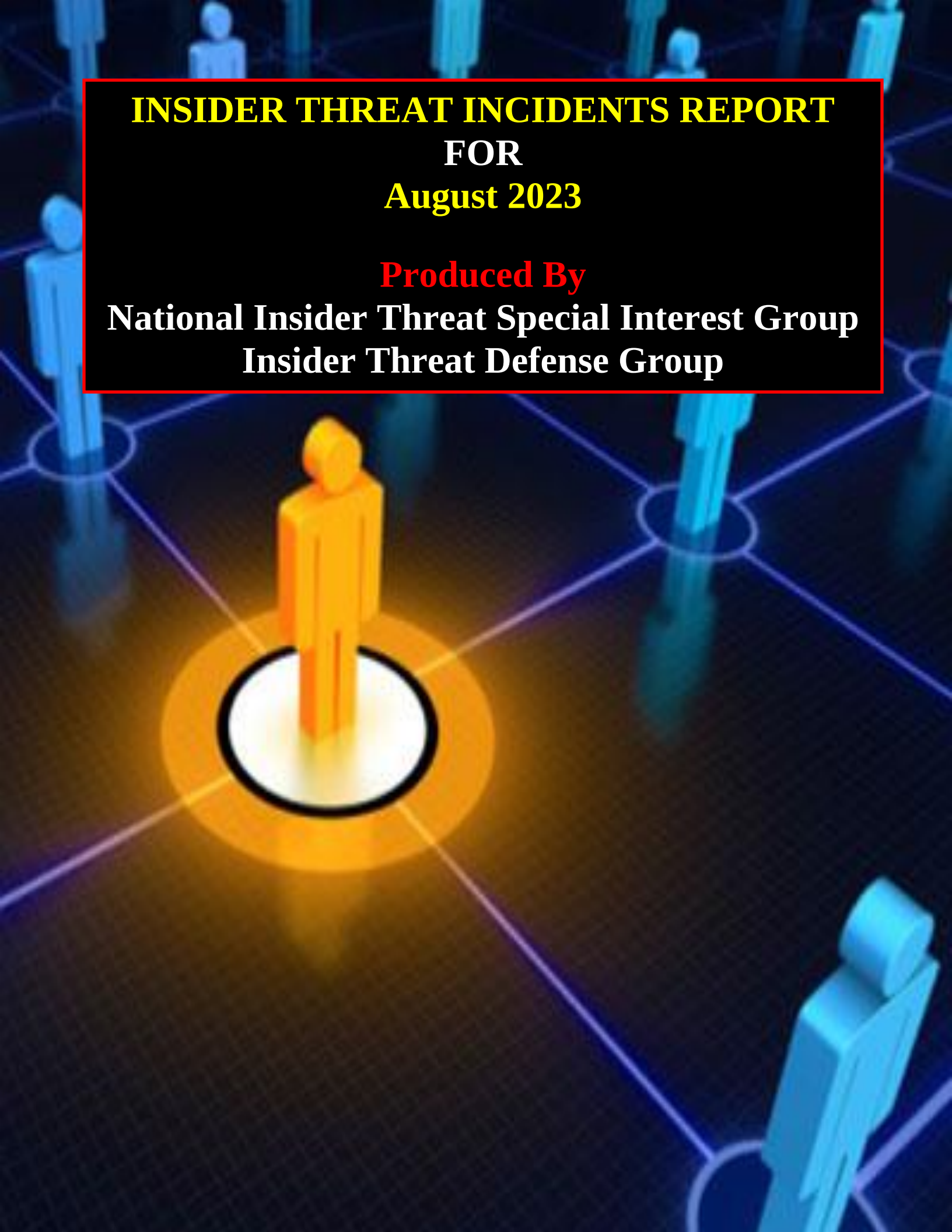

INSIDER THREAT INCIDENTS REPORT
FOR
August 2023

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 **4,600+** 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 must 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.

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

Some organizations invest thousands of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of the Insider Threat Incidents Reports published monthly by the NITSIG, you might have a different perspective on Insider Threats.

The Human Operating System (Brain) is very sophisticated and underestimating the capabilities of a **Negligent, Disgruntled**, **Malicious** or **Opportunist** employee can have severe impacts for organizations.

Some organizations need to re-evaluate their approach to detecting and mitigating Insider Threats, from a holistic approach. Successful Insider Threat Mitigation requires Key Stakeholder Commitments and Business Process Improvements. (CSO, CISO, Human Resources, Supervisors, CIO - IT, Network Security, Counterintelligence Investigators, Legal Etc.)

If you are looking to gain support from your CEO, C-Suite and Supervisors for detecting and mitigating Insider Threats, and want to provide them with the education, justification, return on investment, and funding needed for developing, managing or optimizing an Insider Threat Program, the incidents listed on pages 7 to 26 of this report should help. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

DEFINITIONS OF INSIDER THREATS

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

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

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees'

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

Legal & Liability Impacts (External Costs)

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

NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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

INSIDER THREAT INCIDENTS
FOR AUGUST 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

INDIA

Aerospace Engineer Stole Sensitive Data On Light Combat Aircraft Program And Sold Data On Dark Web - August 16, 2023

It is alleged that Siva Rama Krishna Chennuboina stole the data between July 2020 and February 2021.

Chennuboina allegedly leaked onto the dark web for personal financial gain. Chennuboina had been an Intern at the Indian Institute of Science, where he was involved in projects sanctioned by the Aeronautical Development Agency for the Ministry of Defence. During his internship, he had access to the source code for the Light Combat Aircrafts.

It was alleged that Chennuboina had illicitly obtained the complete source code and published it for sale on the dark web.

The data theft did not come to the attention of authorities for approximately 18 months. (Source)

U.S. GOVERNMENT

Booze Allen Hamilton (BAH) Senior Manager Called Federal Auditors To Stupid To Notice Government Overcharging / BAH Agrees To Pay $377 Million In Restitution To Government

Only a few months into a new finance job, Sarah Feinberg felt stunned when a senior manager with a Northern Virginia-based defense contractor called federal auditors “too stupid” to notice overcharging, according to a federal complaint she filed.

