INSIDER THREAT INCIDENTS REPORT
FOR
October 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

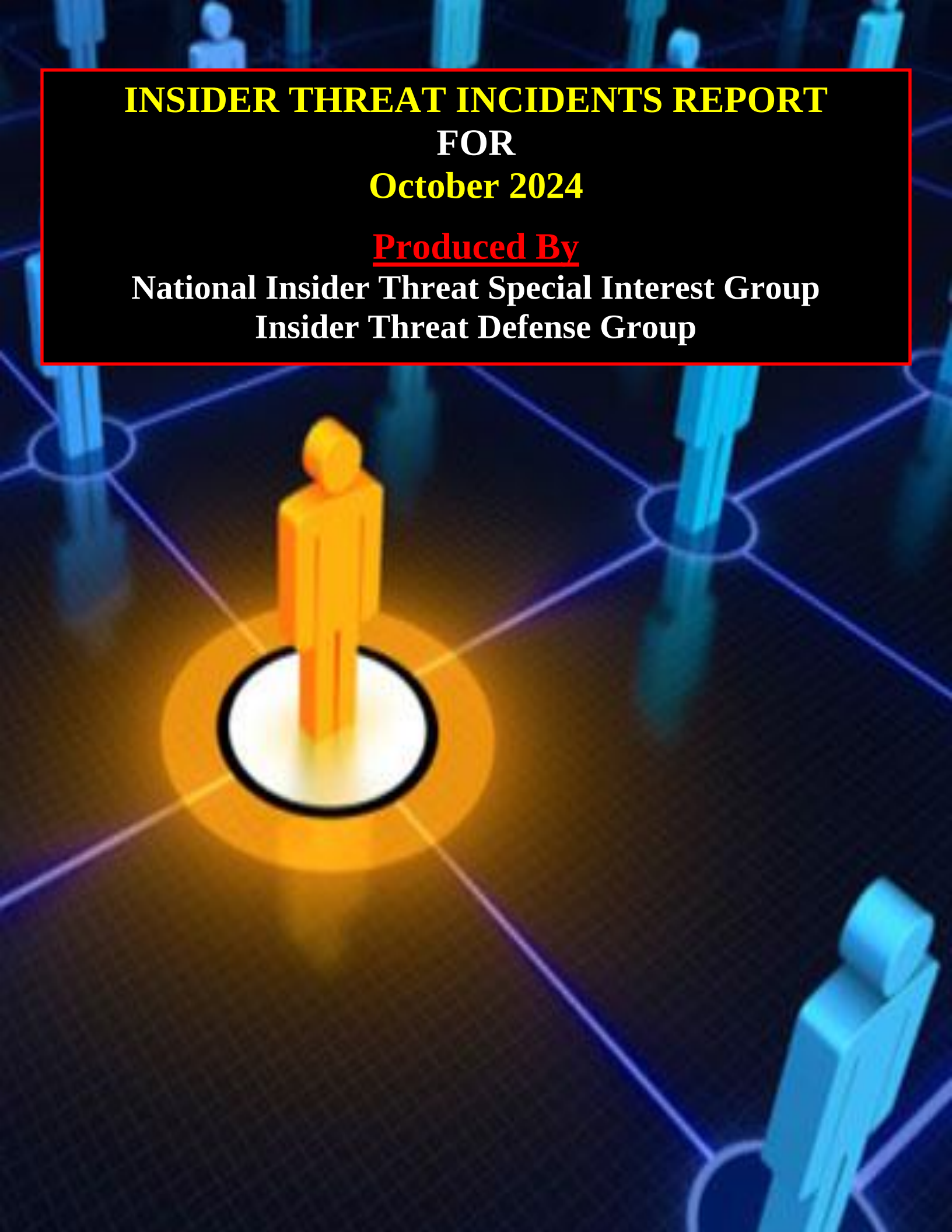

TABLE OF CONTENTS

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 are negligent, malicious or opportunists. 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 15+ years. This research has evaluated and analyzed over **5,800+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

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. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

According to the Association of Certified Fraud Examiners 2024 Report To the Nations, the 1,921 fraud cases analyzed, caused losses of more than **$3.1 BILLION.**

