas for the purpose of ensnaring their victims by earning their confidence, including promises of romance, sharing of an inheritance or other riches, or other scenarios intended to fraudulently induce the victims to provide money or property to the conspirators. Frimpong allegedly laundered hundreds of thousands of dollars in proceeds of these frauds through his various bank accounts across state lines and through contacts in Ghana. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

3 Former New York City Correction Officers Plead Guilty To Sick Leave Fraud - March 7, 2023

Eduardo Trinidad pleaded guilty to federal program fraud, admitting that he fraudulently obtained his salary from the New York City Department of Correction (DOC) by taking sick leave even though he was able to work.

On February 15, 2023, and February 27, 2023, respectively, former New York City correction officers Steven Cange and Monica Coaxum also pleaded guilty to the same charge.

Cange fraudulently obtained more than $139,000 in salary while on sick leave from March 2021 to November 2022.

During that period of time, Cange submitted more than 100 fraudulent medical notes to DOC claiming that he was at physical therapy or another medical provider when records subpoenaed from those providers demonstrate that Cange was not at those appointments. Law enforcement also observed Cange engaging in normal life activities with no apparent difficulty.

Coaxum fraudulently obtained more than $80,000 in salary while on sick leave from March 2021 to April 2022, and Trinidad, her fiancée, fraudulently obtained more than $119,000 in salary while on sick leave from June 2021 to October 2022.

Although Coaxum claimed to suffer from multiple injuries, evidence collected by investigators showed that she was able to work. During her sick leave, Coaxum submitted nearly 50 fraudulent medical notes to DOC stating that she had gone to a medical appointment at a time when law enforcement determined she was elsewhere.

Additionally, evidence showed that on some occasions when Coaxum claimed to be injured and at home, she was traveling and attending parties.

Trinidad also claimed that he was unable to work for over a year due to an injury. But video and photographic surveillance showed Trinidad performing home improvement work, bowling, and traveling abroad without any difficulty or help from equipment like an orthopedic boot, sling or cane which he used when attending required check-ins with DOC medical officials. (Source)

Boston Police Captain Steals 5 Computers And Internal Affairs Records - March 9, 2023

Stephen Jones has been charged with computer theft, tampering with public records, and other offenses in connection with the April 2022 incident. The charges result from an Office of Public Integrity and Accountability's (OPIA) Corruption Bureau investigation.

The investigation revealed Jones removed at least 5 computer towers from the Boonton Police Department, 3 of which contained police information, including files on internal affairs (IA) matters. He stashed the computers in his home and the IA files at his in-laws' home.

Jones was captured on surveillance video late at night on April 13, 2022, removing containers and computer towers from the police department. (Source)

Former Bureau of Prisons Nurse Pleads Guilty To Contraband Smuggling And Bribery Conspiracy - March 9, 2023

From around November 2021 through late August 2022, Ruben Mirabal, who was a registered nurse working for the Federal Bureau of Prisons (BOP) at the Federal Detention Center – Miami (FDC-Miami"), solicited and obtained illegal payments from FDC-Miami inmates in exchange for bringing in and delivering to them prohibited objects, including controlled substances that had been soaked into sheets of paper.

Mirabal accepted thousands of dollars in bribes from these inmates and their associates. Along with these payments, Montanez-Mirabal also solicited and received other things of value from inmates, including the free use of a Lamborghini and a Rolls-Royce. (Source)

Former Detroit Police Officer Sentenced To Prison For Role In Tow Truck Refferal / Bribery Scheme - March 14, 2023

Daniel Vickers spent his career as a police officer in Detroit.

Vickers admitted to conspiring with Detroit Police Lieutenant John Kennedy. The two conspired to commit bribery by accepting money and other items of value in exchange for Kennedy using and promising to use his influence as a supervisor to persuade other officers to make tow referrals to a towing company in violation of the city's ordinance and Detroit Police Department policy.

Vickers also admitted that he and Kennedy conspired to solicit and accept thousands of dollars in cash, cars, car parts, car repairs, and new carpeting for Vickers' home, in exchange for providing the towing company that Kennedy was investigating with information about the status of the Public Integrity Unit's case.

In total, between February 2018, and June 2018, Vickers accepted over $3,400 in bribe payments from the towing company. In addition, Kennedy accepted bribes amounting to $14,950 during the course of the conspiracy. (Source)

2 Police Officers Sentenced To Prison For Cocaine Drug Trafficking - March 28, 2023
Alejandro Martinez was a former Police Officer with the Donna Police Department in Texas.

Martinez and Victor Vallejo pleaded guilty and were convicted for conspiracy to possess with the intent to distribute cocaine.

While serving as a Police Officer, Martinez assisted co-conspirators as they transported illegal drugs by escorting load vehicles in his official capacity as a Police Officer. He also diverted other officers away from the area. (Source)

STATE / CITY GOVERNMENTS / MAYORS

City Employee Sentenced To Prison For Role In Stealing $635,000+ Of COVID-19 Relief Funds - March 22, 2023
John Bernardo was employed by the City of West Haven In Connecticut as a Housing Specialist in the Office of Community Development Administration.