Feinberg said she had warned the manager that the company, Booz Allen Hamilton, was losing tens of millions of dollars and, in her view, billing more than it should on U.S. government contracts to cover the losses.

During the ensuing nine months, she repeatedly raised concerns with senior executives, including internal compliance officials and the chief financial officer, according to the 37-page civil complaint she filed against Booz Allen in 2016 under the federal False Claims Act.

Feinberg stated that Warren Kohm, then the company’s director of financial analytics and strategy, told her that federal auditors were “too stupid” to figure out what Booz was doing. He called the compliance rules ambiguous and said the auditors would not be motivated to collect all of the overcharges even if some billing was not permitted, according to Feinberg’s complaint.

In July, the Justice Department, which investigated her complaint, announced that Booz Allen had agreed to pay $377 million — $209 million in restitution to the federal government and the rest in penalties — to settle the matter, one of the largest awards in a government procurement case in history. (Source)

Federal Government Employee Sentenced To Prison For Leading $3.5 Million Unemployment Insurance Fraud Scheme - August 23, 2023

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

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

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

Huffman's sentencing was originally scheduled for November 29, 2022, but she failed to appear that day without notice or explanation. Prior to her disappearance, Huffman took measures to flee prosecution and conceal her whereabouts, including depleting her bank accounts, selling her vehicle, and turning her phone off. Through means unknown, Huffman obtained the PII of a real person, assumed that person's identity, and procured counterfeit government identification and credit cards in the name of her false alias. Following Huffman's disappearance, the United States Marshals Service (USMS) opened a fugitive investigation. This extensive, months-long investigation uncovered evidence that the defendant, under a false identity, was living and working as a registered nurse in Kansas. On March 4, 2023, approximately 95 days after Huffman's flight from prosecution, she was apprehended by the USMS in Kansas at an Extended Stay hotel. (Source)

U.S. Department Of Agriculture Employee And others Charged For Public Corruption - August 24, 2023

Roberto Rodriguez worked or the U.S. Department Of Agriculture (USDA) as a Rural Development Loan Specialist.

From on or about January 2021 and continuing through Aug. 22, Rodriguez accepted bribe payments from Sandoval and Diaz. In return, Rodriguez allegedly referred applicants of the USDA 504 Single Family Housing Repair Grant and Loan program to the contractors.

Rodriguez did knowingly, corruptly and in violation of his official duty, accept payments from Sandoval and Diaz, according to the allegations. The contractors allegedly paid the bribes with the intent to influence official acts after the federally-funded repairs were completed. (Source)

Department Of Labor Special Agent Sentenced To Prison For Multiple Fraud Schemes Totaling $197,000+ - August 24, 2023

Former Special Agent with the Department of Labor, Thomas Hartley was sentenced to prison for mail fraud in connection with multiple schemes to commit fraud.

Hartley pleaded guilty and 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 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. (Source)

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

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

McFadden was the leader of a scheme responsible more than 400 fraudulent Paycheck Protection Program PPP loan applications.

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

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

Former U.S. Postal Service Mail Carrier & Co-Conspirator Sentenced To Prison For $244,000+ Identity Theft / Fraud Scheme Using Stolen Mail - August 9, 2023

Robenson Fenelon and Squille Traxler, have been sentenced to prison after pleading guilty to conspiracy to commit bank fraud and theft of stolen mail. Fenelon additionally plead guilty to aggravated identity theft.

From at least January 2019 through December 2020, Fenelon and Traxler conspired with mail carriers in a scheme to steal the identities of at least 50 victims, and used that information to defraud financial institutions of a total of $244,222.93.

Traxler was employed as a Mail Carrier with the U.S. Postal Service. Fenelon recruited Traxler to assist in identifying potential identity theft targets.

Fenelon and Traxler used Traxler's access to the mail to obtain the targets' identity information, including names, dates of birth, social security numbers, addresses, phone numbers, and bank account numbers. Fenelon then used that information to access and take over the victims' bank accounts or to open new bank accounts in the victims' names.

Fenelon contacted the victims' banks, purporting to the victims or their relatives, and requested a new debit or credit card for the victim's account. For the newly established accounts, Fenelon applied online or over the phone for new accounts and credit cards.

Fenlon and Traxler then stole the credit cards from the victims' mail. Fenelon and Traxler used the cards to withdraw cash and make personal purchases. They stole checks from the mail and deposited them into the bank accounts they controlled. (Source)

Former U.S. Postal Service Mail Carrier Convicted Of Stealing $4,500+ Of Rebate Checks From Mail - August 10, 2023

In early June 2022, a woman living in Cumberland, Wisconsin contacted her local police department to report a stolen Menards rebate check. When she did not receive the check in the mail as expected, she called Menards and learned that the check had been spent without her knowledge.

Footage of the transaction showed the check was used by Joshua Copas, who was working as a U.S. Postal Service mail carrier at the time.

Further investigation linked Copas to thefts of 30 other Menards rebate checks, all but two of which were to be delivered on his mail route from late March to late May 2022. The collective dollar amount associated with the 31 stolen rebate checks was $4,547.84. (Source)

U.S. Postal Service Mail Carrier On Administrative Leave Sentenced To Prison For Stealing Mail From 900 Customers - August 11, 2023

During the evening of November 21, 2022, an off-duty San Diego Police detective saw a woman in a hooded sweatshirt open a communal mailbox at his apartment complex in Santee, California and remove multiple pieces of mail. As the detective approached, the female closed the mailbox and fled in a White Nissan. After getting the license plate of the vehicle, the detective determined that Rumley resided at the same address as listed for the vehicle registration and referred the matter to the U.S. Postal Service.

Rumley had been placed on administrative leave from her employment at the Santee Post Office earlier that month and was terminated by the Postal Service on December 12, 2022.

