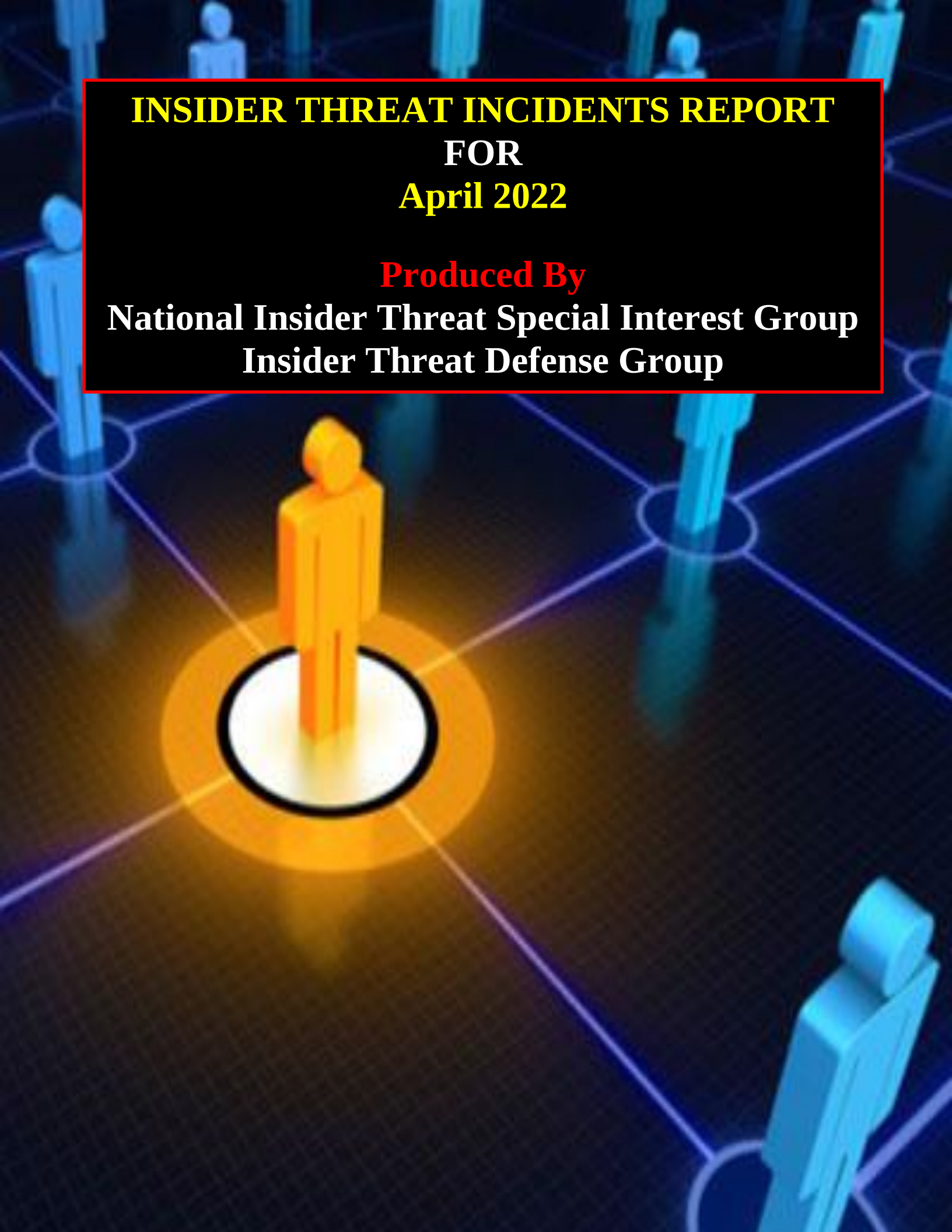


INSIDER THREAT INCIDENTS REPORT
FOR
April 2022

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **3,600+** 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 2020 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

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

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

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 26 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

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

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

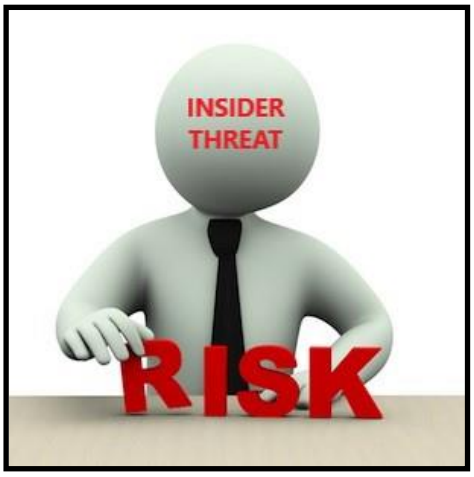
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR APRIL 2022

U.S. GOVERNMENT

4 WHITE HOUSE SECRET SERVICE AGENTS PLACED ON ADMINISTRATIVE LEAVE FOR ROLE IN BRIBERY SCHEME CARREID OUT BY DHS IMPOSTER LAW ENFORCEMENT AGENTS - April 8, 2022

4 Secret Service agents were entangled in an alleged bribery scheme carried out by 2 men masquerading as DHS law enforcement agents. One of the Secret Service agents involved in the bribery scheme was a special agent assigned to First Lady Jill Biden's protective detail. Another was a Uniformed Division Officer at the White House.

Another Secret Service special agent involved in the bribery is assigned to President Biden's detail. A second Uniformed Division officer caught up in the scheme was assigned to protect Vice President Harris's residence.

Both DHS imposter law enforcement agents are U.S. citizens hold passports with visa's to Iran and Pakistan. The 2 men charged with impersonating DHS agents are Arian Taherzadeh and Haider Ali.

Taherzadah offered to give an assault rifle worth $2,000 to the Secret Service agent assigned to Jill Biden. Taherzadeh is also accused of giving members of the Secret Service, as well as a legitimate DHS employee, rent-free apartments, iPhones, surveillance systems, a drone, a flat-screen television, a case for storing an assault rifle, a generator and law enforcement paraphernalia. One of the agents who received the free rent and additional gifts is the Uniformed Division officer assigned to the White House.

The 2 DHS imposters appeared to have targeted the apartment complex, which is home to several law enforcement employees, including many Secret Service and DHS employees. Taherzadeh and Ali seemed to have control of five apartments. When investigators searched the defendants' apartments, they found a drone, handguns, ammunition, bullet-proof body armor, gas masks, zip ties, handheld radios, body cameras, binoculars, a high-powered telescope, and four laptop computers. They also discovered what appeared to be official DHS patches and training manuals, scopes for weapons, components of disassembled rifles, and a list of every resident of the apartment complex. (Source)

UPDATE:

Federal Judge Rejects Detention Of Law Enforcement Imposters - States There Is No Evidence Of Nefarious Effort To Infiltrate Secret Service- April 12, 2022

A federal magistrate rejected prosecutors' request to detain accused law enforcement imposters who compromised Secret Service members, saying there is no evidence that the two pose a national security risk or made a "nefarious" attempt to infiltrate the Secret Service.

The magistrate noted that the owners of an upscale downtown apartment complex where the two suspects allegedly controlled five apartment units had obtained judgements against the suspects for thousands of dollars in unpaid rent.

