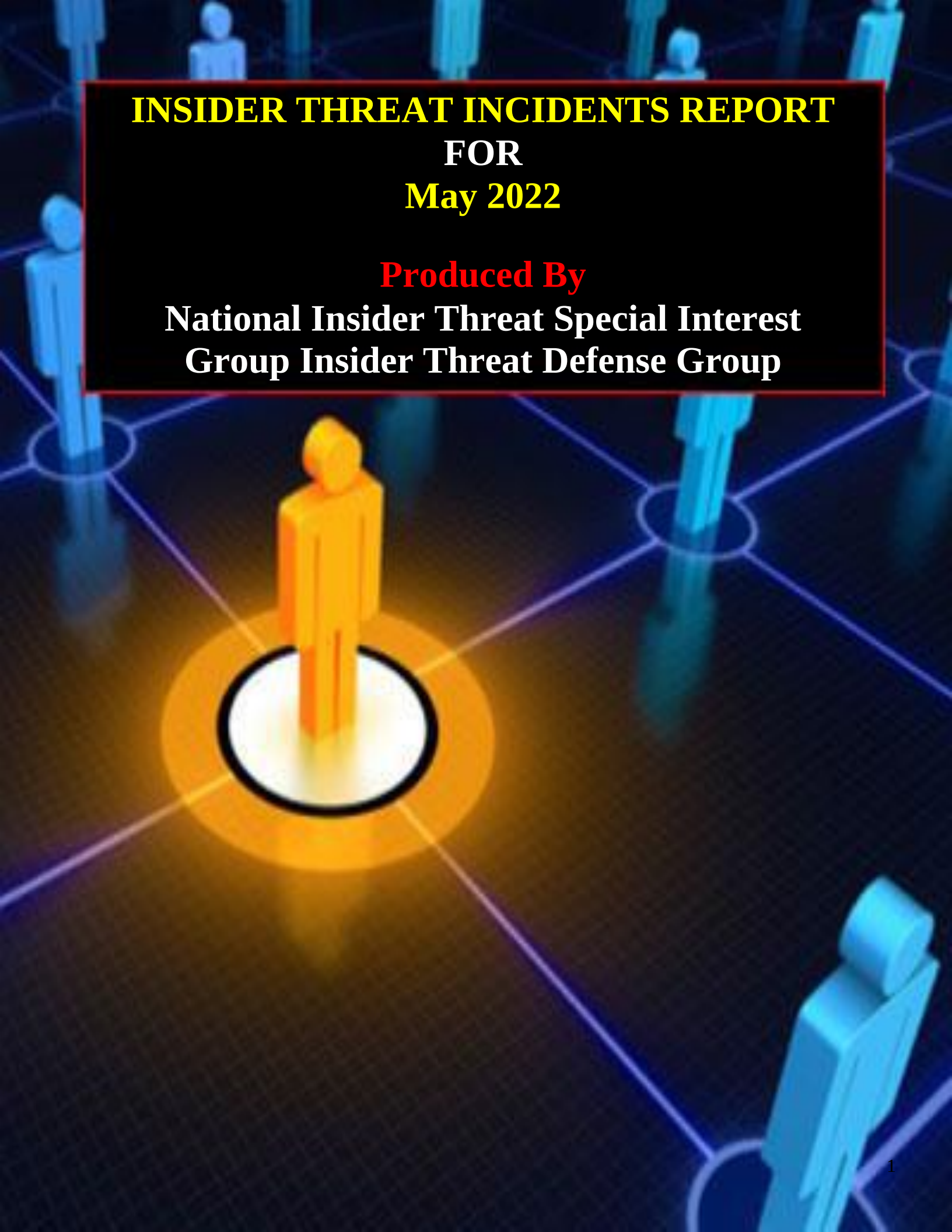

INSIDER THREAT INCIDENTS REPORT
FOR
May 2022

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 **3,700+** 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 19 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 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 / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business

INSIDER THREAT INCIDENTS
FOR MAY 2022

U.S. GOVERNMENT

U.S. Postal Employee & Son Charged With Conspiracy Involving Stolen Postal Money Orders Worth Over $5 Million - May 23, 2022

Dewayne Morris Sr., was a supervisor for post offices in Venice, Playa Del Rey, and Marina Del Rey. He ordered and received 10,000 blank Postal money order forms. A subsequent audit revealed that approximately 5,100 of those 10,000 money order forms were missing. With a maximum value of $1,000 per money order, the potential value of the missing money order forms is $5.1 million.