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

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

In January 2021, DiMassa and Bernardo formed Compass Investment Group, LLC. Beginning in February 2021, Compass Investment Group LLC fraudulently billed the City of West Haven and its COVID-19 Grant Department for consulting services purportedly provided to the West Haven Health Department that were not performed.

From February 2021 through September 2021, the City of West Haven paid Compass Investment Group a total of $636,783.70. Bernardo received a portion of these funds. DiMassa made several large cash withdrawals from the Compass Investment Group LLC bank account, some of which were made shortly before or after he was recorded as having made a large cash "buy-in" of gaming chips at the Mohegan Sun Casino. (Source)

Former City Chief Financial Officer Sentenced To Prison For Embezzling $625,000+ Of City Funds For Personal Use - March 22, 2023
Tracy Hudson was employed first as the City's Occupational Tax Administrator and then as its Chief Financial Officer for the City of Bardstown, Kentucky.

Between 2013 and September 2019, Hudson stole funds from the City of Bardstown by various means, including by taking cash from the City's funds for her own personal use, paying herself for false expense reimbursements, diverting additional payments into her 401K pension plan in excess of the amount withheld from her wages, purchasing personal items on a City credit card without authorization, and crediting payments to her personal accounts with the City despite no actual payment having been made.

The primary method by which Hudson stole from the City of Bardstown was by stealing cash, most often from cash payments made when individuals were paying for City services. Hudson also engaged in various activities which generated interstate wire communications to steal certain of the funds and to conceal her thefts from the City. (Source)

Former State Worker Admits Stealing $140,000 In Unemployment Insurance Funds - March 20, 2023

Vicky Hefner was working for the Department of Labor and Industrial Relations, Division of Employment Security as a Benefit Program Specialist at the time of the crimes, which occurred from July to December of 2020.

Hefner admitted logging into the accounts of approximately eight friends, relatives and associates to either make them eligible for unemployment benefits when they were not otherwise eligible or increase their benefits. She also backdated some claims to increase benefits and changed the status of some who were receiving pandemic-related unemployment assistance to regular unemployment assistance to fraudulently increase the benefits they received, the plea says.

Hefner had worked at the agency since 2009. (Source)

Former Public Works Commissioner Sentenced To Prison For Extortion / For Withholding Permits From Businesses - March 16, 2023

Former Macomb County Commissioner of Public Works Anthony Marrocco was sentenced to three months in prison and fourteen months of home confinement for attempted extortion by withholding county permits from businessmen who refused to contribute to Marrocco's campaign accounts.

Marrocco served as the Commissioner of Public Works from 1993 through 2016. In September 2022, Marrocco pleaded guilty to Count Three of the Indictment charging him with attempted extortion of a Macomb County developer in April 2016. Marrocco admitted that he pressured the developer to spend thousands of dollars to purchase tickets to one of Marrocco's fundraisers. Marrocco threatened to delay or withhold approval of county permits sought by the developer if he did not purchase additional tickets to Marrocco's political fundraiser. (Source)

Former County Assistant Judge Charged W/ Felony For Collecting $8,500 For Hours Not Worked - February 27, 2023

Patricia Duff is a County Assistant Judge. She is accused of collecting $8,500 for hours she did not work pleaded not guilty to two felony charges.

Between Jan. 1 and June 4 of 2033, Duff was paid $10,800 for 448 hours she reported working.

But she only worked 96 hours, equivalent to $2,300.

According to the police affidavit, in a phone call with a Detective, Duff was surprised to learn that she had allegedly over reported hundreds of work hours. She apparently told the investigator she was suffering from depression, had gotten sick with Covid-19 multiple times, and was taking care of a family member who was mentally ill. Robson noted that Duff said she was seeking the help of a psychiatrist. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

No Incidents To Report

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Bookkeeper Pleads Guilty To Embezzling $304,000+ From Labor Union - March 6, 2023

Denise Kovacs was the Bookkeeper at Plumbers AFL-CIO Local 803, a labor union that represents plumbers and pipefitters in central Florida.

During a nearly five-year period of employment, Kovacs stole $43,777 in cash from union dues and charged $261,126 in expenses on the union's credit card. To conceal her theft, Kovacs altered internal business records which kept union officials in the dark about her ongoing embezzlement of funds. (Source)

BANKING / FINANCIAL INSTITUTIONS

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

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

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

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees' to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding.". (Source)

Former Bank Manager Sentenced To Prison For Role In $25 Million COVID-19 Relief Fraud Scheme - March 14, 2023

Daniel Hernandez is a former South Florida Regional Manager for a leading national bank.

Hernandez has been sentenced to 120 months in prison for participating in a conspiracy to defraud the Paycheck Protection Program (PPP) out of loan proceeds.