The judge said there was no "reliable evidence" that a foreign government had provided financing or was supporting the suspects and their outreach to the Secret Service. (Source)

Former Congressional Staffer Pleads Guilty To Theft Of $79,000+ By Inflating Salary & Bonus Payments - March 7, 2022

Sterling Carter was employed as the Director of Operations by a Member of Congress. In that position, Carter was responsible for managing the office's budget and processing payroll and bonus payments for all employees in the office.

Between November 2019 and January 2021, Carter submitted fraudulent paperwork which purported to authorize a higher salary and bonus payments for himself. Carter concealed this theft from the Congressperson and the office's Chief of Staff by falsely representing, in both communications and a budget spreadsheet, that he was only being paid what he was legitimately owed. In total, Carter received $79,491.67 in unauthorized salary and bonus payments. (Source)

Former State Department Employee Sentenced To Prison For Providing Confidential Bidding Information To Bidder And Received $60,000 Kickback Payments in Return - April 8, 2022

May Salehi was a former State Department employee.

Salehi was involved in evaluating bids for critical overseas government construction projects such as U.S. embassies and consulates. Salehi gave confidential inside bidding information to a government contractor, and received $60,000 in kickback payments in return. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

2 Air Force Officers Charged For Theft In Scheme To Steal U.S. Air Force Ammunition - April 27, 2022

United States Air Force Staff Sergeants John Sanger and Eric Eagleton and others engaged in a conspiracy in March 2022 to steal ammunition belonging to the United States Government.

As part of the scheme, Sanger, Eagleton, and their conspirators are alleged to have stolen thousands of rounds of U.S. Air Force ammunition. They also falsified records at Fairchild Air Force Base to conceal the theft. (Source)

Former DHS Employee Convicted For Theft Of Proprietary Software & Sensitive Databases From U.S. Government With Help Other DHS Co-Conspirators - April 11, 2022

A former Acting Branch Chief of the Information Technology Division of the U.S. Department of Homeland Security (DHS-OIG) was convicted of multiple federal charges stemming from the theft of proprietary software and sensitive databases from the U.S. government.

Murali Venkata along with co-conspirators Charles K. Edwards, who previously served as the Acting Inspector General of DHS-OIG, and Sonal Patel, another official at DHS-OIG, executed a scheme to steal confidential and proprietary software from the government along with the personally identifying information (PII) of hundreds of thousands of federal employees.

Venkata worked for DHS-OIG from June 2010 until he was placed on administrative leave in October 2017 following the charges in this case.

Edwards pleaded guilty in January 2022 and Patel pleaded guilty in April 2019 to stealing property from the U.S. government for the purpose of developing a commercial version of a case management system to be offered for sale to government agencies.

Venkata was convicted for his role in the conspiracy, which included exfiltrating proprietary source code and sensitive databases from DHS-OIG facilities, as well as assisting Edwards in setting up three computer servers in Edwards's residence so that software developers in India could access the servers remotely and develop the commercial version of the case management system. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former Catholic School Principal Pleads Guilty To Embezzling $175,000 From Fund For Student Activities And Services / Used Funds To Qualify For Home Mortgage Loan - April 4, 2022

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

From June 2012 through December 2017, Coates devised a scheme to steal from the school's Home School Association, an organization affiliated with the school that supported student services and activities. As the school principal, Coates had access to the Home School Association's checks and could use her discretion to pay expenditures for only school-related purposes. Coates, however, engaged in a pattern of purchasing personal goods and services with the funds. Over the time period, she wrote approximately 66 unauthorized checks and deposited at least $175,000 into her personal bank account. Among other things, she used the funds to help her qualify for a home-mortgage loan. (Source)

Former State Employee Sentenced To Prison For Role In $2 Million Scheme To Defraud the Office of AIDS - March 7, 2022

Christine Iwamoto was employed by the Office of AIDS within the California Department of Public Health until March 2018. The Office of AIDS is responsible for working on behalf of the State of California to combat the HIV and AIDS epidemic.

Between December 2017 and November 2018, Iwamoto participated in a scheme that was coordinated by Schenelle Flores, also employed at the Office of AIDS, to defraud the Office of AIDS. Flores, Iwamoto, other participants in the scheme, and their families and friends obtained at least $2 million in personal benefits, including cash and purchased items.

Flores directed a state contractor to make payments allegedly on behalf of the Office of AIDS and caused the contractor to charge those payments to the state. Flores caused the contractor to pay for personal expenses on its debit cards, order gift cards for personal use, and pay false invoices to shell companies for services allegedly provided to the Office of AIDS.

Iwamoto set up a shell company and coordinated with Flores to submit invoices to the state contractor. Those invoices falsely claimed that Iwamoto's company had provided various consulting and meeting facilitation services to the Office of AIDS. Iwamoto received $450,000 in payments as a result of the invoices. Iwamoto then gave thousands of dollars in cash and blank checks to another employee of the Office of AIDS who was participating in the scheme. Iwamoto also participated in obtaining the gift cards from the state contractor and received hundreds of the gift cards for her personal use. (Source)

Former Airport Finance Director Pleads Guilty To Theft Of $49,000+ Of Federal Funds - April 19, 2022
Melissa Hall was the airport's Finance Director from September 2017 until January 8, 2021,at the West Virginia Huntington Tri-State Airport. Hall was responsible for accounting, depositing and withdrawing funds from multiple revenue sources including ATMs and vending machines.

Hall admitted that between May 2020 and January 8, 2021, she stopped depositing the full amounts she collected from these machines into the airport's bank accounts and also took money from those accounts intended for deposit in the ATMs. During this time period, Tri-State Airport received at least $10,000 per year in federal funding, which was deposited in its bank accounts. Hall admitted to diverting nearly $49,500. (Source)

Former California Department Of Transportation Manager Pleads Guilty To Bid Rigging & Receiving $800,000+ In Bribes (Cash, Home Remodeling, Etc.) - April 11, 2022
Choon Foo "Keith" Yong was a former contract manager for the California Department of Transportation (Caltrans). He pleaded guilty for his role in a bid-rigging and bribery scheme involving Caltrans improvement and repair contracts.

Yong and his co-conspirators engaged in a conspiracy, from early 2015 through late 2019, to thwart the competitive bidding process for Caltrans contracts to ensure that companies controlled by Yong's co-conspirators submitted the winning bid and would be awarded the contract. Yong received the bribes in the form of cash payments, wine, furniture and remodeling services on his home. The total value of the payments and benefits Yong received exceeded $800,000. (Source)

University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government - April 7, 2022
A former University of Kansas (UOK) professor was convicted by a federal jury on three counts of wire fraud and one count of false statements after he deliberately concealed that he was also employed by a government-affiliated university in the People's Republic of China, while working on U.S. government funded research at UOK. Franklin Tao worked as a full-time professor at UOK.

In 2018, Tao accepted a position with Fuzhou University in China that designated him as a Changjiang Scholar Distinguished Professor. The position's guidelines required him to be a full-time employee of Fuzhou University. The Kansas Board of Regents required faculty to file annual reports to notify of any outside employment that did or could impact duties as a conflict of interest. Tao didn't seek permission from UOK before entering the agreement with Fuzhou University, didn't notify KU about the employment, and lied to conceal the employment. (Source)

Former District Court Accounting Supervisor Pleads Guilty To Embezzling $1 Million+ From Court Over 10 Years - April 19, 2022
Dawna Kellogg was employed in the accounting department at the Johnson County District Court, in Kansas.