Morris Jr., distributed the missing money orders to co-conspirators. The money orders Morris Jr. distributed to co-conspirators were materially altered to appear as if they had been paid for and lawfully issued by a post office, when in fact they had not. Morris Jr. also provided co-conspirators with counterfeit driver's licenses bearing fictious identities. The co-conspirators used those counterfeit documents to open checking and savings accounts at financial institutions throughout the country, deposited the stolen money orders into the accounts, and withdrew the cash proceeds before the financial institutions detected the fraud. (Source)

U.S. Postal Service Mail Carrier Arrested For Scheme To Steal $800,000 In Unemployment Insurance Debit Cards - May 26, 2022

From August 2020 to February 2021, Stephen Glover and McKenzie fraudulently obtained debit cards issued by the California Employment Development Department (EDD), which administers the state's unemployment insurance program. The debit cards were issued based on applications for pandemic-related unemployment benefits submitted using approximately 50 stolen identities and containing false statements claiming COVID-related job losses, the affidavit states. The EDD debit cards were issued in the names of victims, some of whom had never resided in, worked in, or even visited California. Glover and McKenzie allegedly split the cash withdrawn using the EDD debit cards, some of which had balances exceeding $30,000.

The scheme allegedly involved more than 50 fraudulent claims to EDD, which resulted in EDD issuing cards that had approximately $798,733 in funds in those names, of which at least $318,771 has been withdrawn from the debit cards. (Source)

Former U.S. Postal Service (USPS) Employee Charged For Stealing $18,000 Of Government Money - May 6, 2022

Beginning in approximately August 2018, Zeon Johnson worked as a Sales and Service Distribution Associate for USPS. As part of his job, Johnson sold stamps and processed money order transactions for USPS customers. From approximately July 2019 through June 18, 2020, Johnson engaged in two schemes to convert USPS funds for personal use.

Johnson intentionally voided cash transaction sales of USPS stamps to customers, resulting in no records being made of cash payments for stamps, and then stole the cash for his own personal use. Johnson stole USPS funds through fraudulent money orders, specifically by issuing himself blank money orders, money order refunds as well as money orders made payable to himself. In total, it is alleged that Johnson stole over $18,000 in USPS funds. (Source)

U.S. Postal Service Engineer Pleads Guilty To Accepting $6,500+ Of Illegal Gratuities And Free Construction Work From A USPS Contractor - May 4, 2022

Thomas Berlucchi , is a Facilities Engineer for the United States Postal Service (USPS).

Berlucchi stands convicted of accepting illegal gratuities from Michael Rymar, who was the owner of a Rochester Hills company, Horizons Materials & Management LLC, which was awarded contracts to repair USPS buildings in Michigan and New York.

From 2015 to 2018, Berlucchi and other USPS engineers awarded Rymar's company over $5 million in contracts. Berlucchi admitted that between 2013 and 2018, he had accepted over $6,500 in illegal gratuities from Rymar because Rymar sought to continue to receive USPS work from Berlucchi. Berlucchi admitted accepting free construction work on his cottage (including exterior stairs and a new roof), free hotel rooms, and donations by Rymar to Berlucchi's preferred organization. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Ft. Bragg Employee Sentenced To Prison For Receiving $773,000 Of Bribes - May 18, 2022

Calvin Alfonza Jordan was a Procurement Agent assigned to the Operations and Maintenance Division, Directorate of Public Works (DPW), at Fort Bragg, NC. To obtain services, a Ft. Bragg facilities user submits a request for a repair or service of a facility, such as a roof leak, damaged floor, or plumbing issue to the DPW. The request creates a Demand Maintenance Order (DMO) that is forwarded to the appropriate commodity section. The DMO is assigned to a DPW technician that specializes in a certain trade, such as roofing, flooring, plumbing, or carpentry.

From 2011 into 2019, Jordan used his position as a Procurement Agent to receive bribes of approximately $200 per DMO from various vendors contracting with DPW, Ft. Bragg, North Carolina, in return for increasing the number of federal contracts given the vendor. It is estimated Jordan received $773,600 in illegal bribes. (Source)

Former Philadelphia Veterans Affairs Medical Center Hospital Employee Pleads Guilty To Stealing $487,000 In Government Funds - May 25, 2022

Bruce Minor was charged with theft of government funds stemming from his theft of $487,000 in Veterans Affairs travel reimbursement funds, which he helped administer as part of his official duties as an travel clerk.

In order to perpetrate the theft, Minor created fraudulent travel reimbursement claims in the names of at least three other VAMC employees and then diverted the fraudulently obtained funds into bank accounts he controlled. Minor admitted to stealing approximately $13,000 in travel funds, though subsequent investigation showed that he stole upwards of $487,000 between December 2015 and September 2019. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

2 Detroit County Roads Division Employees Charged In Their Roles For Embezzling $1.7 Million+ - May 3, 2022

Kevin Gunn and John Gibson and others were engaged in a scheme to defraud Wayne County by using taxpayer dollars to make unauthorized purchases of generators and other power equipment from retailers in Southeast Michigan, which they sold for personal profit.

Between January 2019, and August 2021, Gunn solicited approved Wayne County vendors to purchase generators and other power equipment from local retailers on behalf of Wayne County. The vendors would then submit invoices for these items to Wayne County. In order to conceal the scheme to defraud, Gunn instructed the vendors to falsify the invoices they submitted to the Roads Division, and list items the vendors were authorized to sell to the county under their contracts, rather than the generators and power equipment they were unlawfully acquiring at Gunn's request. Roads Division employees would then approve and pay each vendor's invoice with taxpayer funds. After these fraudulent purchases were verified and approved by Roads Division employees, Gibson, and Gunn took possession of the equipment which was resold over the internet and social media for personal profit.