Hernandez conspired with Erich Barata, Armando De Leon, and others to submit over 90 fraudulent PPP loan applications. The applications were primarily submitted to two banks, Hernandez's employer at the time, and his previous employer, another leading national bank.

Hernandez also conspired to submit fraudulent Economic Injury Disaster Loan applications through the SBA, but most of the applications were declined.

Hernandez and his co-conspirators attempted to defraud the PPP and EIDL programs out of approximately $25 Million. The conspiracy caused approximately $15 million in losses. The investigation has recovered over $800,000 so far. (Source)

Wells Fargo Banker Sentenced To Prison For Role In $3.8 Million International Money Laundering Scheme - February 28, 2023

Leopoldo Aguilera admitted to opening bank accounts under false names and wiring millions of dollars to Mexico, for which he received cash payments from an unspecified criminal organization.

The money he transferred was linked to the sale of narcotics by a Mexican drug cartel, specifically the sale of multi-kilogram amounts of fentanyl in the Midwest, the U.S. Attorney's Office said.

Aguilera opened 26 bank accounts for a money laundering organization. Of those, he created 11 accounts with false names, passport numbers and dates of birth. Those 11 accounts were used to wire $3.8 million to Mexico and prosecutors allege Aguilera conducted most of those wire transfers himself. (Source)

Former Bank Manager Admits To Embezzling about $439,000 From Bank - March 1, 2023

Samantha Cherry admitted that between January 1, 2021 and March 18, 2022, while a Manager at a UMB Bankis, she took cash directly from the vault and moved currency from other cash supplies into her cash drawer totals.

On March 18, 2022, Cherry told co-workers that she stole the money and gave it to her boyfriend, who she said had recently passed away.

Cherry admitted that she embezzled about $439,000 from her employer. (Source)

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

Stephen Reyna was the Branch manager of a Wells Fargo in Texas.

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

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

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

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

4 Co-conspirators Charged With The Theft $200,000 With Help Of Bank Assistant Branch Manager - March 1, 2022

Munson Hunter, Gregory Thurman, Travis Wright and Janem Gibbs are charged with the theft of $200,000.

Janem Gibbs was a former Assistant Branch Manager at Capital One.

Gibbs wire transferred money from a customer's account at Capital One without his knowledge to an account at a New York City bank.

Hunter, Thurman and Wright were charged with wire fraud for moving the stolen money through a series of other accounts at banks in New York, Virginia and Texas. The accounts were opened using fictitious names. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Employee Accused Of Stealing Trade Secrets From Company / Deleted 400 Files - March 16, 2023

Stryker Corporation, which is headquartered in Portage MI, filed a federal lawsuit against Carrie Hendrick, alleging she downloaded confidential information and deleted more than 400 files from the company's servers.

Stryker alleged that Hendrick caused damages to the company of $25,000 or more. Hendrick denied the allegations in a March 9 response to the lawsuit.

She resigned in July of 2022 after working at Stryker in Virginia for about two years.

Her attorney however in response said in a legal filing that Hendrick did not improperly access files and download confidential information onto flash drives as Stryker accused of her doing.
(Source)

Former Employee Charge For Stealing Trade Secrets From Samsung Biologics - March 23, 2023

The Incheon District Prosecutors' Office indicted the employee in relation to having stolen trade secrets from Samsung Biologics including some documents like standard operating procedures (SOP) in June last year before he moved to Lotte Biologics.

Samsung Biologics in sued four of its employees' who are suspected of leaking critical trade secrets to Lotte Biologics. One of the four was found guilty. The other three were cleared of the suspicions.

Samsung Biologics in May last year applied for an injunction for the infringement of trade secrets by three employees' who had moved to Lotte Biologics.

The court issued an injunction against the infringement of trade secrets filed by Samsung Biologics, preventing leaked business secrets of Samsung to be used by Lotte Biologics. (Source)

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

No Incidents To Report

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

Former Chief Operating Officer And Physician For Medical Practice Charged WIth Stealing $650,000 - March 14, 2023

The former Chief Operating Officer (COO) of a medical practice and one of its physicians have been charged with stealing more than $650,000 from their employer.

Francisco Ortiz and James Mersing have been indicted on charges of defrauding Wedgewood Physicians, Inc.

Ortiz used his position as COO to divert funds over a three-year period for his personal benefit and for the benefit of Mersing, a physician formerly employed by Wedgewood.

Ortiz is alleged to have used the funds to pay for personal travel, home improvements, and various items from Amazon, among other things. Ortiz is also alleged to have caused unauthorized bonuses to be paid to Mersing, who then returned a portion of the money to Ortiz as a kickback. (Source)

Surgeon Convicted For Accepting $300,000+ In Bribe Payments To Perform Spinal Surgeries At Corrupt Hospital / 24 Others Convicted In Scheme - March 6, 2023

Dr. Payne was an Orthopedic Surgeon at a now-defunct Long Beach hospital.