After securing a search warrant for the residence, on December 21, 2022, United States Postal Service Inspectors found more than 1,500 pieces of mail in Rumley's residence including, but not limited to, gift cards, credit cards and even several Christmas presents that had all been stolen from nearly 900 customers along her mail delivery route in Santee. Inspectors also found the keys she was given as a mail carrier to access mailboxes. The keys were hidden in a potted plant within her bedroom. In her plea agreement, Rumley admitted that, even after being placed on administrative leave, she kept those keys though she was not authorized to do so and used them to continue to steal mail even after she was terminated. (Source)

Former IRS Employee Sentenced To Prison For Selling Morphine That Contributed To Co-worker's Death - August 21, 2023

Margarita Aispuro-Camacho was sentenced to prison for illegally selling morphine and contributing to the death of her co-worker at the Internal Revenue Service.

In May 2020, the police found the co-worker dead in an apartment. A toxicology report confirmed the co-worker died from an overdose of morphine and other prescription drugs. Importantly, the co-worker did not have a prescription for the morphine.

Agents obtained text messages between the co-worker and Aispuro-Camacho that showed the co-worker bought various prescription drugs from Aispuro-Camacho over an extended period and that the co-worker bought morphine from her the day before the co-worker died. Shortly after the co-workers death, Aispuro-Camacho was fired from the IRS for other reasons.

Aispuro-Camacho ultimately confessed to the crime when confronted by agents. Aispuro-Camacho explained that she had been prescribed the morphine and that she sold it to make a few thousand dollars in extra spending money. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

2 U.S. Navy Sailors Arrested For National Security Reasons Relating To China - August 3, 2023

The Department of Justice arrested two U.S. Navy sailors on national security charges relating to China. Ut is unclear whether the two cases are connected in any way.

The first sailor, a 22 year old Petty Officer assigned to a Navy vessel in San Diego. He was arrested on an espionage charge relating to a conspiracy to share intelligence with a Chinese official.

The Petty Officer who served as a Construction Engineer, is charged with conspiring with a PRC Intelligence Officer to collect and transmit sensitive military information about naval operations. The Petty Officer allegedly accepted bribes and gave the PRC intelligence officer photographs and videos of military exercise plans, operational orders and electrical systems.

The second sailor, based near Los Angeles, is charged with conspiracy and receipt of a bribe from a Chinese official. The sailor faces charges for espionage and for violating export control laws, for collecting and transmitting sensitive national defense information at the direction of a PRC Intelligence Officer. As tasked by the PRC Intelligence Officer, the sailor allegedly transmitted or attempted to transmit more than 50 manuals and other documents containing technical and mechanical data about naval amphibious assault ships Several of these materials were allegedly marked with export control warnings and contained details about the power structure, weapons systems and damage control aboard those ships. (Source)

Former Army Reservist Pleads Guilty To Stealing $15,000 Of Government Funds - August 23, 2023

United States Army Reservist Derrick Branch pled guilty to conspiracy to commit theft of government funds Branch stole $15,469.30 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Police Officer Sentenced To Prison For Accepting $16,000 In Bribes For Firearms Training Certifications - August 18, 2023

William Johnson joined the Baltimore County Police Department and later obtained a qualified handgun instructor certificate from the Maryland State Police.

From May 2019 through September 2021, Johnson solicited and accepted at least $16, 084 in bribes and kickbacks from applicants seeking certain licenses in exchange for Johnson falsely certifying to the Maryland State Police that the applicant had completed the training required by law.

In conversations with the applicants, Johnson made clear that once they paid the money, Johnson would send them the required documentation and they did not need to attend the required classes. (Source)

Former Police Department Lieutenant Charged For Overtime Fraud Scheme - August 25, 2023

Jeffrey Peters (Lieutenant) and a fellow Shreveport Police Department (SPD) Officer fraudulently obtained money by creating and submitting falsified Reports of Overtime to the SPD. These falsified reports stated that Peters had worked overtime hours for the SPD.

The Officer would submit falsified Reports of Overtime to the SPD which Peters would approve as his supervisor. Peters also created and submitted Activity Reports to the SPD which falsely claimed that Peters and the Officer were working assignments together in Shreveport's Police District and the surrounding area, which area included the SPD Headquarters. It is alleged that Peters himself submitted in excess of 50 false reports for overtime.

The indictment further alleges that while Peters was claiming overtime, he was actually not working and was instead at various bars and restaurants. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Housing Authority Director, His Chief Assistant & Contractor Charged For $76,000+ Bribe / $2.5 Million Fraud Schemes - August 29, 2023

Norman Wise, Douglas Daniel and Leonard Coleman were charged with bribery and fraud charges for two schemes: (1) A bribery scheme in which Coleman paid off Wise and Daniel in exchange for contracting work awarded to Coleman at the Chester Housing Authority (CHA). (2) A fraud scheme in which Wise and Daniel created a contracting company that they used to fraudulently bill the CHA and obtain hundreds of thousands of dollars in proceeds. During the time they engaged in these offenses, Wise was the Director of Public Housing for the Chester Housing Authority and Daniel was the Housing Program Manager and Wise's chief assistant.

From July 2014 through March 2022, defendant Coleman made bribe payments separately to Wise and Daniel in exchange for CHA contracting work awarded to his company, Coleman's Contracting. To generate these bribe payments, Wise and Daniel inflated the amount charged on invoices that Coleman submitted to the CHA for work he performed for the CHA. Wise and Daniel then ensured that the CHA paid Coleman on the inflated invoices, and Coleman paid Wise and Daniel bribes in amounts covered by the inflated invoices. Coleman made these payments by depositing funds directly into the personal bank accounts of Wise and Daniel. In total, Coleman made approximately $76,400 in bribe payments to Wise and Daniel around the time that Coleman received approximately $2.5 Million in revenue from the CHA. (Source)

Former Manager For Registry of Motor Vehicles Sentenced To Prison For Accepting $1,200 In BribesTo Pass Individuals Who Took Driver Permit Tests - August 8, 2023

Mia Cox-Johnson is a former Manager of the Registry of Motor Vehicles (RMV) Service Center in Brockton, Massachusetts.