A review of invoices from Wayne County vendors revealed that between January 16, 2019, and August 3, 2021, Wayne County vendors purchased 596 generators, and a variety of other power equipment including lawnmowers, chainsaws, and backpack blowers. The purchase of these items was not authorized under any vendor contract with Wayne County nor were the items ever provided to or used by Wayne County. The total value of equipment purchased as part of the scheme was approximately $1.7 million in taxpayer funds. (Source)

Former College Dean Sentenced To Prison For Embezzling $650,000+ From Student Organization For Trips To The Caribbean - May 5, 2022

While serving as the volunteer Executive Director of the student association, Carmita Colmean withdrew cash and issued checks from the group's bank accounts for her personal benefit.

Coleman used debit cards linked to the organization's accounts to make various personal purchases, including for trips to the Caribbean. She attempted to cover up the fraud by submitting false and misleading reports that concealed the withdrawals. When a new individual was appointed to replace Coleman as Executive Director, Coleman knowingly delayed turning over access to the organization's bank accounts so that she could continue spending the money for her personal benefit.

During the fraud scheme, which lasted from 2011 to 2016, Coleman separately worked as a dean and professor at various colleges of pharmacy. (Source)

2 Former New York Utility Managers Of National Grid Sentenced To Prison For $50 Million+ Contract Bribery & Kickback Scheme - May 6, 2022

Patrick McCrann and Richard Zavada were National Grid managers employed in the facilities department, who steered contracts to certain contractors in exchange for hundreds of thousands of dollars in bribes and kickbacks.

One of the contractors secured more than $50 million in facility maintenance contracts from National Grid during the time that the contractor was paying bribes to McCrann and Zavada.

The illicit payments to McCrann and Zavada took multiple forms, including cash, the purchase of recreational vehicles, home improvements, landscaping and overseas vacations. As part of the investigation, agents recovered approximately $300,000 in cash from a safe deposit box held by Zavada. (Source)

State Employee Charged In Role In $1 Million+ Unemployment Fraud Scheme - May 18, 2022

3 women have been charged in a criminal complaint for their alleged role in a $1.6 million dollar unemployment insurance fraud scheme aimed at defrauding the State of Michigan and the U.S. Government of funds earmarked for unemployment assistance during the COVID19 pandemic.

Charged were Antonia Brown, Kiannia Mitchel and Angela Johnson

Antonia Brown was employed by the State of Michigan as an Unemployment Insurance Examiner assigned to the Benefit Payment Control Unit. Part of her duties included reviewing, approving and adjudicating various Pandemic Unemployment Assistance (PUA) and Unemployment Insurance Assistance (UIA) claims.

Starting in March 2020, Kiannia Mitchel and Angela Brown fraudulently filed and / or accessed over 123 PUA claims, resulting in the disbursement of approximately $1.6 million in federal funds earmarked for PUA and UIA benefit payments. The complaint alleges that Brown acted outside the scope of her authority by electronically accessing, altering, and approving approximately 101 of the fraudulent claims which were all associated with Johnson and Mitchell's residences. Mitchel and Johnson are alleged to have received money from third parties to assist them with the claims and paid Brown for her assistance in processing the fraudulent claims. (Source)

District of Columbia Fire / EMS Employee Pleads Guilty For Accepting $60,000+ In Bribery Scheme Involving Undelivered Goods - May 26, 2022

Louis Mitchell is a former employee of the District of Columbia Fire and Emergency Medical Services Department (FEMS).

Mitchell pleaded guilty to a bribery charge for accepting more than $60,000 in payments from a District of Columbia contractor in exchange for directing purchase agreements and orders to the contractor and then falsely certifying that goods that FEMS had paid for had been delivered.

Mitchell was a warehouse supply technician at FEMS. In that role, he was responsible for verifying deliveries of goods to the warehouse before the agency would issue payments to the relevant vendors. Beginning in at least 2016 and continuing through in or about 2020, Mitchell and a FEMS contract administrator engaged in a bribery scheme with a contractor whose company was an approved vendor for supplies.

As a result of the bribery scheme, FEMS paid the company more than $150,000 for goods that never were delivered. Mitchell personally received at least $61,250 in bribes from the contractor. (Source)

Former School District Finance Director Sentenced To Prison For Embezzling $94,000+ - May 18, 2022 In 2006, the Christopher Gehris was hired as a controller for the Phoenixville Area School District (PASD).

PASD's Business Office and later promoted to business manager. In 2018, he was appointed to serve as the Director of Finance. From 2013 until 2019,

Gehris cashed checks made payable to himself and to cash, received checks and direct deposits into his personal checking account for start-up money for student activities, stole cash from school programs, and obtained gift cards for personal expenditures, all in furtherance of his embezzlement scheme. He also admitted that he hid his thefts by altering receipts and falsifying reports submitted to the Board of School Directors.