He was found guilty of accepting more than $315,000 in bribes and kickbacks for performing spinal surgeries.

The owner of the hospital (Michael Drobot) was sentenced to prison for committing a massive workers' compensation insurance fraud scheme, the Justice Department announced.

Drobot conspired with doctors, chiropractors, and marketers to pay kickbacks and bribes in return for the referral of patients to hospital for spinal surgeries and other medical services.

These services and surgeries were paid for primarily through the California workers' compensation system. During its final five years, the scheme resulted in the submission of more than $500 Million in medical bills for spinal surgeries involving kickbacks.

Payne received bribes from Drobot of up to $15,000 for each spinal surgery that he performed at the hospital. The top bribe payment was for lumbar spinal surgeries that Payne performed on patients at the hospital with implants from one of Drobot's companies. Drobot and Payne covered up the bribes by disguising them as payments for marketing services and fees based on a sham contract. In total, Payne received more than $315,000 in illegal payments.

To date, 24 defendants, among them doctors and surgeons, have been convicted for participating in the kickback scheme. (Source)

Former Employee Charged With Embezzling $150,000+ From Non-Profit Healthcare Over 9 Years Period - March 1, 2023

Michele Rose served as the Medical Staff Coordinator for a nonprofit for many years.

During her employment, Rose would occasionally make business-related purchases with her personal funds, for which she would be reimbursed by the business upon proof of receipt.

From March 2011 to December 2020, Rose allegedly used her position to embezzle $153,769.00 by writing 165 fraudulent checks to herself for reimbursement of purchases that she never made. Rose made numerous false representations to organization leadership to obtain signed, blank checks to reimburse herself for nonexistent expenses. Once the blank checks were signed, Rose wrote them to herself for various amounts and deposed the funds into her personal account. Rose then fraudulently concealed the fake reimbursements by omitting them from financial reports to organization leadership. (Source)

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

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

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

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

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

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

President Of Oklahoma Steel Manufacturer Pleads Guilty To Directing Outside Payroll Service To Pay Him $2.6 Million+ Over A 5 Year Period - March 13, 2023

From 2014 to 2019, Phillip Albert of Tulsa was President of Pelco Structural LLC and directed its outside payroll service company to pay him over $2.6 million. Albert instructed that the payments be classified as reimbursements rather than income, so that federal income taxes would not be withheld, and the payments would not be reported on his Forms W-2 as wages. (Source)

Former Partner / Sales Person At Broker-Dealer Firm Charged With Making $3.4 Million+ In Insider Trading Scheme - March 30, 2023

Christopher Matthaei was a partner and senior salesperson at a Charlotte, North Carolina-based broker-dealer with offices in Red Bank, New Jersey.

From May 2020 through February 2021, Matthaei illegally traded on material, non-public information, or MNPI, that he received from a conspirator, a friend who worked at a large Canadian asset management firm. The MNPI pertained to SPACs that were engaged in confidential merger negotiations and shared information with the asset management firm as a potential investor in the SPAC deals. The conspirator received this MNPI every time a SPAC was placed on his firm's confidential restricted list, meaning that the firm's employees' were prohibited from buying or selling the SPACs' securities, either personally or via another person or third party.

Despite knowing about these trading restrictions, the conspirator shared the MNPI with Matthaei, who then purchased securities in the SPACs using his personal brokerage accounts. In June 2020, Matthaei paid for a private plane and extended trip with the co-coconspirator and their families to a luxury resort on the island of St. Barth, where they continued to engage in the insider trading scheme.

Matthaei made more than $3.4 Million in illegal trading profits from the insider trading scheme. (Source)

Former Employee Pleads Guilty To Embezzling $1.8 Million From Employer Over 12 Year Period - March 1, 2023

Between April 2008 and April 2020, Joanne Dinoto stole more than $1.8 Million from her employer.

Dinoto falsely inflated her compensation, using her employer's corporate credit card for personal expenses, and forging at least two checks to herself drawn on her employer's checking account.

To hide her scheme, Dinoto modified her employer's accounting records. Dinoto later collected unemployment benefits from the Massachusetts Department of Unemployment Assistance under her true Social Security number, despite the fact that she was then working full time for a different employer, a lighting company under a fake Social Security number. (Source)

Former Financial Manager For Property Manager Company Pleads Guilty To Embezzling $1 Million+ - March 9, 2023

Mai Houa Xionga was employed as a Financial Manager for a Minneapolis-based property management company that provided financial services to homeowners' associations (HOAs).

Xiong's duties included bookkeeping, and as a manager she had access to the victim associations' financials, bank accounts, vendor and contractor payments, and bookkeeping systems.

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

As part of the scheme, Xiong repeatedly accessed bank accounts and conducted electronic transfers of funds directly into her personal bank accounts. Xiong disguised these transfers by mislabeling them to make it appear as if they were legitimate homeowner association expenses. Xiong also used her authority as a signatory to make cash withdrawals directly from the HOAs' accounts, including making withdrawals after she was fired from her position in July 2021.