Johnson took money in exchange for passing scores on learner's permit tests for both passenger vehicle driver's licenses and Commercial Driver's Licenses (CDLs).

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.

Customers were told to request a paper test instead of taking the test on the RMV computer. Cox-Johnson personally graded these customers' paper tests and gave the applicants passing scores.

On Dec. 28, 2018, Cox-Johnson accepted $1,000 in cash – delivered from a friend on behalf of another individual – in exchange for a passing score for the individual's relative who had failed the passenger vehicle learner's permit test six times when taking it in their native language. Cox-Johnson agreed to score the relative as having passed the permit test regardless of whether they had truly passed. Cox-Johnson did, in fact, pass the relative's test, which was taken on paper in English.

On Oct. 21, 2019, a customer came to the Brockton RMV and took three multiple-choice tests they needed to pass in order to get a commercial learner's permit – a prerequisite to taking the road test for a CDL. Cox-Johnson accepted $200 in cash from an individual to score the customer as having passed the tests even if they did not actually pass. In fact, the applicant failed one of the tests, but Cox-Johnson falsely gave the applicant a passing score. (Source)

Former Amtrak Contract Employee Pleads Guilty To $311,000 Timecard Kickback Scheme Involving 2 Other Co-Conspirators - August 10, 2023

Edel Acanda, 40 pleaded guilty to one count of theft of government funds for his role in a kickback scheme involving contractor employees providing services for Amtrak.

2 other defendants pleaded guilty to conspiracy to commit wire fraud for their roles in the kickback scheme. Bryan De Castro Palomino and Jean Barbier.

De Castro Palomino, Barbier, and Acanda were employees at a company that had a federal government contract with Amtrak.

From 2018 to 2020, De Castro Palomino, who was the Warehouse Manager, inflated Acanda and Barbier's timecards to falsely reflect that Acanda and Barbier worked hours that they did not work. In exchange, Acanda and Barbier sent De Castro Palomino part of their paychecks. De Castro Palomino received $77,966 in exchange for his services to fraudulently edit Acanda and Barbier's timecards.

De Castro Palomino admitted that he is responsible for $155,929 in restitution to Amtrak. Acanda admitted that he is responsible for $81,114 in restitution to Amtrak. Barbier admitted that he is responsible for $74,414 in restitution to Amtrak. (Source)

Former Tennessee State Senator And Co-Conspirator Sentenced To Prison For Campaign Finance Scheme - August 11, 2023

Former Tennessee State Senator and practicing attorney Brian Kelsey was sentenced today to one year and nine months in prison, followed by three years of supervised release, for violating campaign finance laws and conspiring to defraud the Federal Election Commission (FEC) as part of a scheme to benefit his 2016 campaign for U.S. Congress.

Kelsey secretly and unlawfully funneled money from multiple sources, including his own Tennessee State Senate campaign committee, to his federal campaign committee. To carry out the scheme, Kelsey conspired with others, including Joshua Smith, who owned a members-only social club in Nashville, of which Kelsey was a member, and controlled a Tennessee political action committee affiliated with the club.

Kelsey, Smith, and others caused a national political organization to make illegal and excessive contributions to Kelsey's federal campaign committee by secretly coordinating with the organization on advertisements supporting Kelsey's federal candidacy, which caused false reports of contributions and expenditures to be filed with the FEC.

Kelsey and his co-conspirators orchestrated the concealed movement of $91,000 – $66,000 of which came from Kelsey's State Senate campaign committee, and $25,000 of which came from a nonprofit corporation that publicly advocated on legal justice issues – to a national political organization for the purpose of funding advertisements that urged voters to support Kelsey in the August 2016 primary election.

Kelsey and his co-conspirators also caused the political organization to make $80,000 worth of contributions to Kelsey's federal campaign committee in the form of coordinated expenditures. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former School Principal Charged With Misusing Nearly $40,000 In School Funds For Vacations With Friends - August 1, 2023

Naia Wilson is the former Principal for New Mission School in Hyde Park, Massachusetts. Wilson was employed as Head of School for New Mission School from 2006 until about June of 2019

Wilson has been charged with one count of wire fraud for allegedly engaging in a scheme to defraud Boston Public Schools of approximately $38,806 by misusing school funds for her own personal use.

Beginning in September of 2016 and continuing until May of 2019, Wilson allegedly requested checks from the external fiscal agent school account to be issued in the name of other individuals, fraudulently endorsed those checks to herself and then deposited them into her own bank account without the nominee ever knowing or authorizing her to do so.

Wilson allegedly requested checks from the external fiscal agent that were used to pay for two all-inclusive personal vacations to Barbados for Wilson and her friends in 2016 and 2018. For both the 2016 and 2018 Barbados trips, Wilson requested that the external fiscal agent issue checks payable to other people who went on the trips and then converted that money to pay for the all-inclusive hotel and airfare. Wilson also fraudulently endorsed the checks used to pay for the 2018 trip. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

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

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

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

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

Former Credit Union President Sentenced To Prison For Embezzling $254,000+ - August 1, 2023

Tara Kewalis was the President and Chief Executive Officer of Skyline Financial Federal Credit Union located in Waterbury, Connecticut.

From approximately September 2016 until her employment was terminated in March 2021, Kewalis used her position to access the credit union's accounting system to create fraudulent accounts, make fraudulent entries, and steal $254,532 in credit union funds. (Source)

Former Bank Teller Pleads Guilty To Stealing $87,000+ From Funds Deposited By Convenience Store - August 23, 2023

Kayla Evans worked as a teller for the Synovus Bank, where a local convenience store kept its account. An auditor for the store began noticing substantial discrepancies between the amount of cash presented to the bank for deposit compared to the amount credited to the store and worked with the bank to determine the cause.