Gehris pleaded guilty to embezzling from a program receiving federal funding and admitted that he stole approximately $94,613 from the PASD. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former County Sheriff's Deputy Pleads Guilty To $5.6 Million Fraud Scheme / Used Funds For Gambling, Private Jet Trips, Buying Luxury Cars & Other Items For His Girlfriends - May 10, 2022

Christopher Burnell is a a former San Bernardino County sheriff's deputy. He pleaded guilty to multiple felonies for deceiving victims into investing at least $5.6 million with him, then using their money on extravagant gambling, taking private jet airplane rides and buying luxury items for his girlfriends.

Burnell falsely claimed to have accumulated tens of millions of dollars from lawsuits he purportedly won against the San Bernardino County Sheriff's Department and Kaiser Permanente; from selling a patent for an air-cooled, bullet-resistant vest to Oakley Inc.; and through investments in small businesses and money-lending opportunities.

After deceiving victims into believing he was a wealthy businessman, Burnell then induced victims to invest up to hundreds of thousands of dollars at a time with him by offering exclusive investment opportunities that promised rates of returns as high as 100% to be repaid in a few weeks. In some instances, Burnell asked the victim for an initial trial investment with him, during which he would fulfill his promised returns – and gain the victim's trust – only to ask for a larger amount from

But these investment opportunities did not exist. Rather, Burnell spent the money on maintaining a life of luxury. Burnell spent victims' money on, among other things, gambling and luxury items, including losing more than $2 million in gambling at the San Manuel Casino in Highland, $500,000 in private jet trips, $70,000 on Louis Vuitton merchandise, and $175,000 on luxury cars and an apartment lease for his then-girlfriends. (Source)

Former Homeland Security Investigations Agent Found Guilty Of Accepting $100,000 In Bribes - May 3, 2022

Over an 18 month period that started in September 2015, Felix Cisneros accepted cash, checks, private jet travel, luxury hotel stays, meals and other items of value from a person who was associated with a criminal organization. Cisneros received approximately $100,000 in checks and gifts from Individual 1 in 2015 and 2016.

Cisneros accepted cash payments and other benefits to help an organized crime-linked person, including taking official action designed to help two foreign nationals gain entry into the United States. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Administrator Arrested For Stealing $360,000 From Church For Personal Use - May 25, 2022

From June 2013 to February 2018, Chanell Easton worked as an administrator at a church in Yuba City.

During her employment, Easton stole over $360,000 from the church, including from its food pantry and youth ministry, during a years-long embezzlement scheme. Without the church's knowledge or authorization, Easton opened five business credit card accounts in the church's name. Easton used these five credit cards, as well as a credit card used by the church's youth pastor, to make personal purchases—including at a hair salon, retail stores, online retailers, a vacation rental service, and to buy concert tickets—and then paid off the resulting balance with the church's money. Easton also transferred money directly from the church's bank accounts to her own personal account, paid down the balance of her own personal credit card, and paid her cellphone provider for her personal bills and for new phones.

Easton also stole money from the church by writing checks to others for personal expenses and by writing checks to herself, on which she forged the signatures of the church's treasurer or the head volunteer of the church's food pantry. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Teller Pleads Guilty To Embezzling $349,000+ - May 11, 2022

From January 2013, to November 2016, Karen Tigler was employed as a multi-service banker with the Hancock Whitney Bank.

From February 9, 2015, to October 28, 2016, Tigler embezzled approximately $349,556 from a client account by using 100 counter checks to debit funds from the clients account.

Tigler forged the signatures of the client and various others on the counter checks to conceal her embezzlement scheme. (Source)

Wells Fargo Bank Employees Recruited To Help Steal $120,000+ From Bank Customer Accounts - May 13, 2022

Michael Drummond admitted to orchestrating a scheme that was carried out in 2017 in which Drummond recruited Wells Fargo bank employees who would make unauthorized withdrawals from Wells Fargo customer accounts. The bank employees used the bank's internal systems to check the account balances of customers without the customer's knowledge. Those employees then told Drummond the customer's name and account balance.

Drummond then sent another accomplice into the bank to pose as the customer and to withdraw the funds, unbeknownst to the actual customer. The conspirators used this scheme to steal $124,000 in cash. (Source)

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

Hospital Registered Nurse Pleads Guilty To Stealing Cancer Patients' Pain Medication For Personal Use - May 26, 2022

Alison Marshall, a registered nurse who previously was employed in the interventional radiology unit of a hospital in Kalamazoo, Michigan, removed liquid fentanyl and replaced it with saline solution in July and August of 2020.

On August 20, 2020, another nurse working in the interventional radiology unit recognized that a 72-year-old cancer patient undergoing a percutaneous chest tube placement procedure did not receive the expected pain relief from the liquid fentanyl that was administered at the outset of the procedure. Hospital records revealed that Marshall checked out doses of fentanyl for patients 14 times from in July and August of 2020 but then canceled the transactions and purportedly returned the fentanyl back into the interventional radiology unit's inventory. FDA laboratory examination of the vials with the glued caps revealed needle punctures consistent with tampering, and laboratory testing demonstrated that the vials were substantially diluted, containing 3% or less of the amount of reported fentanyl.