After her termination, Xiong began collecting Unemployment Insurance (UI) funds. However, even after Xiong found new employment, she continued to wrongfully obtain public UI benefits. (Source)

Former Employee Sentenced To Prison For Embezzling $339,000+ Over 6 Years - March 9, 2023

Ronald Miller was the Warehouse and Labor Supervisor for a small floor covering business, were he had worked for 25 years. He was responsible for supervising the company's installers, scheduling their weekly shifts and drafting their timesheets. He also had the authority to hire flooring installers.

Beginning March 27, 2014, he used several schemes over the next 6 1/2 years to steal.

Miller submitted false timesheets for his partner, who did not work for the company. He then collected his partner's paycheck and forged his partner's signature to deposit the money in his own account, his plea agreement says.

Miller falsely inflated the hours worked by his son without his son's knowledge and did the same for himself by falsely claiming he was working on installation projects.

Miller also submitted fraudulent invoices claiming he'd made purchases at two fake companies and paid himself with company credit cards or caused the company to issue checks to pay the fake invoices.

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

Former Director Of Finance Sentenced To Prison For Embezzling $270,000+ From Non-Profit Organization - March 3, 2023

Kristina Ballard worked for a nonprofit organization in Washington, D.C. Between August 2014 and December 2020, at which point she was fired for poor performance. She served as the organization's Director of Finance.

From January 2015 through December 2020, Ballard embezzled $271,465 from the organization.

She fraudulently wired organization funds to bank accounts that she controlled, intercepted credit card rewards checks issued to the organization, and then deposited those checks into a bank account she controlled, and fraudulently charged personal purchases on the organization's credit card.

Ballard started embezzling from the D.C. non-profit just four days after she was indicted in Arlington County, Virginia, for embezzling from a previous employer. In July 2015, a Virginia court sentenced her to four years of probation. On Nov. 5, 2020, she used the organization's credit card from her new employer to pay $24,694 in restitution to the Virginia court for her prior embezzlement scheme with another employer.

In conjunction with her sentencing in the case with her previous employer, Ballard said she had learned from her mistakes and would "never let something like this happen again." In fact, between the time she was indicted in Virginia in January 2015 and sentenced in July 2015, she had embezzled more than $30,000 from her new D.C. employer. Following the imposition of the probationary sentence, Ballard went on to steal approximately $240,000 more from the D.C. non-profit.

Ballard concealed her fraud from the D.C. employer by listing various beneficiary names on wire transfers and creating fake invoices, often using fake company names. She also forged the Executive Director's signature on the credit card rewards checks before she deposited them. (Source)

Financial Manager Charged With Embezzling $200,000+ From Client Over 6 Years - March 16, 2023
Katie Laroche was a Financial Manager who handled bookkeeping, accounting, and other financial services for her clients.

Laroche created, owned, and operated a business, Capital City Consulting Firm, that purported to provide financial management services.

From about February 2015 through March 2021, Laroche engaged in a scheme to defraud Victim 1 and Victim 1's businesses by withdrawing funds from Victim 1's accounts under false pretenses and using the funds for her own benefit.

Laroche falsely represented that the funds were being used to pay federal income taxes. When Victim 1 asked Laroche about the status of Victim 1's tax obligations, Laroche lied to Victim 1 to hide her scheme. Laroche also arranged for monthly payments to be automatically withdrawn from Victim 1's account without Victim 1's knowledge or consent to pay for an automobile insurance policy benefitting someone other than Victim 1. In total, Laroche embezzled $233,363.53 from Victim 1. (Source)

Former Employee Charged With Embezzling $100,00 From Employer - March 9, 2023
Madonna Peterson worked for an Indian Tribal Organization.

Between January of 2017 and July of 2021 Peterson stole more than $100,000 from her employer. (Source)

IT Contractor For Australian Maritime Museum Charged For Diverting $90,000 To His Own Bank Account - March 6, 2023
A third-party IT contractor working at the Australian National Maritime Museum allegedly accessed its accounting system and illegally changed bank account details stored in the system to his own.

The museum allegedly detected anomalies in financial information related to contracted companies in November last year and engaged independent forensic investigators, who identified the alleged fraud.

In addition to allegedly altering details of stored accounts, police said the financial details of several individuals and businesses were also unlawfully obtained, resulting in the man allegedly using credit card information to make a series of unauthorized purchases.

Police raided the man's home in Macquarie Park in Sydney's north, where they seized a laptop, hard drives and a mobile phone, which will be subject to further forensic analysis.

The total value of money allegedly diverted in this matter at $90,000. (Source)

Former Manager Of Motor Vehicles Pleads Guilty To Passing Learner's Permit Tests In Exchange For Money - March 31, 2023
Mia Johnson is the former Manager of the Registry of Motor Vehicles (RMV).