A subsequent investigation found that from July 2019 through February 2021, Evans personally handled the store's deposits, frequently skimming large amounts of cash for her personal use from the amount presented and crediting a smaller deposit to the store. In total, Evans stole approximately $87,748 from the convenience store's deposits. As part of her plea, Evans agrees to pay restitution for the full loss caused by her criminal conduct, and to never seek employment in any financial institution. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

2 Former Tesla Employees Accused Of Leaking Data On 75,000+ Employees To Foreign Media Outlet - August 19, 2023

The Maine Attorney General's Office announced the data breach in an advisory notice published on its website.

The 2 former Tesla employees are accused of mishandling employee data, accidentally leaking over 75,000 individuals' information to a foreign media outlet.

A foreign media outlet (Handelsblatt) informed Tesla on May 10, 2023 that it had obtained Tesla confidential information. The investigation revealed that 2 former Tesla employees misappropriated the information in violation of Tesla's IT security and data protection policies and shared it with the media outlet, Tesla wrote in its initial report of the incident.

Handelsblatt stated that it does not intend to publish the personal information, and in any event, is legally prohibited from using it inappropriately.

Tesla immediately took steps to contain the incident. Tesla identified and filed lawsuits against the 2 former employees, These lawsuits resulted in the seizure of the former employees' electronic devices that were believed to have contained the Tesla information. (Source)

New York Nick's Allege Former Employee Stole Trade Secrets - August 22, 2023

The New York Knicks sued the Toronto Raptors, their new head coach and a former Knicks scouting employee, saying the defendants conspired to steal thousands of videos and other scouting secrets over the past few weeks.

The Knicks said the theft occurred in recent weeks after the Raptors hired and recruited a mole within the Knicks organization.

The lawsuit identified him as Ikechukwu Azotam, who since August 2021 had directed the planning, organizing and distribution of all video scouting responsibilities for the Knicks coaching staff.

They blamed Raptors head coach Darko Rajakovic, hired in June, along with player development coach Noah Lewis, the Raptors' parent company - Maple Leaf Sports & Entertainment Limited - and 10 unidentified Raptors employees, saying that they received propriety information and sometimes directed Azotam to misuse his access to Knicks information.

In June, the Raptors began recruiting Azotam to assist their novice head coach in assembling a new coaching and video operations staff.

Azotam notified the Knicks in late July that he was leaving. His final day was Aug. 14, and the Knicks' security team identified the theft last Tuesday

In early August, Azotam began to illegally convert and misappropriate the Knicks' confidential and proprietary data, the lawsuit said. On Aug. 11, he sent two emails from his Knicks email address to his new Raptors email address containing "proprietary information with highly confidential material. (Source)

CHINESE ESPIONAGE TARGETING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES
No Incidents To Report

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

Hospital Nurse Found Guilty Of Murdering 7 Babies In Neonatal Unit - August 18, 2023

The nurse who led "a campaign of violence" and enjoyed "playing God" has been found guilty of murdering 7 at a hospital.

Lucy Letby was also convicted of trying to kill 6 other babies at the Countess of Chester Hospital's Neonatal Unit in England, during a yearlong killing spree between June 2015 and June 2016.

Letby was variously accused of "getting a thrill" out of murdering babies and killing one infant because she wanted to get the attention of a doctor she had a crush on.

Prosecutors described her as an "opportunist" who had targeted sick children while she was alone with them and used their vulnerabilities to "camouflage" her attacks, which had "patterns" or similarities.

A "confession" Post-it note, found by police at her home, read, "I don't deserve to live. I killed them on purpose because I'm not good enough to care for them." She added, "I am a horrible evil person" and: "I AM EVIL I DID THIS."

WARNING: The complete details about this incident on this below are very distributing. (Source)

Chiropractic Clinic Employees Sentenced For Roles In $3.5 Million+ Disability Fraud Scheme - August 17, 2023

Clarissa Pogue and Christina Barrera were convicted by a jury in U.S. District Court in St. Louis of one felony count of conspiracy to defraud the Social Security Administration, along with Chiropractor Vivian Carbone-Hobbs. Carbone-Hobbs was also convicted of 10 counts of health care fraud and two counts of theft of money from the United States. Pogue was also convicted of one count of theft of money from the United States.

The three conspired with Thomas G. Hobbs, Carbone-Hobbs' husband, and others to fraudulently obtain disability payments for patients who were not disabled or injured.

Thomas Hobbs admitted that beginning in 2011, he fraudulently assisted patients in receiving more than $3.5 Million in disability benefit payments through the Social Security Administration's Disability Trust Fund and through private disability benefit insurance providers.

Hobbs charged patients thousands of dollars in exchange for the preparation of disability forms. He also coached patients in how to lie to the Social Security Administration and private insurers about their ability to perform basic activities like lifting things, sitting, standing and walking. Patients also had to pay hundreds of dollars for annual appointments to keep qualifying for disability payments. (Source)

Former Employee Of Family Services Organization Found Guilty Of $483,000+ Of Fraudulent Medicaid Billing Practices - August 3, 2023

Eric King is a former employee of Eye For Change Youth and Family Services, Inc., a non-profit corporation in Cleveland, Ohio.

From June 2018 through May 2021, King defrauded Medicaid by causing Medicaid to be billed for services not actually performed or for services that were not actually performed for the amount of time the billing codes reflected; for falsifying progress notes into Medicaid beneficiary electronic records; for creating false progress notes; and for using the identities of clients without authorization to bill Medicaid.

As a result of King's conduct, Medicaid paid over $483,000 for fraudulent billings. King is scheduled to be sentenced on November 15, 2023. (Source)

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

Furniture Company Employee Pleads Guilty To Embezzling $27 Million+ From Employer - August 30, 2023

Yi He was a long-time and trusted employee of a furniture company that provides furniture to retailers like Wayfair, Overstock, Kohls, Walmart and Ashley. Yi was solely responsible for payroll and payroll tax-related duties for the company.

From 2018 until 2022, Yi embezzled money from the company's bank account into his own personal and financial investment accounts. Yi submitted false and fraudulent bank and financial statements to the company's leadership to remain undetected.