On August 24, 2020, Marshall met with hospital representatives and admitted diverting fentanyl for her own use by removing vials of injectable fentanyl from the medication dispensing machines, extracting the fentanyl using syringes, replacing the medication with saline, gluing the plastic tampering caps back onto the vials, and returning the vials back into the unit's medication dispensing machines. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION - May 2, 2022

Gongda Xue worked as a scientist at the Friedrich Miescher Institute for Biomedical Research (FMI) in Switzerland, which is affiliated with Novartis. His sister, Yu Xue, worked as a scientist at GlaxoSmithKline (GSK) in Pennsylvania. Both Gongda Xue and Yu Xue conducted cancer research as part of their employment at these companies.

While working for their respective entities, Gongda Xue and Yu Xue shared confidential information for their own personal benefit.

Gongda Xue created Abba Therapeutics AG in Switzerland, and Yu Xue and her associates formed Renopharma, Ltd., in China. Both companies intended to develop their own biopharmaceutical anti-cancer products.

Gongda Xue stole FMI research into anti-cancer products and sent that research to Yu Xue. Yu Xue, in turn, stole GSK research into anti-cancer products and sent that to Gongda Xue. Yu Xue also provided hundreds of GSK documents to her associates at Renopharma. Renopharma then attempted to re-brand GSK products under development as Renopharma products and attempted to sell them for billions of dollars. Renopharma's own internal projections showed that the company could be worth as much as $10 billion based upon the stolen GSK data. (Source)

Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets That Cost $120 Million to Develop - May 9, 2022

From December 2012 through Aug. 31, 2017, Dr. Xiaorong You was employed as Principal Engineer for Global Research at Coca-Cola, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various bisphenol-A-free (BPA-free) technologies.

You stole valuable trade secrets related to formulations for BPA-free coatings for the inside of beverage cans. You was granted access to the trade secrets while working at The Coca-Cola Company in Atlanta, Georgia, and Eastman Chemical Company in Kingsport, Tennessee. The stolen trade secrets belonged to major chemical and coating companies including Akzo-Nobel, BASF, Dow Chemical, PPG, Toyochem, Sherwin Williams, and Eastman Chemical Company, and cost nearly $120,000,000 to develop.

You stole the trade secrets to set up a new BPA-free coating company in China. You and her Chinese corporate partner, Weihai Jinhong Group, received millions of dollars in Chinese government grants to support the new company (including a Thousand Talents Plan award). Documents related to You's Thousand Talents Program application were admitted at trial; those documents, and other evidence presented at trial, showed the defendant's intent to benefit not only Weihai Jinhong Group, but also the governments of China, the Chinese province of Shandong, and the Chinese city of Weihai, as well as her intent to benefit the Chinese Communist Party. (Source)

Former Employee Of NASA Contractor Charged With Smuggling And Exporting Sensitive American Aviation Technology To Beijing University - May 26, 2022

Jonathan Yet Wing Soong is charged with smuggling and violating export control laws by allegedly secretly funneling sensitive aeronautics software to a Beijing university.

Soong was employed by Universities Space Research Association (USRA) between April 2016 and September 2020 as a program administrator. USRA is a nonprofit corporation contracted by the National Aeronautics and Space Administration (NASA) to distribute domestically and internationally sensitive aeronautics-related software developed through the Army's Software Transfer Agreement (STA) program. As USRA's STA program administrator, Soong was responsible for overseeing certain software license sales, conducting export compliance screening of customers, generating software licenses, and, on occasion, physically exporting software.

Soong unlawfully and without a license exported and facilitated the sale and transfer of software to Beihang University. (Source)

McDonald's Employee Arrested For Stealing Customer's Credit Card # From Drive-Thru By Taking Pictures - May 14, 2022

Police in Alabama have arrested a fast-food restaurant employee after a customer said their debit card information was stolen.

The investigation started when a customer told them that someone was using their debit card information to make purchases at various businesses.

Detectives narrowed down who had access to the person's information and determined it happened when the card was used at an area McDonald's drive-thru.

The employee, identified as 20-year-old Shytavious Davis, took pictures of the person's debit card before giving it back. Security video confirmed Davis did take pictures of the card. (Source)

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

Insurance Company Executive Sentenced To Prison For Embezzling $5.8+ Million From His Employer / Used FundsTo Purchase Mercedes, Audi, Diamonds, Gold Bars - May 11, 2022

From October 2018 to June 2020, Kevin Mix authorized approximately 42 wire transfers totaling more than $5.8 million from Insureon to his personal bank accounts and the accounts of shell companies that he created.

Mix was Insureon's Accounting Controller and responsible for managing the company's accounting operations. Mix attempted to conceal the fraudulent transfers by making false entries in the company's records, creating fake emails, and making false statements to company representatives and the company's bank.