Between December 2018 and October 2019, Johnson conspired to take money in exchange for agreeing to give customers passing scores on their multiple-choice learner's permit tests even if they did not pass. These customers were told to request a paper test instead of taking the test on the RMV computer. Cox-Johnson scored these customers' paper tests.

On Dec. 28, 2018, Cox-Johnson accepted $1,000 in cash – delivered from a friend on behalf of another individual – in exchange for giving a passing score to the individual's relative who had failed the passenger vehicle learner's permit test six times when taking it in their native language.

On Oct. 21, 2019, a customer came to the RMV and took three multiple-choice tests they needed to pass in order to get a commercial learner's permit Johnson accepted $200 in cash from an individual to score the customer as having passed the tests even if they did not actually pass. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE

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

Christine Fletcher pleaded guilty to bank fraud and tax evasion. As part of her plea agreement, Fletcher will pay at least $2,188,870 in restitution to her former employer.

Fletcher worked for a company and various other entities owned by her employer for approximately 38 years. She was entrusted to manage her employer's various Bank of Oklahoma Financial (BOKF) and Trust Company of Oklahoma bank accounts. She was also entrusted with preparing and providing financial statements and related information to the company's tax preparer.

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

To avoid being detected, she routinely made unauthorized transfers between and among various BOKF and Trust Company of Oklahoma accounts before misappropriating the funds for her own personal use.

One of the many ways she fraudulently moved money, included making unauthorized transfers from some accounts into a specific individual's account. From there, Fletcher prepared forged checks bearing the individual's name and made the checks payable to herself or on her own behalf. Fletcher also admitted to routinely paying her credit card bills with the unauthorized and forged checks. (Source)

Former Charter Schools Accountant Charged In $2.5 Million+ Fraud Scheme / Used Funds For Travel, Cosmetic Surgeries, Home Improvement, Etc. - March 6, 2023

Cole Arnold was an accountant for Academica West Services, which provides services for charter school business operations. Arnold provided financial services to several charter schools in Utah.

Beginning in August 2017 and continuing through June 2022, Arnold used his position to steal $2,563,348.23 from North Davis Preparatory and Ascent Academies.

Arnold's Faudulent Activities Included:

Creating false invoices, bills and credit card statements claiming fees for school supplies, teacher salaries, and other fictitious line-item expenses, for the purpose of generating payments to credit cards controlled by himself.

Creating false computer journal entries claiming a variety of school related expenses; passing fraudulently obtained money through Venmo and a bank account in the name of Upper Limit Innovation, a registered Utah business that Arnold was a co-owner and registered agent of, to transfer the fraudulently obtained money.

The stolen charter school funds were used by Cole for travel, concerts, cosmetic surgeries, home improvements, jewelry, furniture, electronics, and other personal expenses. (Source)

Former Chief Financial Officer Sentenced To Prison For Embezzling $1.9 Million+ / Used $750,000 Of Money To Pay For Personal Expenses - March 14, 2023

Christopher Firle was the Chief Financial Officer of a holding company that managed several vehicle dealerships.

From January 2016 through September 2019, Firle misappropriated over $1.9 Million from the company. He carried out his embezzlement scheme in multiple ways, including by using company credit cards to pay for over $750,000 in personal expenses.

The unauthorized charges included tickets to sporting events and purchases at several retail stores, including Bergdorf Goodman, Chanel, Hermès, Nordstrom, and Tiffany & Co. Firle also initiated over 30 unauthorized wire transfers from the company to a family member. Those transfers totaled over $500,000. Additionally, Firle issued over 30 unauthorized company checks to himself that totaled over $165,000, and he withdrew more than $50,000 from a company account without authorization. Finally, Firle issued himself excess bonus payments totaling almost $160,000. (Source)

Former IT Director Admits To Embezzling $1 Million+ Since 2012 / Used Money For Personal Expenses - March 16, 2023

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

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

Hicks' criminal conduct came to light in March 2022, when AT Wall Companies hired forensic analysts to determine the source of a cyberattack and to assess vulnerabilities in its computer system.

Hicks refused to provide his computer and passwords, as per company policy. Information and analysis provided by the company to the Warwick Police Department, Homeland Security Investigations, and the United States Attorney's Office subsequently revealed that Hicks had embezzled over one million dollars from the company since 2012. (Source)

Former Delta Air Lines Ticketing Specialist Pleads Guilty To Issuing $447,000 Of Free Tickets - March 10, 2023

Aquil Muhammad worked as a Delta Air Lines Ticketing Specialist in Minneapolis, Minnesota. In 2016, he began issuing no-fare tickets to various individuals, including family members and other acquaintances.

Muhammad issued non-revenue tickets without a corresponding Non-Cash Incentive Certificate. That is, he issued free tickets, without compensation to Delta. These non-revenue tickets generated tax liability to Delta even though they had no associated cost. Muhammad also created fraudulent Transportation Credit Vouchers and Delta Travel Vouchers to cover the required taxes.