For example, in one wire transfer in February 2022, Yi wired himself $100,000. Yi falsified that month's bank account statement by removing the transaction entirely.

In total, Yi stole $26.5 million from the company.

Yi also helped oversee an employee incentive LLC that rewarded company employees with 10 or more years of service. The LLC offered employees a way to earn more and supplement retirement. Yi similarly embezzled from the LLC's bank accounts. For example, in one wire transfer in April 2022, he paid himself $200,000 by falsely categorizing the transfer as "Rent." In total, he stole $635,000 from the LLC.

Yi will pay more than $27 million in restitution to the furniture company and LLC, and he will forfeit two homes in Reynoldsburg and one home in Columbus. (Source)

Former Auditor For Commercial Real Estate Agency Pleads Guilty To Embezzling $2.7 Million+ Over 10 Years - August 21, 2023

From 2008 to January 2022, Varun Aggarwal worked in the Internal Auditing Department of the Newport Beach-based KBS Realty Advisors and rose to the level of the department's director.
Beginning at least as early as January 2012 and continuing until January 2022, Aggarwal used his position at KBS to embezzle his employer's money.

As a member of the company's internal auditing group, Aggarwal was familiar with KBS's policies and procedures for payments to vendors. Aggarwal used his knowledge of KBS's policies and procedures to have his friends and family serve as approved vendors to do contracting work for KBS.

After several of these companies became approved vendors for KBS, Aggarwal used these approved vendors to submit fraudulent invoices for consulting services that were not performed for the company.

He then funneled the payments on the invoices from KBS to his own bank accounts, through the approved vendors, at times without informing the vendors that the invoices and the payments on the invoices were for his own benefit.

Aggarwal fraudulently obtained approximately $2,729,718 from KBS that he caused it to pay to the approved vendors that ultimately went to himself. Aggarwal resigned from KBS in January 2022 after the company began investigating the invoices, according to court documents. (Source)

Senior Vice President of Finance Charged With Embezzling $2.7 Million+ Company - August 25, 2023

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

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

Former Bookkeeper Sentenced To Prison For $2 Million+ Wire Fraud Scheme Over 7 Years - August 22, 2023

Christina Joyner worked for 25 years as a Bookkeeper for Quanz Motor Car Company, doing business as Quanz Auto Body.

From approximately July 2014 through September 2021, Joyner used her position as bookkeeper to defraud the company of over $2 Million.

Joyner accomplished this by issuing checks to herself and coding them to give the appearance they were for legitimate business expenses, using company credit cards to make personal, online purchases, retaining money from cash transactions and creating fraudulent pay stubs for her husband that were used as proof of income to obtain loans. Joyner maintained email reminders to herself to modify entries in the accounting software and manipulated the software to conceal her actions. (Source)

Law Firm Office Manager Charged With Embezzling $1.1 Million+ From Law Firm - August 8, 2023

Jairo Santos worked as the Office Manager for his law firm.

Between March 9, 2016, and February 2023, Jairo Santos allegedly deposited approximately 806 unauthorized checks from the victim law firm made payable to Santos into his personal checking accounts. The total value of these unauthorized deposits was approximately $1,191,683. Further, as part of the scheme to defraud, Santos made and deleted entries in the general ledger for the victim law firm that concealed the fact that the payments were made for Santos's own use. The indictment further alleges that Santos deposited these checks from the victim law firm knowing that the payments were not authorized by the firm or its senior partner and knowing that they exceeded the amounts he was legitimately owed by the firm for his salary and expenses. (Source)

Contractor Employee Charged With Embezzling $900,000+ From Employer - August 16, 2023

According to allegations in the indictment, from 2016 to 2021, Michelle Wilshire was employed by a family-owned business identified in court documents as Company A. During the relevant time, Wilshire was in charge of Company A's Comdata account, a third-party payment processing and debit card issuing service, which Company A used for fleet management and payment services for its drivers.

Wilshire executed a scheme to defraud her employer by issuing multiple Comdata prepaid debit cards in her name and in the names of other individuals, including former employees, fictitious employees, and current employees who were not aware the cards existed. Wilshire allegedly caused Comdata to load funds onto the prepaid debit cards, which the defendant then withdrew via ATM cash withdrawals. Between November 2017, and July 2021, Wilshire allegedly withdrew more than $528,000 from prepaid Comdata debit cards.

In addition to the debit card scheme, Wilshire allegedly embezzled Company A's funds by using Comdata's Comchek and Comchek Mobile services to issue checks in the defendant's name and to make multiple wire transfers into Wilshire's personal bank account, totaling over $315,000. Wilshire also allegedly caused more than $58,000 of Company A's funds to be transferred through Comdata into the bank account of a former company employee. (Source)

Former Manager For Oil Trading Company Charged In International $600,000 Bribery Scheme - August 21, 2023

Javier Aguilar was a former Manager and Oil Trader for Vitol Inc., the U.S. affiliate of the Vitol group of companies which together form one of the largest energy trading firms in the world.

Between August 2017 and July 2020, Aguilar and others knowingly, willfully and corruptly offered and paid bribes to and for the benefit of Mexican officials. He allegedly intended to obtain and retain business for Vitol related to Petróleos Mexicanos (PEMEX), a state-owned oil company of Mexico, and PPI, a wholly-owned and controlled subsidiary of PEMEX with its principal place of business in Houston.

Aguilar met with procurement managers at PPI between September 2017 and April 2018 and agreed to pay bribes for confidential, inside information to assist Vitol in winning business from PPI, including a contract to supply ethane to PEMEX through PPI. In particular, Aguilar allegedly agreed to make payments totaling approximately $600,000 in order to assist Vitol in winning the ethane contract.