As the Accounting Supervisor for the court, Kellogg managed the accounting department, collected funds from each separate county system, recorded funds collected, processed daily reports, and deposited the collected funds into the court's bank account. The court utilized a case management system named the Justice Information Management System (JIMS), which had an accounting function to maintain the court's financial transactions.

Kellogg stole cash that the court received, such as bail bond payments, and either spent or deposited the embezzled proceeds into her personal accounts.

Kellogg agreed to not contest that the total loss resulting from the scheme to defraud was $1,135,988.13, which consists of $359,296.63 from 2007 through 2009 and $776,691.50 from 2010 through June 2017. (Source)

Former Motor Vehicle Administration Employee Pleads Guilty To Role In Scheme To Provide Fraudulent Driver's Licenses To Applicants Who Paid A Fee - April 22, 2022

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

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

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

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Police Officer And Electrical Contractor (His Brother) Charged In $36 Million+ Fraud Scheme - April 29, 2022

Mass Save is a Massachusetts organization that provides residents and businesses financial support and technical services to help save money and use less energy.

Joseph Ponzo, a full-time Boston Police Officer, and his brother, Christopher Ponzo, an owner of an electrical contracting company, conspired to bribe an employee of Mass Save in exchange for the employees assistance in procuring Mass Save contracts.

From 2013 to 2017 the employee of Mass Save was provided $1,000 in cash on a weekly basis, including a John Deere tractor, a computer, home bathroom fixtures and free electrical work, in exchange for the procurement of over $36 million in Mass Save contracts. (Source)

Former Correctional Officer Sentenced To Prison For Smuggling Cell Phones Into Prison For Money - April 5, 2022

Kyle Bower was a correctional officer at Dauphin County Prison in Harrisburg, PA. He agreed to smuggle cell phones into the prison for money on behalf of inmates. Between October 2015 and January 2016, he smuggled phones into the prison for inmates and was paid hundreds of dollars for each phone. (Source)

2 New York City Correction Officers Among 6 Defendants Charged With Conspiring To Accept Bribes & Smuggle Contraband Into Prison For Gang Members - April 5, 2022

6 defendants are charged with conspiring to bribe correction officers employed by the New York City Department of Corrections (DOC) as part of contraband smuggling conspiracies.

Correction Officers Krystle Burrell and Katrina Patterson, and inmates Ashley Medina, Imani Matthews and Terrae Hinds were arrested.

Cell Phones and narcotics were smuggled into the prison for members of the Bloods Gang.

New York City Correction Officer Katrina Patterson accepted at least $34,090 in bribes from Ashley Medina and Imani Matthews on behalf of Michael Ross in exchange for Patterson smuggling contraband into the Robert Davoren Center on Rikers Island for Ross. Ross arranged for the bribes to be sent to Patterson.

New York City Correction Officer Krystle Burrell accepted bribes in exchange for smuggling contraband into the Anna M. Kross Center on Rikers Island for inmate Terrae Hinds, facilitating Hinds' contraband smuggling business and permitting Hinds and others to violate DOC regulations. Hinds, arranged for approximately $9,780 in bribe payments to be sent to Burrell. In exchange, Burrell smuggled at least two unauthorized cell phones to Hinds, and also facilitated Hinds' sale of narcotics and other contraband items at the Anna M. Kross Center. (Source)

Former New York Police Pleads Guilty To $5,000 Bribery Scheme Involving Prostitution Business And Sex Trafficking - April 8, 2022

Wayne Peiffer is a former police officer in Brewster, New York. He pleaded guilty to conspiracy to commit extortion and conspiracy to commit bribery. Peiffer was charged for his role in protecting two Queens-based prostitution businesses from law enforcement when operating in Brewster, in exchange for free sexual services.

From approximately 2010 through October 2018, Peiffer provided protection to members of a prostitution business and a sex trafficking organization that each transported women from Queens to Brewster, New York, for the purposes of engaging in prostitution. Peiffer's protection included advance notice of law enforcement activities and assistance with avoiding detection and apprehension. In exchange, Peiffer directed members of the prostitution business and sex trafficking organization to deliver women to him, including at the Brewster Police Department station, for free sexual services. (Source)

Former Law Firm Paralegal Charged With Embezzling $600,000 From Bankruptcy Estate Funds Over 9 Years - April 21, 2022

Becky Sutton fraudulently embezzled the funds from 2009 to 2018 while working on bankruptcy matters at the law firm.

Sutton orchestrated the fraudulent transfers of bankruptcy funds from fiduciary bank accounts intended for creditors to accounts Sutton controlled, including her personal bank account, credit card account, student loan account, and mortgage account. In one instance, Sutton used a company with a name similar to a true creditor to disguise her fraudulent diversion of the funds, the indictment states. (Source)

Prison Correctional Officer Pleads Guilty To Smuggling Drugs Into Prison For Bribes - April 22, 2022
Alexander Cole worked as a correctional officer at the Charlotte Correctional Institution (CCI) in Punta Gorda.

In June 2021, on three separate occasions, Cole agreed to smuggle methamphetamine or MDMA into the prison where he worked and provide the contraband to an inmate. He agreed to do so in exchange for payments of $400, $1,000, and $4,000, respectively.

On each occasion, Cole picked up a package containing what he believed were the controlled substances and then entered CCI. Cole would then conceal the packages containing the purported controlled substances and notify the inmate that they were available for retrieval. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Bookkeeper Charged With Embezzling $175,000+ From Church - April 18, 2022
Anita Hobdy was charged with wire fraud, stemming from fraudulent charges made from First Baptist Church of LaPlace, in Louisiana.

Hobdy worked as a bookkeeper for the church's daycare center and embezzled over $175,000 from church accounts from 2015 through 2021. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Goldman Sachs Investment Banker Paid Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company - April 8, 2022
Ng Chong Hwa, also known as "Roger Ng," a citizen of Malaysia and a former Managing Director of The Goldman Sachs Group, Inc., was convicted by a federal jury in Brooklyn on all counts of a superseding indictment charging him with conspiring to launder billions of dollars embezzled from a Malaysia development company (1MDB). He conspired to violate the Foreign Corrupt Practices Act (FCPA) by paying bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

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

Ng was employed as a Managing Director by various subsidiaries of Goldman Sachs and acted as an agent and employee of Goldman Sachs from approximately 2005 to May 2014.

Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs. They also conspired to launder the proceeds of their criminal conduct through the U.S. financial system by funding major Hollywood films such as "The Wolf of Wall Street," and purchasing, among other things, artwork from New York-based Christie's auction house including a $51 million Jean-Michael Basquiat painting, a $23 million diamond necklace, millions of dollars in Hermes handbags from a business based on Long Island, and a luxury real estate in Manhattan.

Through its work for 1MDB during that time, Goldman Sachs received approximately $600 million in fees and revenues, while Ng received $35 million for his role in the bribery and money laundering scheme. In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB. (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)

Former UBS Financial Advisor Pleads Guilty To Defrauding $5 Million+ From His UBS Clients Over 6 Years - April 14, 2022

From about 2012, and continuing to 2020, German Nino was a financial advisor working at a branch office of UBS Financial Services Inc. in Miami. Nino oversaw and managed UBS investment accounts for various customers, including three victims who were related and who had various investment accounts at UBS.