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

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

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

The Human Operating System (Brain) is very sophisticated and underestimating the motivations and capabilities of a malicious or opportunist employee can have severe impacts for organizations.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report and other shows. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 26** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR OCTOBER 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT

5 IRS Employees Sentenced To Prison For $1 Million+ COVID-19 Relief Fraud Scheme / Used Funds To Purchase Cars, Travel, Etc. - September 30, 2024

Brian Saulsberry was employed by the IRS as a Program Evaluation and Risk Analyst in the Human Capital Office in Memphis, Tennessee. Saulsberry laundered funds he received from a scheme to defraud the Economic Injury Disaster Loan (EIDL) program, a federal stimulus program authorized to provide loans to small businesses experiencing substantial financial disruptions due to the COVID-19 pandemic as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Saulsberry submitted false EIDL applications and obtained $171,400 in loan funds. After obtaining the fraudulent loan funds, Saulsberry transferred the funds to his personal checking account. He then used the loan funds for purposes not authorized by the EIDL Program, but instead transferred $100,000 to an investment account, knowing that the property involved in the transaction was derived from unlawful activity.

In addition to Saulsberry, four other former IRS employees, Courtney Westmoreland, Fatina Hewitt, Roderick White and Tina Humes were convicted for defrauding federal stimulus programs authorized as part of the CARES Act, including the EIDL Program and the Paycheck Protection Program.

The five former federal employees collectively sought over $1 million. They then used the loan funds to invest in personal accounts, purchase cars and luxury goods, and pay for personal travel, including trips to Las Vegas. (Source)

United States Department of Agriculture Employee Sentenced To Prison For Role In $1 Million Contracting Fraud Scheme To Benefit His Private Company - October 25, 2024

Ifediora Oli, an employee of the United States Department of Agriculture (USDA), was sentenced to prison for conspiring with two local government officials to defraud the District of Columbia and the Washington Metropolitan Area Transit Authority (WMATA) of money, property, and their employees' honest services. As a result of the conspiracy, a private company owned and operated by Oli improperly received over $1 million. Between 2018 and 2023 Oli was employed at USDA while separately acting as the Principal of Highbury Global Group, Inc. (Highbury).

Obinna Ogbu was employed at WMATA as an information technology (IT) customer support manager who sometimes also served as a WMATA contracting officer's technical representative (COTR) on certain WMATA contracts. Bridgette Crowell was a public employee who managed contracts at the District's Office of Contracting and Procurement (OCP) and, before that, WMATA.

Beginning in 2018, Oli and Ogbu agreed to use Ogbu's official position and connection to Crowell to steer funds from WMATA IT-related contracts to Highbury. As part of the conspiracy, Oli and Ogbu agreed to commit bribery. Specifically, Oli and Ogbu agreed that Oli would give Ogbu things of value in exchange for Ogbu misusing his position at WMATA to benefit Oli. By 2023, Oli and Highbury had received nearly $500,000 through this corrupt scheme. (Source)

U.S. Postal Service Employee Admits To Stealing $46,000+ Of Money Orders - October 3, 2024
Tanya Lee Holbrook began working as a postmaster of the Gardiner post office in Montana in September 2022.

In February 2023, the manager of postal operations in Montana contacted the U.S. Postal Services Office of Inspector General regarding concerns that Holbrook was stealing office bank deposits.

An investigation determined that Holbrook routinely issued money orders to herself and others but did not submit the funds for them to USPS. Between November 2022 and September 2023, Holbrook delayed approximately 48 bank deposits, totaling $46,755, from the Gardiner post office. While Holbrook usually sent the cash later when she was paid, she never provided funds for eight deposits, which totaled $24,443, from January 2023 to September 2023. When interviewed, Holbrook confessed to the thefts. Holbrook stated that she issued herself or family members money orders without remitting payment and then delayed sending the funds. Holbrook eventually fell so far behind that she was unable to pay for several deposits. (Source)

U.S. Postal Service Employee Arrested For $10,000 COVID Relief Fraud - October 23, 2024
During the COVID pandemic, the United States Small Business Administration (SBA) offered Targeted Economic Injury Disaster Loan (EIDL) Advances that did not need to be repaid. The advances were for small businesses that were in low-income communities and received a reduction in revenue of more than 30% during an eight-week period.