Muhammad issued these non-revenue tickets from late 2016 through December 2017.

He ultimately issued more than 230 tickets, with a lost revenue total of approximately $447,000.

Each of the tickets were issued using Muhammad's unique agent security identifier. In addition, many of the tickets included Muhammad's personal email address as the contact for the passenger. He would sell these free tickets, often being paid through Square. (Source)

Former Real Estate Company Employee Admits To Embezzling $487,000 / Used Money To Purchase Vehicle - March 1, 2023

Crystal Hendrix admitted to a scheme to defraud her former employer, a real estate company.

Hendrix handled payroll as part of her duties and had access to the company bank accounts.

From about January 2018 to Dec. 2020, Hendrix sent over 140 payments from the company bank account to her own bank account, totaling approximately $483,037. Hendrix used the money at restaurants and to buy a vehicle. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Former Maui Jim / Sunglass Manufacture Employee Pleads Guility T0 $100,000+ Of Mail / Wire Fraud - March 21,2032

Erica Hornof was an employee Maui Jim.

Maui Jim is a sunglass manufacturer and maintains its world headquarters in Peoria, Illinois/

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

From 2021 until 2022 Hornof stole sunglass parts 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)

Former County Employee Pleads Guilty To Stealing Road Maintenance Equipment & Providing To Pawn Shops - February 27, 2023

Jonathan Smith was a County Road Supervisor.

Smith was originally arrested last year after stealing road maintenance equipment and two catalytic converters from Jackson County taxpayers.

Authorities say several items were recovered at various pawn shops in connection the investigation. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

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

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

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

In early January 2021, Sewell, a Garda Armored Truck Driver, recruited Pollard and the other codefendants to stage his robbery. After formulating the plan over Snapchat, Pollard, Murphy, Burge, and Calhoun traveled from Cedartown to Sewell's apartment in North Charleston on January 15, 2021. Later that day, they drove around North Charleston looking for the best location to stage the theft. On January 16, 2021, Sewell parked his truck full of money outside an ATM in North Charleston.

Pollard and the other codefendants approached Sewell and pretended to restrain him at gunpoint. They then loaded $1.9 Million in cash into black trash bags and immediately fled back to Cedartown. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former U.S. Postal Service Mail Carrier Sentenced To Prison For Teaching Other Mail Carriers How To Deliver Drugs Through Mail - March 30, 2023

Former USPS Mail Carrier Robert Sheppard was sentenced to prison for recruiting fellow mail carriers, and teaching them how to deliver packages of cocaine and marijuana while he was on disability leave.

In 2015, Sheppard worked as a U.S Postal Service (USPS) Mail Carrier. In exchange for receiving bribes, Sheppard used his position to deliver five-pound packages of drugs through the U.S. mail 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. But he offered to recruit other mail carriers to deliver drugs for Frazier in exchange for referral fees in the form of a mix of cash and marijuana. Frazier agreed to the arrangement.

Sheppard then contacted two coworkers, Tonie Harris and Clifton Lee. Sheppard explained to Harris and Lee that they could earn bribes for delivering packages of drugs along their mail routes, and taught them how to arrange the deliveries to avoid detection. Harris and Lee agreed to participate in the scheme, and 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, per parcel. (Source)

Executive Director Of Police Officers' Association Charged With Importing Fentanyl - March 29, 2023

The Executive Director (Joanne Segovia) of the San Jose Police Officers' Association (SJPOA) has been charged with attempting to illegally import a controlled substance, according to the United States Department of Justice. Segovia is accused of ordering thousands of opioids to her home and agreeing to distribute them in the United States.

A federal criminal complaint states that Segovia used her personal and office computers to order the drugs between October 2015 and January 2023, including fentanyl. At least 61 shipments were mailed to her home from countries including Hong Kong, Hungary, and India, the DOJ said.

Law enforcement first learned of the connection to Segovia, who has been with the SJPOA since 2003, when investigating a network in India that ships drugs into the United States. A network operative's phone was searched, and Homeland Security agents found messages that mentioned "J Segovia" at an address in San Jose, including the words "180 pills SOMA 500mg," the complaint shows.

U.S. Customs and Border Protection records showed that five shipments to Segovia's address were intercepted between July 2019 and January 2023. The packages contained more than a kilogram of controlled substances such as Zolpidem and Tramadol.

The packages mailed to Segovia's home had innocuous labels, such as "Shirts Tops," "Chocolate and Sweets" and "Gift Makeup," according to the DOJ. Homeland Security said shipments from several foreign countries with such labels often contain illicit drugs. (Source)

Former Police Officer Pleads Guilty To Cocaine Trafficking While On Duty - March 13, 2023

Keven Rodriguez was on duty and employed as a Patrol Officer with the Raleigh Police Department when he sold cocaine to a confidential informant on January 24, 2022.