From about May 2014 to February 2020, Nino made a total of 62 unauthorized transfers from three UBS accounts belonging to the victims, which totaled $5,833,218.59. To accomplish the wire fraud scheme, Nino made materially false and fraudulent statements to his victims and concealed and omitted material facts including misrepresenting the true performance, balance, and rate of return of the accounts he managed.

Nino forged the signature of his clients on documents purporting to authorize transfers out of the accounts; preparing a fraudulent land purchase contract and forging a victim's signature on the land purchase contract to make it appear that the victim was purchasing land in Colombia by using money from the victim's account, Nino removed one of the victim's email from the victim's UBS email account profile so that the victim would not receive email notifications from UBS about unauthorized transfers; and preparing fraudulent UBS account statements and client review statements, which falsely inflated the balance and value of the victims' accounts. (Source)

Former Credit Union Employee Arrested For Steals $19,000 From Customer Account To Put Down Payment On Car - April 2, 2022

Madisyn Gore who was a credit union employee, was accused of creating a fraudulent debit card on the account in their name.

Using funds from the victim's account, Gore made multiple purchases and put a large down payment on a vehicle. More than $19,000 was taken from the victim's account, according to the release. (Source)

Former Bank Employee Admits Role In $1.6 Million Fraud Scheme - April 13, 022

Dayquann Williams used his position as a bank employee, first at Citizens Bank and then at Santander Bank, to access customer information and provide that information to others who obtained funds from the accounts through unauthorized transactions.

Between late 2018 and early 2020, as a mortgage development officer at Santander Bank, Williams searched bank records for older customers who had at least $100,000 in their accounts. He then passed along customer identifying and account information to others who used that information to cause approximately 70 fraudulent checks totaling approximately $1.6 million to be issued and more than $2 million in ACH transactions to be made or attempted. Not all of the fraudulent checks or ACH transactions ultimately cleared customers' accounts.

During the conspiracy, Fitzgerald-Williams also attempted to negotiate a fraudulent check in the amount of $34,700 made payable to him. (Source)

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

Health Care Charity Must Pay $8 Million+ In Restitution For Embezzlement, Bribery By Former Executives, Employees & Members Of State Legislature - March 31, 2022

Springfield, Missouri-based nonprofit Preferred Family Healthcare will pay more than $8 million in forfeiture and restitution to the federal government and the state of Arkansas under the terms of a non-prosecution agreement, which acknowledges the criminal conduct of its former officers and employees. Preferred Family Healthcare must relinquish the illegal profits it garnered from a wide-ranging fraud and bribery scheme.

Under the terms of the non-prosecution agreement, Preferred Family Healthcare will forfeit more than $6.9 million to the federal government and pay more than $1.1 million in restitution to the state of Arkansas related to the misuse of funds from the state's general improvement fund.

By signing the non-prosecution agreement, representatives of Preferred Family Healthcare admitted that former officers and employees of the charity engaged in a conspiracy to, amongst other criminal activity, embezzle funds from the charity and to bribe several elected state officials in the Arkansas House of Representatives and the Arkansas Senate. As a direct result of these actions, Preferred Family Healthcare realized a financial benefit. Although Preferred Family Healthcare's board of directors did not receive full or accurate information about these actions, the board, through lack of proper oversight, allowed its officers and employees to violate federal law. (Source)

Former Healthcare Employee Sentenced To Prison For $1.4 Million + 4 Year Wire Fraud, Money Laundering Scheme / Used Fund For Airfare, Vehicle Payment - April 29, 2022

Steven Racich was an employee of Apria Healthcare, a national business with a branch in Peoria, Illinois. Apria offers clinical services and sells at-home medical equipment, including CPAP machines. Racich worked at Apria from 2008 to 2017, and served as the branch manager.

During an internal audit in December 2017, Apria officials discovered the Peoria office was incurring unexplained and excessive shipping costs. The investigation established that Racich was stealing CPAP machines from Apria and selling them to third parties for his own profit, using Apria's accounts to ship the machines. It was discovered that Racich created a business and used an alias to communicate with customers, paying himself through a PayPal account under the alias name. The embezzlement occurred from as early as 2013 until Racich was terminated in December 2017. The fraud netted Racich over $1.4 million in profit. Racich used the unlawful funds to support his lifestyle, spending it on airfare, vehicle payments, and weekend trips. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

GE Employee Convicted For Stealing Turbine Trade Secrets To Benefit China Using Steganography - April 1, 2022

Xiaoqing Zheng was employed at GE Power & Water in Schenectady, New York, as an engineer specializing in sealing technology. He worked at GE from 2008 until the summer of 2018.

The trial evidence demonstrated that Zheng and others in China conspired to steal GE's trade secrets surrounding GE's steam and gas turbine technologies, knowing or intending to benefit the People's Republic of China and one or more foreign instrumentalities, including China-based companies that research, develop, and manufacture parts for turbines.

Zheng, while employed at GE , exploited his access to GE's files by stealing multiple electronic files, including proprietary files involving design models, engineering drawings, configuration files, and material specifications having to do with various components and testing systems associated with GE gas and steam turbines. Zheng e-mailed and transferred many of the stolen GE files to his business partner, Chinese businessman Zhaoxi Zhang, who was located in China. Zheng and Zhang used the stolen GE trade secrets to advance their own business interests in two Chinese companies - Liaoning Tianyi Aviation Technology Co., Ltd. (LTAT) and Nanjing Tianyi Avi Tech Co. Ltd. (NTAT), companies which research, develop, and manufacture parts for turbines.

Xiaoqing Zheng, an American citizen believed to also hold Chinese citizenship, is accused of using a technique called steganography to conceal the GE data inside the binary code of an innocuous-looking "digital picture of a sunset" that he then sent to his personal email address. The picture looked innocent. Just a sun peeking over the horizon. The caption: "Happy Fourth of July."

Zheng allegedly acknowledged stealing GE data on multiple occasions. He is also believed to have copied more than 19,000 files from a GE-issued computer to an external storage device in 2014.

During a federal search of Zheng's home in Niskayuna, New York, FBI agents found and confiscated a handbook detailing resources the Chinese government will give to individuals or entities for the provision of certain technologies. Agents also found five trips to China over the past two years on Zheng's passport. (Source)

Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company - March 7, 2022

Xiang Haitao was employed by Monsanto and its subsidiary, The Climate Corporation, from 2008 to 2017, where he worked as an imaging scientist.

In June 2017, the day after leaving employment with Monsanto and The Climate Corporation, Xiang attempted to travel to China on a one-way airplane ticket. While he was waiting to board his flight, federal officials conducted a search of Xiang's person and baggage. Investigators later determined that one of Xiang's electronic devices contained copies of the trade secret. Xiang continued on to China where he worked for the Chinese Academy of Science's Institute of Soil Science. Xiang was arrested when he returned to the United States in November 2019. (Source)

Samsung Employee Allegedly Captures Sensitive Chip Manufacturing Information With Smartphone - March 30, 2022

The Korea JoongAng Daily suggests that a Samsung Foundry employee might have photographed confidential information for the company's chipmaking technologies.