To promote the bribery scheme and to conceal the proceeds derived from it, Aguilar and his co-conspirators caused the bribes to be paid through a series of transactions and shell companies, according to the charges. (Source)

Bookkeeper For Housing And Redevelopment Authority Program Sentenced To Prison For Embezzling $200,000+ Public Housing Rent Payments - August 11, 2023

Between January 2010 and July 18, 2018, Marcie Thumann worked as a Bookkeeper for the Albert Lea Housing and Redevelopment Authority (HRA), a government program that received both federal and state funding to remedy the shortage of available low-incoming housing units. Thumann, who was responsible for recording and reconciling payments to the HRA, received tenants' rent payments via cash, check, or money order.

During her tenure as the HRA's bookkeeper, Thumann routinely embezzled HRA rent payments for her own personal use and benefit. She did so by pocketing cash payments and altering the payee information on payments made by check and money order.

Thumann then manipulated the HRA's computer system to conceal the money she stole, avoid detection, and prolong her fraud scheme. In total, Thumann stole at least $213,217 from the Albert Lea HRA.(Source)

Puerto Rico Mayor Sentenced To Prison For Accepting $27,000 In Bribes For Awarding Contracts - August 22, 2023

From 2021 until 2022, Reinaldo Vargas-Rodríguez, was the Mayor and highest-ranking government official in the municipality of Humacao.

Starting in 2021, Vargas-Rodríguez was involved in a bribery conspiracy in which he received and accepted cash payments from two businessmen in exchange for awarding municipal contracts for waste disposal services, asphalt and paving services, and debris removal, and paying outstanding invoices on the contracts.

Vargas-Rodríguez received at least $27,000 in cash bribes from January 2021 through July 2021 from the two businessmen. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

CEO Of Company Embezzled $4 Million+ To Pay For Various Personal & Relatives Expenses - August 9, 2023

Between 2010 and 2017, Gerhard Bauer was the CEO and President of a U.S. subsidiary company.

He embezzled more than $4 Million by writing corporate checks to pay various personal expenses. He also created fake invoices to justify the expenses. He paid over $1,490,000 for the construction of his Virginia farm, winery, and horse ranch. He also paid over $146,000 for private school tuition for his relatives. (Source)

Former Employee For On-line Used Car Retailer Charged For $2 Million+ Embezzlement Scheme / Used Funds For Lavish Lifestyle (Cars, Travel, Etc.) - August 24, 2023

John Whisenant worked in a variety of roles at an online used car sales company beginning in October 2018. About a year after he began with the company, Whisenant was promoted into a role where he had access to the company bank accounts and accounting software.

Beginning in about June 2019 and continuing until November 2021, Whisenant used his access to make 57 wire transfers totaling over $2 Million into accounts he controlled. Whisenant disguised the transfers as legitimate business expenses in the company's accounting software with a variety of false entries.

Whisenant used the money for a lavish lifestyle. He bought luxury automobiles such Porches and Mercedes. He spent $123,096 for a 2022 Audi E-Tron and bought a $98,100 Tesla. He rented luxury homes in Southern California and purchased two airline tickets to Paris at a cost of nearly $23,000 each. (Source)

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

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

Khosropanah held senior positions at a Richmond-based company that operates convenience stores across the country.

His role focused on information technology, and he was responsible for purchasing computers and other electronics for the company. Upon receiving invoices for certain purchases, Khosropanah made unauthorized material modifications to the invoices before submitting them to his accounting department for approval.

Through these modifications, Khosropanah was able to misappropriate computers and electronics and conceal his misappropriations. He then sold the misappropriated assets on eBay and to a third-party wholesaler without the knowledge or consent of his employer. The defendant sold approximately 850 laptops and other electronics, causing a loss of over $1.9 Million to his employer. Khosropanah used the proceeds from the fraudulent sales to purchase luxury cars, including a Ferrari. (Source)

Law Firm Financial Controller Defrauds Firm Out Of $1.5 Million By Inflating Salary Over 3 Years - August 23, 2023

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

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

Home Health Aide Agency Employee Convicted Of $500,000+ Of Identity Theft Fraud To Purchase New / Used Vehicles - August 24, 2023

Aisladys Diaz was a private duty health aide who worked with a home health aide agency. The agency provided home health aides to residents at senior communities in Miami-Dade County.

From May to June 2020, Aisladys Diaz stole the personal identifiable information of two elderly residents under her care.

Aisladys Diaz then shared the information with her daughter, Ailensy Buron Diaz, Berto Omar Rodriguez Fonseca, a finance manager at a car dealership in Miami Lakes, and others who used the information to purchase numerous new and used vehicles at car dealerships, at a cost totaling over $500,000, and apply for credit cards, an Economic Disaster Injury Disaster Loan (EIDL), and a Small Business Administration (SBA) loan under the Coronavirus Aid, Relief, and Economic Security (CARES) Act. (Source)

Former Realty Company Employee Sentenced To Prison For Embezzling $487,000 For Personal Use - August 11, 2023

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

From about Jan. 8, 2018 to Dec. 9, 2020, Hendrix sent over 140 payments totaling approximately $483,037 to her own bank account. Hendrix used the money at restaurants and to buy a vehicle, her plea agreement says. (Source)

Former Labor Union President Sentenced To Prison For Embezzling $200,000+ / Used Funds For Gambling & Personal Expenses - August 4, 2023

Byron Clemons is the former President of the Alton chapter of the AFSCME Labor Union.

Clemons withdrew a total of $202,100 from the Local 124's U.S. Bank account from February 2021 to January 2022. The defendant used the funds to gamble at casinos and pay personal expenses. (Source)

Former Islamic Center Director Sentenced To Prison For Embezzling $82,000+ To Pay For Persoanl Expenses - August 10, 2023

From at least 2009 until March 2019, Ahmed Ahmed was employed as the Director of the Ibn Taymiyah Masjid and Islamic Center (ITMIC) on Mock Road in Columbus, Ohio.

During his tenure as director, Ahmed used his position of trust to embezzle funds from the religious organization. Specifically, Ahmed wrote unauthorized checks from ITMIC's accounts to himself.