Mix used the stolen money to purchase, among other things, several real estate parcels in the Chicago area and Ohio, Mercedes-Benz and Audi automobiles, multiple diamonds and gold bars, and membership for a private charter jet service. (Source)

Former Bookkeeper Pleads Guilty To Embezzling $3.1 Million From Employer Over 5 Years / Used Funds For Travel & Investments - May 26, 2022

Nancy Martin admitted to defrauding her employers Mid-Kansas Wound Specialists and Emergency Services P.A.

Martin worked for the businesses as a Bookkeeper, Business Manager, and Chief Operating Officer. An audit revealed that from 2012 to 2017, Martin embezzled approximately $3.1 million by fraudulent obtaining money from her employers' banks. She used funds to pay for personal expenses, travel, and investments then made false accounting entries to disguise the embezzlement as payments or transferred funds between entities. (Source)

Former Chief Financial Officer Charged With Embezzling $2.7 Million - May 5, 2022

Vicki Berka used her position as the Chief Financial Officer and bank account login credentials to embezzle approximately $2.7 million from Bader Rutter & Associates for over three years.

Berka initiated numerous ACH transfers from Bader's corporate accounts into a bank account she controlled and then made false entries in Bader's general ledger to disguise her embezzlement. (Source)

Former General Manager Charged For Embezzling $1.2 Million+ Over 16 Years From Employer - May 2, 2022

Darrel Pike was the General Manager of an Ontario, Calif. subsidiary of a supply and service company based in Wilmington, Mass.

From in or about 2005 to 2021, Pike allegedly prepared and submitted fraudulent invoices to his employer on behalf of a fake temporary staffing company, Consumer Information Systems (CIS), for staffing services CIS purportedly provided at his employer's Ontario location. Pike added approving initials of company personnel to the invoices without their knowledge or consent.

Through the fraudulent invoices, Pike allegedly caused the company to pay approximately $1,271,206 to CIS, which he deposited into a bank account he controlled. (Source)

National Labor Organization Employee Sentenced To Prison For Embezzling $270,000+ From Union / Used Funds To Purchase Clothing, Shoes, Jewelry, Etc. - May 24, 2022

From October 2014 through June 2018, Donnell Owens worked as a Secretary to the Director of Communications at the American Federation of Government Employees (AFGE), a labor organization headquartered in Washington, D.C.

During this period, Owens embezzled more than $270,000 in AFGE funds for his use and the use of others.

Owens submitted false and fraudulent check requests for payments related to services, such as photography and videography, that were purportedly provided by alleged vendors. As a result of these submissions, AFGE funds were subsequently disbursed. These check requests listed fictitious dollar amounts for fake work assignments supposedly performed by vendors, who were not actually hired by AFGE. In fact, the purported vendors who allegedly performed the fake work assignments were really friends and associates of Owens, who he recruited as part of his illegal scheme.

Owens also had access to an Amazon account and a union credit card linked to it. During the scheme, Owens also used this account and linked credit card to embezzle items and make dozens of unauthorized personal purchases, including clothing, shoes, jewelry, and party supplies. Additionally, Owens used union credit cards to purchase items from other online retailers for personal use, including T-shirts for his online business, microphones, and flowers. (Source)

Former Company Accountant Admits To Embezzling $800,00 From Employer For 7 Years - May 4, 2022

Renae Swanson was an accountant and controller for Williams Plumbing & Heating. Swanson's duties included uploading electronic payroll files to the bank for funding and processing payroll transactions to the company's employees.

From about December 2012 until May 2019, Swanson fraudulently altered that process, resulting in her increasing the amount of money she received from Williams Plumbing & Heating, none of which was authorized. The government calculated that Swanson embezzled approximately $805,013. (Source)

Former Chief Financial Officer Of $21 Billion Bio Pharmaceutical Company Charge For Insider Trading - May 10, 2022

From 2018 through October 2020, Usama Malik was the Chief Financial Officer (CFO) of a New Jersey based bio pharmaceutical company listed on the NASDAQ Stock Exchange.

On April 6, 2020, the company publicly announced for the first time that its breast cancer drug – an antibody-based drug designed to treat certain breast cancer patients who had very limited treatment options beyond chemotherapy – had proven effective in pre-market clinical trials. In October 2020, another bio pharmaceutical company acquired the company for which Malik worked for approximately $21 Billion.

Malik was among the first, and one of the few, employees who received the material non-public information about the breast cancer drug before the public announcement.

Within minutes of obtaining that information, Malik passed it along to an individual who lived with Malik at the time, and was formerly employed by the same company as him. The individual more than doubled her investment, realizing gross profits of $213,618, because of the infomration provided to him by Malik. (Source)

General Manager Of Restaurant Embezzled $20,000+ / Had Prior Criminal History With Another Restaurant - May 4, 2022

The restaurant owner Jason Webb says this is just the beginning when it comes to the damage George West has done.

He said the records of the embezzled $20,552 are just what he was able to get quickly to investigators from the past few months. Webb believes the true total will end up being around $100,000 as Webb said most of it came from the money the restaurant received through the Paycheck Protection Program to help offset pandemic setbacks.