The employee is accused of having photographed his computer screen displaying this information with his smartphone while working from home. Additionally, they did not take a handful of photographs; instead, reports in the Korean press speculate that hundreds of trade secrets have been photographed. (Source)

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

Former Operations Manager Technology Support Firm Sentenced To Prison For Embezzling $350,000 / Used Funds To Buy Hot Tub, Home Gym, Airline Tickets, Concert Tickets - April 1, 2022

Matthew Hernandez is a former manager of a small, San Diego-based technology support firm.

Hernandez stole from the firm in 4 different ways, over the course of 7 years, from 2010 to January 2017:
1- He issued checks and made online payments from the firm's business checking account directly to his USAA account to pay off personal credit card debt.
2- He used the corporate credit card to make unauthorized, non-business-related purchases; To buy a $3,500 hot tub, a home gym, a knife set, a TAG Heuer racing watch, roundtrip flights, , and concert tickets.
3- He issued multiple paychecks to himself for a single pay period.
4- He issued checks from the firm's business checking account directly into his personal bank account.

To conceal his fraudulent conduct, Hernandez falsified the firm's books to make the fraudulent payments look legitimate. The fraudulent conduct was first discovered in January 2017 when Hernandez overdrew $10,000 from the firm's business checking account. The firm extensively reviewed its books and records, identified Hernandez's fraudulent purchases and transactions, and provided that information to federal law enforcement. The firm's efforts to identify Hernandez's fraudulent conduct took years to complete and was instrumental in moving the investigation and prosecution forward. (Source)

Former Assistant Controller Charged With Embezzling $3 Million+ To Pay For Personal Expenses - April 28, 2022

Tammy Simpson was an Assistant Financial Controller for 14 years, working for Triad Metals International (Triad).

Between 2012 and when she was terminated in October 2019, Simpson stole money and used it to pay personal expenses charged to her credit cards and to make payments on personal loans. She allegedly did so by paying her personal credit card bills and loan payments with electronic transfers from the company's business checking account. Simpson is also alleged to have kept credit cards from employees who had left the company and used them to charge personal expenses including airfare and other entertainment expenses for her family and friends, and to pay her personal tax liabilities and those of other individuals for whom she prepared tax returns.

The Indictment seeks forfeiture of $3,199,192.68, which represents the total amount of money Simpson allegedly embezzled from her now former employer. (Source)

Former Accounting Controller Charged With Embezzling $2.3 Million+ Over 5 Years / Used Funds For Personal Gain - April 11, 2022

From 2001 through February 2021, Gerard Beauzile worked as Accounting Controller, heading a New York-based company's accounting department. On a monthly basis, from 2014 through December 2020, Beauzile issued company checks to himself, and deposited those checks into his personal bank account at bank branches in New York, near his employer's headquarters.

Over the course of the scheme, Gerard Beauzile issued approximately 140 checks to himself totaling in excess of $2.3 million, which he used for his own benefit. Beauzile hid his scheme by failing to enter some of the checks into the victim company's accounting system; causing checks to appear as though they were made payable to vendors when, in fact, Beauzile issued them to himself; changing the vendors invoices to correspond with the accounting of those checks; and falsifying the victim company's bank account. (Source)

Company Controller Pleads Guilty To Embezzling $1.4 Million Over 7 Years - April 13, 2022

Until 2018, Gerald Burke was employed as the controller of a privately owned metal stamping company. She was responsible for the company's finances, including directing payroll and signing checks on behalf of the company.

From October 2011 until his termination in 2018, Burke embezzled $1.4 million by authorizing additional payroll payments to himself and by writing checks to himself and his credit card company from the company account. (Source)

Former Bookkeeper Pleads Guilty To Embezzling $1 Million+ Over 7 Years To Pay Personal Credit Cards - April 13, 2022

Joan Donald worked as a bookkeeper for Dovetail, a high-end interior design company based in Bethany Beach, Delaware.

For more than 7 years, Donald perpetrated a scheme against Dovetail and its owner, an elderly woman with ailing health, by using Dovetail's funds to pay Donald's personal credit card bills. When confronted with the fraud, Donald confessed that she had been embezzling money from Dovetail for years. A full forensic accounting conducted by the FBI revealed that Donald had stolen over $1 million. (Source)

Former Car Dealership Sales Associate Pleads Guilty To $1 Million Wire Fraud Scheme - April 12, 2022
From March 2019 to October 2021, William Turner was employed at Patriot Chevrolet in Bartlesville. Turner sold cars, assisted customers in obtaining financing for the purchase of vehicles, and received commission payments for his sales.

Starting in May 2020, Turner devised and carried out a scheme where he used stolen identities to purchase vehicles in those individuals' names and sometimes sold the vehicles to other people for cash. The vehicles would then leave the dealership's lot, and Turner would receive the commissions.

In his plea agreement, the former sales associate stated that on Sept. 14, 2020, he knowingly used identification belonging to another individual to submit a false loan application to Ally Bank for the purchase of a 2019 KIA Sorento in the approximate amount of $32,917 from Patriot Chevrolet. Turner stated that he received a commission for the purported sale of the vehicle, and after the sale was approved, he caused the Kia Sorrento to be transferred to an acquaintance who subsequently made payments to Turner via CashApp for the vehicle. Turner admitted that he acted with the intent to defraud the dealership.

Turner is alleged to have been responsible for more than $ 1 million in fraudulent vehicle sales. (Source)

Former Office Manager Sentenced To Prison For Fraudulently Obtaining $1 Million+ From Employer Over 8 Years - April 19, 2022
Tammy Moore was an Office Manager for a company in Loves Park, Illinois that made custom components for a variety of industries.

Moore admitted in a plea agreement that from 2012 to 2020, she fraudulently obtained more than $1 million from the company. Moore issued company checks to herself and her husband's business from the company's account, forged the signature of the company's owner on checks, deposited the checks into her personal bank account and her husband's business account for her personal benefit, and then initiated online transfers to move the money. Moore concealed these transactions by making it appear as though the checks were for legitimate business purposes and by deleting the company's records of the forged checks. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $850,000+ To Pay Personal Credit Card - April 6, 2022
Cindy Wojtaszek was the Bookkeeper of a business. Between November 2012 and July 2018 McCarthy paid her personal credit card from the company's bank account. To conceal her fraud, McCarthy altered the company's monthly bank statements to make it appear that payments were being made to a vendor. Through approximately 200 transactions, McCarthy defrauded the company of over $850,000. (Source)

Union President Convicted Of Stealing $84,000+ / Used Funds For Himself, Wife, Friends - April 6, 2022
Between September 2013 and September 2017, Jonathon Ortino was National Treasury Employees Union President. The union represents Customs and Border Protection officers in California and Nevada.

Beginning in February 2014, Ortino improperly took more than $84,000 in Union money, using it on himself, his wife, his friends, and other associates. (Source)

Former Associate Director Admits Embezzling Hundreds Of Thousands Of Dollars - March 7, 2022
David Buckingham held the title of Associate Director and head of the New York office of a global maritime service group headquartered in London, England.

From 2016 through 2018, Buckingham used his position and access to the company's bank accounts to embezzle hundreds of thousands of dollars by writing checks to himself or to cash. Buckingham falsified the company's books and records in an effort to make the payments appear to be legitimate business expenses and to cover up his fraud. From in or around February 2016 to October 2018, Buckingham also willfully failed to account for and pay over to the IRS payroll taxes for the employees of the company in the amount of $277,051. (Source)

Project Manager For Mechanical Contractor Pleads Guilty To Role In $396,000+ Construction Project Fraud Scheme - April 12, 2022
Don Richards was a Senior Project Manager at a Massachusetts-based mechanical contractor.