Each year from 2015 through 2018, Ahmed increased the amount he embezzled, writing himself $4,500 in checks in 2015; approximately $11,000 in checks in 2016; $12,900 in checks in 2017; and approximately $21,000 in checks in 2018.

Ahmed spent thousands of dollars of ITMIC funds to pay his own personal credit card bill and towards the purchase of his own personal vehicle.

Ahmed also defrauded the Columbus Metropolitan Housing Authority's housing choice voucher program. From 2014 until at least 2020, Ahmed submitted false claims to obtain housing subsidies he would not otherwise qualify for given his true income and assets.

Finally, Ahmed fraudulently applied for Pandemic Unemployment Assistance nine times from August until October 2020. During that same time frame, Ahmed generated at least $4,000 in revenue by producing and posting approximately 126 YouTube videos to his YouTube channel. Ahmed will pay more than $82,000 in total restitution. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

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

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

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

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

She then transferred the bulk of the money for her own use. Becoming more brazen, between August and November 2021, Guillory transferred $247,000 directly from company accounts to her own bank accounts.

Again, she made fraudulent accounting entries and reused legitimate invoices to make it appear the payments were for appropriate business purposes. In all, Guillory made at least 867 secret transactions using interstate wires that totaled $2,536,086.

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

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

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

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

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

Sickels fraudulently acquired equipment through false representations to PSU ODA that the equipment was necessary to upgrade, replace, or maintain PSU ODA servers, when, in fact, Sickels knew that the equipment was not necessary. Sickels subsequently sold the equipment for his personal benefit to third parties.

The scheme lasted from approximately 2005 to 2017, in Centre and Mifflin Counties. Sickels was also ordered to pay $267,264.87 in restitution. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Former University Financial Advisor Sentenced To Prison For $5.6+ Million Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

From about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland.

He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee. As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied.

Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Nurse Pleads Guilty To Drug Diversion From Hospital - August 4, 2023

According to admissions made in connection with her guilty plea, beginning in May 2019, Andrea Falzano used her capacity as a Nurse in the emergency department at a Massachusetts based hospital to withdraw controlled substances from a locked drug cabinet.

These substances included morphine, fentanyl, and hydromorphone, all of which are opioids and Schedule II controlled substances. In total, Falzano withdrew these substances 412 times for 299 already discharged patients over an approximately five-month period. (Source)

Nurse Practitioner Pleads Guilty To Unlawful Drug Distribution - August 11, 2023

Danielle Simonson admitted that from at least January 2020 through October 2022, she unlawfully prescribed controlled substances to a total of 54 patients. These included prescriptions for the opioids Hydrocodone and Oxycodone, Benzodiazepines (Clonazepam, Diazepam, Lorazepam), and Amphetamine. Simonson admitted that she issued a total of 63 oxycodone prescriptions to two residents without treating either of them for a medical condition. The Suffolk County residents usually paid Simonson by mailing her packages of cash.

In the civil settlement agreement, Simonson admitted that she improperly prescribed controlled substances to 105 patients (including the 54 listed in her criminal plea agreement), often without ever examining patients and maintaining medical records justifying her decision to prescribe controlled substances. Simonson agreed to pay $200,000 to settle claims that the United States could have brought against her pursuant to the Controlled Substances Act. (Source)

Hospital Nurse Pleads Guilty To Stealing Controlled Substances From Hospital - August 31, 2023

Morgan Miralles admitted that she diverted the controlled substances that were supposed to be dispensed to patients, for her own personal use by falsifying documents, including the omission of information on required log entries tracking the disbursement of controlled substances. She stole fentanyl, morphine, hydromorphone, and hydrocodone. (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'

Employee Charged With Attempted Murder Of Co-Worker With Hammer - Resulting In Skull Fractures, Brain Bleeds, Broken Jaw, Missing Teeth - August 30, 2023

Austin Hahn allegedly strolled over to his friend and bludgeoned him from behind with a tinner hammer before 7:30 a.m. on Aug. 20 at the Bright Sheet Metal Co. in Indianapolis.

He then left the warehouse and calmly tossed the hammer in the trash in front of an employee who was outside and unaware of the altercation. As Hahn walked by the co-worker, he allegedly paused, patted him on the chest and said, "S--- happens". Hahn then climbed into his car and drove to his mother's house.

Responding officers arrived to find the victim with skull fractures, brain bleeds, a broken jaw and missing teeth.

Hahn's colleagues told police that he and the victim were "the best of friends" before a dispute occurred several weeks ago. But Hahn had apologized, and they thought the bad feeling had been quelled. (Source)

U.S. Postal Service Employee Charged With Stabbing A Supervisor At Postal Facility - September 1, 2023

Edwin Cuadrado is a U.S. Postal Service (USPS) employee.

According to the criminal complaint, Cuadrado first engaged in a verbal and physical altercation with one of his USPS supervisors at a nearby gas station late in the afternoon on August 25. Shortly thereafter, Cuadrado drove his USPS vehicle into the main employee parking lot of the USPS mail processing and distribution facility. While in the parking lot of that facility, three different supervisory USPS employees attempted to speak with Cuadrado regarding the recent altercation. Cuadrado responded by brandishing a knife and stabbing one of the supervisors before leaving the scene. Responding paramedics treated the wound to the back of the supervisor's head before that supervisor was taken to a hospital for further treatment. (Source)

Kentucky Fried Chicken Employee Charged After Shooting Customer In Parking Lot - August 11, 2023

A 23-year-old Kentucky Fried Chicken (KFC) employee is accused of shooting and injuring a woman outside the fast-food restaurant.

Savannah Police Chief Lenny Gunther said during a news conference that the suspect, Sherman Hendrix, allegedly shot and injured a woman during the popular fast-food chain's lunchtime rush. Gunther called the shooting, "not random," but did not share what led up to the altercation. (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)

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

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

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

The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. (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 / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,600+ 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

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

The NITSIG had to suspend meetings and the ITS&E in 2020 to 2022 due to the COVID outbreak. We are working on resuming meetings in the later part of 2023, and looking at holding the ITS&E in 2024.

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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