West worked on the restaurants food truck at first for about a year. Webb said west was trustworthy and hardworking. Webb say's he trusted West enough to become his general manager.

A few months ago, when Webb started taking a closer look at the financials, suddenly West stopped showing up to work saying he was dealing with his dad's death. After West left, Webb's four employees left too leaving him without a staff.

According to previous reports from The Charleston-Gazette Mail this is not West's first go-around. He worked at the now closed Quarrier Diner in Charleston in 2015, coming from a work-release program on parole after facing fraudulent schemes charges.

He later was accused of writing bad checks and ultimately was blamed for the diner's closure. (Source)

Former Labor Union Secretary-Treasurer Pleads Guilty To Embezzling $30,000 To Pay For Personal Expenses - May 11, 2022

From April 2013 through April 2019, Anthony Jordan worked as the Secretary-Treasurer of the Brotherhood of Locomotive Engineers and Trainmen.

Jordan embezzled funds from the union by writing unauthorized checks to himself from unions checking account, and by making unauthorized direct debits, ATM withdrawals, and cash back transactions from the unions checking account.

Jordan embezzled $30,519.76 from the union. He used the union's funds to pay for personal expenses, such as for veterinary services, utilities, cell phone service, internet and cable, groceries, personal tax returns, convenience store transactions, and more. (Source)

Former Chief Financial Officer Pleads Guilty To Embezzling $433,000+ For 6 Years To Pay Off His Credit Cards - May 12, 2022

David McManus was the Chief Financial Officer for a Hartford-based company for nearly 14 years.

Between 2012 and 2018, McManus embezzled approximately $433,584 from the company by using company funds to pay off his personal credit card expenses, and by issuing reimbursements to himself for personal expenses unrelated to the company. (Source)

Union Financial Secretary Charged With Embezzling $112,00+ Of Union Funds - May 19, 2022

NEW ORLEANS, – BRIAN GERALD, age 50, a resident of Franklinton, Louisiana, was charged today in a one count indictment for embezzling assets of a local labor union in violation of Title 29, United States Code, Section 501(c), announced United States Attorney Duane A. Evans.

Brian Gerlad was the Financial Secretary of United Steelworkers Local 13-189. From on May 25, 2018 and continuing through on or about September 8, 2020, Gerald embezzled $112,594.18 from the union account. (Source)

Former Law Firm Bookkeeper Charged With Embezzling $3 Million+ - May 25, 2022

Janet Blissitt worked as a bookkeeper and assistant at a law firm in Boca Raton, Florida. She had access to several of the firm's business bank accounts, including the firm's client trust accounts.

Starting in October 2021 and continuing through March 2022, Blissitt transferred money from several of the law firm's business accounts to her personal account and other business bank accounts in New Jersey and Ohio. Blissitt would sometimes falsely note that the purpose of the transfers was to pay fees. Blissitt embezzled an estimated $3 million from the law firm. (Source)

NETWORK / IT SABOTAGE

Disgruntled IT Administrator Wipes Employer's Databases / Causing Severe Impacts - Sentenced To 7 Years In Prison - May 15, 2022

Han Bing is a former Database Administrator for Lianjia, a Chinese real-estate brokerage giant. He has been sentenced to 7 years in prison for logging into corporate systems and deleting the company's data.

Bing allegedly performed the act in June 2018, when he used his administrative privileges and "root" account to access the company's financial system and delete all stored data from two database servers and two application servers.

This has resulted in the immediate crippling of large portions of Lianjia's operations, leaving tens of thousands of its employees without salaries for an extended period and forcing a data restoration effort that cost roughly $30,000.

The indirect damages from the disruption of the firm's business, though, were far more damaging, as Lianjia operates thousands of offices, employs over 120,000 brokers, owns 51 subsidiaries, and its market value is estimated to be $6 billion.

According to documents released by the court of the People's Procuratorate of Haidian District, Beijing, H. Bing was one of the five main suspects in the data deletion incident.

Bing had repeatedly informed his employer and supervisors about security gaps in the financial system, even sending emails to other administrators to raise his concerns.

However, he was largely ignored, as the leaders of his department never approved the security project he proposed to run.

This was confirmed by the testimony of the Director of Ethics at Lianjia, who said Bing felt that his organizational proposals weren't valued and often entered arguments with his supervisors. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Employee Pleads Guilty To Leading Role In $29 Million+ Kickback Scheme - May 4, 2022

Eugene DiNoto was a longtime employee of his company, a family-owned global business headquartered in New York, but with manufacturing facilities in Belcamp and Abingdon, Maryland.