From November 2014 through February 2018, Richards conspired to defraud his employer and the project owners by inflating change orders on certain projects he was managing. As part of this conspiracy, a co-conspirator subcontractor, who was a principal of an insulation company, made payments to Richards and also for Richards's benefit, including gift cards and funds for a golf club membership. Richards and the co-conspirator submitted inflated change orders to Richards's employer to offset some of the costs of the payments the co-conspirator made to Richards.

Richards has agreed to pay restitution in the amount of $396,966. (Source)

Former Employee Attempts To Extort Employer For $150,000 Using Stolen Company Data - April 12, 2022
Frances Eddings and Jude Denis were convicted for accessing a computer system without authorization for financial gain from a non-profit charity organization.

On several occasions over the course of several days after Denis left her employment at the Prostate Cancer Foundation (PCF), PCF computers were accessed, and documents were downloaded to her laptop and emailed to Eddings. In a series of emails sent by Eddings to PCF, the defendants demanded a payment of $150,000 in lost wages for Denis, as well as a $37,500 payment for Eddings for acting on Denis' behalf. In those emails, Eddings threatened to release the documents to the public if their demands were not met. When their demands were ultimately not met, Eddings sent a series of emails to the PCF Board, PCF donors, and members of the media, sharing her previous correspondence and attaching the documents. (Source)

Construction Company Finance Manager Sentenced To Prison For Embezzling $500,000 From Customer - April 13, 2022
Lynn Tempel managed the finances of William Tempel Construction (WTC).

The customer hired and paid $4.41 million to WTC to build a dream home. Instead, Lynn Tempel stole money from the victim from 2013 to 2016. When caught, Tempel did not admit her fraud, rather she falsified 153 subcontractor invoices to cover up her scheme. Tempel provided to the victim invoices in which she had fraudulently inflated the amount of payment required. Tempel also withdrew $566,848 in cash from the company's business account during the period of the fraud.

Tempel also falsified IRS form 1099s for a family member, which underreported income for that family member by $399,525. Such an underreport then allowed the family member to illegally receive Medicaid. (Source)

Former Officer Manager Admits To Embezzling $445,000 Over 7 Years To Pay Credit Card Bills - April 14, 2022

Crystal Klatt was employed as an office manager by a property management company located in Hamden. Clients of the property management company would allow the company access to their bank accounts in order to allow the management company to make payments on behalf of the respective client. Klatt had access to the client's bank accounts as part of her job responsibilities.

Between approximately December 2014 and January 2021, Klatt diverted a total of $446,859.82 from the bank accounts of at least 14 clients to pay her personal credit card charges. (Source)

Former Hotel Senior Analyst Admits Role In $300,000+ Embezzlement Scheme Over 6 Years - April 14, 2022

Marco Alvarez is a former hotel employee of a nationwide hotel chain. As senior analyst for strategic sourcing for a national hotel chain, Alvarez was responsible for administering the company's corporate credit card program. He was authorized to approve applications for credit cards and to access account information for such credit cards.

From April 2014 through January 2020, Alvarez embezzled funds from the hotel through the unauthorized use of the hotel's corporate credit cards to purchase goods and services. Alvarez admitted that he knowingly opened and used corporate credit cards to make $317,582 in unauthorized personal purchases and attempted to conceal them by transferring credits owed to the hotel to these credit cards to offset the unauthorized charges made. (Source)

President Of Government Contractor Pleads Guilty To Bribing GSA Contracting Official $43,000 For $1 Million+ Contract Award - April 15, 2022

Jennifer Strickland is the President of SDC Contracting LLC, a company that contracted with the federal government to provide construction and renovation services at federal buildings.

From July 2018 until December 2019, Strickland made cash payments to a GSA contracting official totaling $43,500, in return for the award of a contract valued at approximately $1,369,501.00. (Source)

Financial Manager Charged With Embezzling Over $200,000 From Client Over 6 Years - April 20, 2022

Katie Laroche was a financial manager who handled bookkeeping, accounting, and other financial services for her clients.

From 2015 through 2021, LAROCHE embezzled $233,363.53 from one of her clients. Laroche the embezzlements by falsely indicating that withdrawals and transfers out of the victim's account were for tax payments, when in fact the money was deposited into Laroche's personal account or used for her own purposes. (Source)

Independent Contracted Accountant Sentenced To Prison For Second Embezzlement Scheme Costing Company $73,000 - April 20, 2022

Walter Tymoczko was an independent contractor performing accounting work for a local company.

From October 2018, until October 2019, Tymoczko embezzled funds from the company by utilizing an Inuit QuickBooks payroll program. Tymoczko used the program multiple times to transfer funds from the victim's bank account to his own bank account and a family member's bank account for a total of $73,206.77.

The court was further advised that Tymoczko has a previous federal felony conviction for embezzling from various clients. In the previous case, Tymoczko was sentenced to 24 months in prison and ordered to pay a total of $254,974.60 in restitution to various victims. (Source)

Former USDA Animal Inspector Pleads Guilty To Accepting $40,000+ In Bribes - April 25, 2022

Roberto Adams pleaded guilty to accepting over $40,000 in bribery payments while employed as a U.S. Department of Agriculture (USDA) lead animal health technician.

Adams inspected cattle entering the United States to determine if they met the necessary health requirements to enter the country. Over the course of at least 14 months, Mexican cattle brokers paid Adams to allow cattle into the country without proper quarantine or legitimate inspection. (Source)

Former Mayor Sentenced To Federal Prison For Accepting $5,000 Bribe From Red-Light Violation Camera Company - April 27, 2022

Louis Presta is the the former Mayor of Crestwood, Ill. He was sentenced to prison for improperly soliciting and receiving benefits from a representative of a red-light camera company that provided services to the Chicago suburb.

According to Presta's plea agreement with the government, the red-light camera company provided camera services to Crestwood that enabled the municipality to issue tickets to motorists for certain traffic violations. While the company was attempting to provide additional such services to Crestwood, then-Mayor Presta asked for and accepted benefits from a representative of the company. Presta told the company's representative that the percentage of red-light traffic violations that Presta approved would remain high or increase – in exchange for a cash payment to Presta from the representative, the plea agreement states. (Source)

Former General Manager Of Los Angeles Department Of Water & Power Sentenced To Prison For Accepting Bribes To Secure $30 Million Contract - April 27, 2022

David Wright was the former general manager of the Los Angeles Department of Water and Power. He was sentenced prison for accepting bribes from a lawyer in exchange for his official action to secure a three-year, $30 million no-bid LADWP contract for the lawyer's company.

Wright served as LADWP's general manager from September 2016 until July 2019, when he resigned at the direction of the mayor of Los Angeles. (Source)

THEFT OF COMPANY PROPERTY

Former Amtrak Employee Sentenced To Prison For Stealing $76,000+ Worth Of Chainsaws / Chainsaw Parts And Selling For Personal Profit Over 8 Years - April 19, 2022

Jose Rodriguez had been an Amtrak employee since October 2007, most recently as a senior engineer and repairman, based out of an Amtrak facility in North Brunswick, New Jersey.