Rodriguez sold 56 grams of cocaine while in uniform with his duty issued firearm. Rodriguez then sold cocaine to the confidential informant on two other occasions, February 2, 2022 and February 8, 2022 while still employed with the Raleigh Police Department. Rodriguez was arrested on February 23, 2022. (Source)

Medical Office Nurse Sentenced To Prison For Illegal Oxycodone Prescription Scheme - March 21, 2023

Between March 2020 and June 2022, Jacquelyn DeVito worked as Nurse at an urgent care medical office.

During this employment, she offered patients separate home health services through her privately-owned company, Bee Home Medical LLC. DeVito used Bee Home Medical patients' names and dates of birth to prescribe oxycodone, a Schedule II controlled substance, without their knowledge or consent and issued those prescriptions to local retail pharmacies.

When the prescriptions were filled and ready to be picked up, DeVito went to the pharmacies and acquired the controlled substances by falsely stating that she was the victim patients' caregiver and was picking up the controlled substances on their behalf. In this manner, DeVito prescribed and acquired more than 2,900 oxycodone pills. Many of the victim patients had no knowledge that DeVito had issued the prescriptions in their names and confirmed that there was no legitimate need for them to receive the medication. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Hobby Lobby Employee Shoots & Kills Manager At Distribution Center – March 1, 2023

A Hobby Lobby employee shot and killed a manager at a distribution center on Wednesday in Oklahoma City, according to police.

The suspect had a dispute with the victim before the shooting around 5:00 p.m., according to police.

The man suspected of shooting and killing his supervisor died when he crashed his car during a police chase, police said Thursday. (Source)

Family Dollar Employee Charged With Murder After Firing Shots At Shoplifter Who Punched Him - March 25, 2023

Kevin Madrid was an employee of an Arizona Family Dollar store.

Madrid confronted the serial shoplifter and told him to leave the store at which point the shoplifter punched him in the face which knocked off Madrid's eyeglasses.

Madrid then allegedly pulled out a gun and shot the shoplifter at least 10 times, including several times when the shoplifter was on the ground.

Madrid stated "he had made the worst decision of his life," police said in his probable cause statement.

One employee in the store said that Madrid fired as many as 15 shots and admitted after the shooting that he could not control his anger. (Source)

Dunkin' Donut Employee Accused Of Shooting Customer After Argument - March 8, 2023

Khalil Abdul Shakur Shaheed, an employee at the Clearwater, Florida Dunkin Donuts' got into a disagreement with a customer (Jewitt Steele) who was trying to buy ice cream for his girlfriend and his two children at the store's conjoined Baskin Robbins.

Shaheed was arrested in the neighboring Sam's Club parking lot with the gun reportedly still on him. He is charged with aggravated battery with a deadly weapon and carrying a concealed firearm.

Police are hoping a Steele will be able to give them details about the argument that led up to the shooting. (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

EMPLOYEE EXTORTION

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lottery Official Tried To Rig $14 Million+ Jackpot By Inserting Software Code Into Computer That Picked Numbers - Largest Lottery Fraud In U.S. History - 2010

This incident happened in 2010, but the articles on the links below are worth reading, and are great examples of all the indicators that were ignored.

Eddie Tipton was a Lottery Official in Iowa. Tipton had been working for the Des Moines based Multi-State Lottery Association (MSLA) since 2003, and was promoted to the Information Security Director in 2013.

Tipton was first convicted in October 2015 of rigging a $14.3 Million drawing of the MSLA lottery game Hot Lotto. Tipton never got his hands on the winning total, but was sentenced to prison. Tipton was released on parole in July 2022.

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005. Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

That software code was replicated on as many as 17 state lottery systems, as the MSLA random-number software was designed by Tipton. For nearly a decade, it allowed Tipton to rig the drawings for games played on three dates each year: May 27, Nov. 23 and Dec. 29.

Tipton ultimately confessed to rigging other lottery drawings in Colorado, Wisconsin, Kansas and Oklahoma.

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

Eddie Tipton was making almost $100,000 a year. But he felt underappreciated and overworked at the time he wrote the code to hack into the national lottery system.

He was working 50- to 60-hour weeks and often was in the office until 11 p.m. His managers expected him to take on far more roles than were practical, he complained.

Tipton Stated: "I wrote software. I worked on Web pages. I did network security. I did firewalls," he said in his confession. "And then I did my regular auditing job on top of all that. They just found no limits to what they wanted to make me do. It even got to the point where the word 'slave' was used."

Nobody at the MSLA oversaw his complete body of work, and few people truly cared about security, he said. That lack of oversight allowed Tipton to write, install and use his secret code without discovery.
Video Complete Story Indicators Overlooked / Ignored

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,400+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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

FTK ENTERPRISE

FOR NETWORK INVESTIGATIONS AND POST-BREACH ANALYSIS

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

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

DOWNLOAD

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

GET A DEMO

exterro

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