Beginning in 2012, DiNoto and another employee, Elliott Kleinman, began to use their management positions at the company to execute a fraudulent billing scheme whereby they would get illegal kickbacks from various vendors doing business with the company, which used drums to store and transport its products. As the facility managers, DiNoto and Kleinman oversaw the purchasing and storing of drums for use at the Harford County manufacturing facilities. They also had authority to review drum invoices and authorize payments to the drum vendors. (Source)

Former Mercyhealth Vice President Of Marketing Sentenced To Prison For Role In $3.1 Million Kickback / Fraud Scheme - May 4, 2022

Between 2015 and 2020, Barbara Bortner and co-defendant Ryan Weckerly engaged in a kickback scheme in which Weckerly submitted inflated invoices to Bortner for his marketing work for Mercyhealth. Once Bortner approved his marketing invoices, Weckerly received payments from Mercyhealth and provided money to Bortner using either cash or checks. In return for the payments, Bortner agreed to use Weckerly's business, Morningstar Media Group, as the primary marketing agency for Mercyhealth.

In order to disguise the true nature of the kickback payments, Bortner created a fictitious company named WeInspire LLC. During the timeframe of the kickback scheme, Weckerly wrote over 103 checks to WeInspire LLC from one of his business accounts. The cumulative total of these checks was $2,051,975. In addition, bank records show that Weckerly provided Bortner with over $1,000,000 in cash kickback payments. Based on the government's financial analysis of Weckerly's accounting and bank records, the total monetary amount of the fraud was $3,136,200.72. (Source)

Roofing Company Vice President & Co-Conspirators Sentenced To Prison For Stealing $1.8 Million+ In Fake Invoice Billing Scheme - May 2, 2022

Baker Roofing Company (BRC) hired George Garven in 2011 to serve as the Vice President and General Manager of its Charlotte branch office.

In 2014, Robert Helms and William Davis partnered together to provide roofing subcontracting services to BRC through Davis's business, R&K Davis Holdings (R&K).

Between 2015 and 2020, R&K was used as a vehicle to fraudulently bill BRC for subcontracting work that was never performed.

Garven obligated BRC to pay R&K by generating fake invoices and subcontracts in R&K's name. The criminal proceeds, were funneled into business bank accounts controlled by Helms and Davis and then disbursed to Garven in various forms, including gift cards and checks. The checks included fraudulent memo lines to make it appear they were related to legitimate business. Garven also directed Helms and Davis to use the embezzled funds to pay contractors to perform work on Garven's residential properties. In furtherance of the scheme, Garven paid Helms and Davis each approximately $140,000 in cash. (Source)

Former Employee Pleads Guilty In Role To Steal $1.8 Million+ From Employer To Fund Investments & Personal Business - May 6, 2022

Duane Larmore, worked for Shore Appliance Connection. Larmore duties included maintaining the books and records for the company.

From September 2016 through March 2020, Larmore conspired with others to steal more than $1.8 million from Shore Appliance Connection.

Larmore and his co-conspirators stole over $1 million from Shore Appliance to use for their own purposes, including to make investments and to pay business expenses for the co-conspirator's business. (Source)

Former U.S. Golf Association Employee Sentenced To Prison For Role In Stealing 23,000+ Tickets Worth $3 Million+ And Then Selling Them Over 7 Years - May 11, 2022

Robert Fryer was employed by the United States Golf Association (USGA) in its Admissions Office.

Beginning in 2013 in connection with the U.S. Open held at the Merion Golf Club, while working for the USGA in their admissions office, Fryer realized that he could exploit a weakness in the USGA's ticket tracking protocol and steal tickets to the U.S. Open without the knowledge of the USGA.

Rather than notify his employer of this flaw, Fryer admitted that he stole thousands of U.S. Open tickets in connection with the U.S. Open at Merion. Fryer arranged to sell the stolen tickets to Jeremi Conaway, who at the time worked for another ticket brokerage in the area. Fryer continued to steal and sell tickets to Conaway for every subsequent U.S. Open through 2019, and he would have stolen tickets to the 2020 U.S. Open except it was held without fans that year due to the pandemic. Fryer admitted to stealing more than $3 million worth of U.S. Open tickets and selling them for approximately $1.2 million to his two co-conspirators, who themselves sold the tickets for a profit. (Source)

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 - May 19. 2022

Chenyan Wu and Lianchun Chen, a married couple who worked as research scientists for a major American pharmaceutical company, pleaded guilty to criminal charges stemming from their efforts to gather confidential mRNA research from that company to advance the husband's competing laboratory research in China.

The couple has been married since at least 1993. During his career, Wu had worked for multiple pharmaceutical companies, including the major one identified in court records only as Company A, where his wife also worked. In 2010, Wu moved to China, and in 2012, he opened a laboratory there, which he named TheraMab. TheraMab focused on mRNA vaccine research.

While her husband was in China, Chen remained in the United States, working for Company A in San Diego from at least 2012 through September 9, 2021. During that time, her research for Company A focused on mRNA vaccines.

From as early as November 2013, through at least June 2018, Chen repeatedly accessed Company A computers and copied confidential Company A materials. Chen emailed those confidential Company A materials to her husband in China over her personal Hotmail account.

These confidential Company A materials included PowerPoints and Word documents with DNA and mRNA sequencing data, marked Company A Confidential. By 2013, Wu was no longer employed by Company A. He had started TheraMab, a competing laboratory in China focused on mRNA research. (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

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

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 (**3,700+ 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