Between March 2012 and July 2020, Rodriguez obtained 114 chainsaws, 122 chainsaw replacement bars, and 222 replacement chains from Amtrak, the total value of which was over $76,000, under the false pretense that this equipment would be used for Amtrak projects, but then sold the equipment either on an online auction service or directly to purchasers. Rodriguez used the U.S. Postal Service to mail the stolen chainsaw and chainsaw parts to purchasers throughout the United States, including purchasers in Ohio, Pennsylvania, and West Virginia. (Source)

Former Production Supervisor For Drug Manufacturer Sentenced To Prison For Theft Of $750,000 Of Medical Products Over 8 Years - April 20, 2022

Gary Settino was the Production Supervisor of manufacturing at a Long Island Drug Manufacturer, American Regent, in New York

Settino stole Adequan, a drug manufactured by the company, and then resold it. Adequan is an injectable equine drug administered to horses to treat degenerative drug disease.

Settino's thefts of thousands of bottles of Adequan covered a period of eight years, from 2012 to 2020. Settino sold those drugs worth $750,000 for hundreds of thousands of dollars to trainers and veterinarians at New York racetracks, including Belmont Park. Settino's conduct endangered the health of horses because the drugs were not maintained, stored or transported in accordance with proper procedures for ensuring the safety, effectiveness and efficacy of the drugs. At times, Settino transported the drugs in shoeboxes stored in his car. (Source)

Former Information Technology Director Pleads Guilty Using $320,000+ Of Organizations Funds To Purchase / Sell 162 Apple Computers - April 27, 2022

Tyler Fuhrken pleaded guilty to using $320,098 from the Port of Corpus Christi to purchase Apple computers for personal use while employed as its IT director.

The investigation revealed that from May 22, 2016, to Feb. 4, 2021, Fuhrken authorized the purchase of 162 Apple computers. He had the authority to do so as necessary for the port. However, he did not record the purchased computers in the port's asset control system or inventory.

Authorities traced a series of suspicious PayPal deposits into Fuhrken's bank account. They were from a computer reseller located in New York who acknowledged purchasing many Apple computers from Fuhrken. Fuhrken would invoice the reseller for the computers on PayPal and would ship the computers from Texas to the resale shop located in New York.

The reseller provided authorities with a list of the computers he purchased. They were able to identify the 162 Apple computers missing from the port. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Former State Employee Sentenced To Prison For Role In $2 Million Scheme To Defraud the Office of AIDS - March 7, 2022

Christine Iwamoto was employed by the Office of AIDS within the California Department of Public Health until March 2018. The Office of AIDS is responsible for working on behalf of the State of California to combat the HIV and AIDS epidemic.

Between December 2017 and November 2018, Iwamoto participated in a scheme that was coordinated by Schenelle Flores, also employed at the Office of AIDS, to defraud the Office of AIDS. Flores, Iwamoto, other participants in the scheme, and their families and friends obtained at least $2 million in personal benefits, including cash and purchased items.

Flores directed a state contractor to make payments allegedly on behalf of the Office of AIDS and caused the contractor to charge those payments to the state. Flores caused the contractor to pay for personal expenses on its debit cards, order gift cards for personal use, and pay false invoices to shell companies for services allegedly provided to the Office of AIDS.

Iwamoto set up a shell company and coordinated with Flores to submit invoices to the state contractor. Those invoices falsely claimed that Iwamoto's company had provided various consulting and meeting facilitation services to the Office of AIDS. Iwamoto received $450,000 in payments as a result of the invoices. Iwamoto then gave thousands of dollars in cash and blank checks to another employee of the Office of AIDS who was participating in the scheme. Iwamoto also participated in obtaining the gift cards from the state contractor and received hundreds of the gift cards for her personal use. (Source)

Former Employee Sentenced To Prison For $4 Million Fraud Invoice Scheme With Help Of Husband For Personal Gain - April 19, 2022

April and James Thompson have each been sentenced for mail fraud after stealing over $4 million from Forest Investment Associates (FIA), an Atlanta-based company that provides timberland investment advisory and management services for institutional timberland investors.

April Thompson worked in Texas for Kingwood Forestry Services (Kingwood), which is a natural resource consulting firm that provides a variety of forestry services to landowners.

Forest Investment Associates (FIA) contracted with Kingwood to retain contractors to provide field services on behalf of FIA's clients, such as clearing land, road grading, or other services.

After the work was completed, Kingwood would send invoices to FIA for the work performed by the contractors. FIA, in turn, paid the invoices directly to the contractors. At Kingwood, April Thompson was responsible for managing the submission of invoices to and requesting payment from FIA.

Between approximately May 2011 and April 2019, April Thompson submitted over 400 fraudulent invoices totaling more than $4 million to Forest Investment Associates (FIA) for work that her husband, James Thompson, had allegedly performed at FIA timber properties. James Thompson never worked as contractor for FIA or Kingwood and had never performed work on any FIA timber property. After April Thompson submitted the invoices, FIA mailed checks to the Thompsons which they deposited into bank accounts they jointly controlled.

The Thompsons used the stolen money for their own personal benefit, including to operate James Thompson's trucking businesses, support his race car hobby, purchase silver and gold coins, install a pool at their home, and even treat themselves and friends to a Hawaiian vacation. (Source)

Former Water District General Manager Charged For Role In Stealing $25 Million Of Federally Owned Water - April 14, 2022

Dennis Falaschi was the general manager for a public water district in Fresno, California. He exploited a leak in the Delta-Mendota Canal and engineered a way to steal over $25 million in federally owned water.

In 1992, Falaschi was informed that an old, abandoned drain turnout near milepost markers 94.57 and 94.58 on the Delta-Mendota Canal was leaking water from the Delta-Mendota Canal into a parallel canal that the water district controlled. The drain was connected to a standpipe on the bank of the Delta-Mendota Canal that used a gate and valve to redirect water from the Delta-Mendota Canal into the water district's canal. The gate had been cemented closed years earlier. The cement had since cracked and water was coming through it.

Thereafter, Falaschi instructed an employee to install a new gate inside the standpipe so that the site could be opened and closed on demand. He later instructed the employee to install a lid with a lock on top of the standpipe and an approximate two-foot elbow pipe off the valve of the standpipe that angled down 90 degrees into the water district's canal. The lid concealed the theft because it prevented people from seeing that the gate inside the standpipe was functional. The elbow pipe further concealed and expedited the theft because it enclosed the water flow from the Delta-Mendota Canal into the water district's canal and was installed in such a way that it was generally submerged under the water.

Falaschi subsequently instructed employees to use the site to steal federal water from the Delta-Mendota Canal on multiple occasions until the site was discovered in April 2015. He used the proceeds of the theft to pay himself and others exorbitant salaries, fringe benefits, and personal expense reimbursements. (Source)

Former Healthcare System Employee Admits Role In $116,000+ Embezzlement Scheme - April 28, 2022

In January 2020, Lorita Fair began working in the payroll department of Yale New Haven Health Systems (YNHHS) as a temporary employee performing payroll functions. In May 2020, Fair was hired as a full-time employee as a Payroll Processing Associate at YNHHS.

Shortly thereafter, Fair began engaging in a scheme to embezzle money and funds from YNHHS by creating fraudulent entries in the YNHHS payroll system that resulted in Fair and two other individuals receiving payroll payments to which they were not entitled.

As part of the scheme, Fair made fraudulent entries in the YNHHS payroll system, either by directly entering the fraudulent payments into the online system, or by manually adding lines to a spreadsheet of payroll payments after the spreadsheet had been reviewed and approved internally at YNHHS. The fraudulent payments would then be made by direct deposit from the YNHHS payroll system into Fair's and the other two individuals' personal bank accounts. The other two individuals then kicked back to Fair a portion of the fraudulent payroll funds they each received. Between June and December 2020, Fair caused a total of $116,260.41 in fraudulent payroll payments to be made to herself and the other two other individuals receiving payroll payments to which they were not entitled. (Source)

Former Small Business Administration Employee Sentenced To Prison For Role In $18,000+ Identity Theft Scheme - April 19, 2022

Jay Soulliere was a Disaster Recovery Specialist for the Small Business Administration (SBA) from September 2020 until March 2021. His job responsibilities included assisting people applying for disaster-related loans.

In the fall of 2020, Soulliere stole from SBA's computer system the personal information of two victims who had applied for loans. Soulliere gave that information to a co-conspirator, Matthew Moore Vodak, Jr., who used it to commit various acts of identity theft, including buying a Land Rover with a fraudulent check and driver's license, taking over a credit card, applying for loans and credit, and producing fake identification documents. Soulliere also listed one of the victims as a member of his household in a bid to obtain state benefits. During the offense and the prosecution, Soulliere repeatedly used methamphetamine and he absconded from a halfway house. When he was arrested by federal agents, he had another person's identification document in his possession and lied to agents about his identity.

Soulliere pled guilty to conspiracy to commit identity theft and aggravated identity theft. Soulliere was also sentenced to three years of supervised release following incarceration and ordered to pay more than $18,000 in restitution. (Source)

Former Police Chief Pleads Guilty In Role To Illegally Traffic 200 Fully Automatic Machine Guns - April 18, 2022

Dorian LaCourse is the former Chief of Police in the Village of Addyston, Ohio.

LaCourse was charged by a federal grand jury for using his law enforcement position to illegally help two federally licensed firearms dealers in Indiana acquire and resell approximately 200 fully automatic machine guns using false documents.

LaCourse, Marcum, and Petty, illegally exploited a law enforcement exception to the federal ban on the possession or transfer of fully automatic machine guns. As Chief of Police, LaCourse signed multiple "demonstration letters" falsely stating that the Village of Addyston Police Department was interested in purchasing various types of machine guns, including military-grade weapons, and asking that Marcum and or Petty give the demonstration. Marcum and Petty then sent the letters to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) in order to obtain the weapons. Addyston is a village in southwestern Ohio of approximately 1,000 residents. LaCourse was the village's only full-time police officer.

LaCourse also placed direct orders for German-made machine guns that were purported to be paid for by the Police Department. In fact, the purchases were fully funded by Marcum and Petty and intended to bypass restrictions on the importation of such weapons by anyone other than the police or the military. (Source)

Former Employee Of Travel Insurance Company Sentenced To Prison For Role In $650,000 + Wire Fraud Scheme - April 15, 2022

Marie Caceres was employed by Seven Corners, a travel insurance business.

Between May 2011 and September 2016, Caceres prepared and submitted thirty fraudulent insurance claims to Seven Corners totaling more than $650.000. As part of the scheme, Caceres and her accomplices created fictitious names under which they purchased insurance policies from the victim company. Caceres and her accomplices created false email addresses in the name of a hospital in Venezuela and submitted claims to the victim company for purported emergency medical services provided to the fictitious individuals during international travel.

In fact, none of these expenses were ever incurred and Caceres had created artificial customer accounts and false documents in support of the claims. As a result of the fraud, the victim company paid over $588,000 to accounts controlled by Caceres' accomplices. (Source)

Project Manager For Mechanical Contractor Pleads Guilty To Role In $396,000+ Construction Project Fraud Scheme - April 12, 2022

Don Richards was a Senior Project Manager at a Massachusetts-based mechanical contractor.

From November 2014 through February 2018, Richards conspired to defraud his employer and the project owners by inflating change orders on certain projects he was managing. As part of this conspiracy, a co-conspirator subcontractor, who was a principal of an insulation company, made payments to Richards and also for Richards's benefit, including gift cards and funds for a golf club membership. Richards and the co-conspirator submitted inflated change orders to Richards's employer to offset some of the costs of the payments the co-conspirator made to Richards.

Richards has agreed to pay restitution in the amount of $396,966. (Source)

Former Casino Vice President / General Counsel & Former State Senator Plead Guilty To Felonies Involving Political Contribution Schemes - April 18, 2022

John Keeler is the former Vice President and General Counsel of an Indiana based casino company New Centaur LLC.

He paid $41,000 with New Centaur corporate funds to Maryland-based political consultant Kelley Rogers. Keeler then directed Rogers to funnel $25,000 to a local political party committee in Marion County, Indiana. To further conceal the nature of the contribution, Keeler caused New Centaur's federal tax return filed with the Internal Revenue Service to falsely describe the $41,000 payment to Rogers as a deductible business expense. (Source)

Former Employee Pleads Guilty To His Role In Defrauding His Employer Of $549,000+ Using Shell Companies / Fake Invoices - April 21, 2022

Michael Goll was a branch manager for his employer. His company provides material handling equipment to businesses.

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

Former Manager For Guided Tour Company Sentenced To Prison For Role In Embezzling $295,000+ From Employer With Help Of Another Employee - April 25, 2022

Between October 2010 and August 2016, Estela Laluf held a management position at a New Jersey guided-tour company.

During that time, Laluf and another employee, who held an accounting position at the company and had authority to write checks against the company's bank accounts, devised a scheme to embezzle funds from the company. Laluf would direct the employee to write company checks to actual company employees and contractors, which did not reflect any actual work or services done by those individuals.

The employee would then cash these checks, and Laluf and the employee would convert the resulting funds to their personal use. Laluf and the employee embezzled hundreds of thousands of dollars from the company. (Source)

TERRORISM

Former Train Engineer Sentenced To Prison For Intentionally Derailing Locomotive Near U.S. Navy Hospital Ship - April 13, 2022

On March 31, 2020, Eduardo Moreno drove a train at high speed and did not slow down near the end of the railroad track. He intentionally derailed the train off the tracks near the United States Naval Ship Mercy, a hospital ship then docked in the Port of Los Angeles.

No one was injured in the incident, and the Mercy was not harmed or damaged. The incident resulted in the train leaking a substantial amount, approximately 2,000 gallons of diesel fuel, which required clean up by fire and other hazardous materials personnel. Clean-up crews recovered approximately 400 gallons of fuel from the fuel tank and the ground adjacent to the derailment, according to court documents. Moreno caused $755,880 in damage because of the derailment.

Moreno acknowledged that he "did it," saying that he was suspicious of the Mercy and believed it had an alternate purpose related to COVID-19 or a government takeover. Moreno stated that he acted alone and had not pre-planned the attempted attack. (Source)

PREVIOUS INSIDER THREAT INCIDENT REPORTS

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data (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)

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)

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)

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**3,600+ 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

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

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

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.

https://www.insiderthreatdefense.us/news/

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

https://twitter.com/InsiderThreatDG

Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

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

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

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **875+** 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