Between June 28 and 30, 2020, Brooks Stewart devised a scheme to defraud the SBA by electronically applying for an EIDL advance and providing false representations in her application. Afterwards, she fraudulently received a $10,000 EIDL advance. (Source)

U.S. Postal Service Employee Sentenced To Prison For Stealing $5,000 Worth Of Cash & Gift Cards From Mail - October 9, 2024
Justin Crain was employed as a U.S. Postal Service Mail Processing Clerk at its Indianapolis Processing and Distribution Center.

The Postal Service's Office of Inspector General began an investigation after it identified numerous mail items that passed through the Indianapolis processing center and had been opened before being delivered to their intended recipients. Video surveillance captured Crain opening numerous greeting cards and removing cash and gift cards from inside.

Over the course of just two hours, Crain was seen dozens of times rifling through mail items attempting to find cash. Crain was interviewed by investigators and admitted to stealing approximately $5,000 over the course of a few months. (Source)

U.S. Postal Service Manager Who Stole Drugs From Mail, Shared With Co-Worker Sentenced To Prison On Drug & Gun Charges - October 25, 2024
On multiple occasions between May 2018, and May 2, 2022, Ralph Minni used his position as the post office station manager to take parcels containing controlled substances, such as marijuana, out of the mail stream and into his private office, remove the contents, and then return the empty packages back into the mail stream.

Minni then transported the controlled substances to his residence, where he would store and redistribute the narcotics to other individuals. On three occasions in March and April of 2022, Minni distributed quantities of cocaine to a coworker, who then proceeded to snort the cocaine off Minni's office desk in his presence.

On May 2, 2022, a search warrant was executed at Minni's residence during which investigators recovered quantities of marijuana, approximately 700 grams of cocaine, approximately 40 firearms, and over 19,000 rounds of ammunition. Minni was arrested that same day after leaving the Greece Post Office. Officers recovered a quantity of marijuana from inside his vehicle, which he had removed from a mailed package and planned to take back to his residence for subsequent sale and distribution. (Source)

Former U.S. Postal Carrier Indicted For Throwing Baskets Of Mail Into Trash Dumpster - October 3, 2024

On August 3, 2024, DuJuan Butler was driving a U.S. Postal Service truck while delivering the mail in Antioch, Tennessee.

A woman happened to look out her window and saw Butler take baskets of mail from the Postal truck and throw them into dumpsters behind a strip mall. The woman filmed Butler and then uploaded her video to TikTok where it was viewed millions of times. Other Postal Service employees were later able to recover the discarded mail from the dumpsters. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Defense Contractor Acting As Front Company Sentenced To Prison For Fraudulently Selling Military Components To DoD & Money Laundering - October 24, 2024

Yuksel Senbol was sentenced to 15 months in prison for conspiracy to defraud the United States, conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, money laundering, conspiracy to violate the Export Control Reform Act, violating the Export Control Reform Act, and violating the Arms Export Control Act. Senbol entered an order of forfeiture in the amount of $275,430.90, the proceeds of Senbol's fraud and money laundering scheme.

Beginning in approximately April 2019, Senbol operated a front company in the Middle District of Florida called Mason Engineering Parts LLC. She used this front company to assist her co-conspirators, Mehmet Ozcan and Onur Simsek, to fraudulently procure contracts to supply critical military components to the Department of Defense. These components were intended for use in the Navy Nimitz and Ford Class Aircraft Carriers, Navy Submarines, Marine Corps Armored Vehicles, and Army M-60 Series Tank and Abrahams Battle Tanks, among other weapons systems.

In order to enable Ozcan and Simsek to manufacture the components in Turkey, Senbol assisted them in obtaining sensitive, export-controlled drawings of critical U.S. military technology. Using software that allowed Ozcan to remotely control her computer — and thus evade security restrictions that limited access to these sensitive military drawings to computers within the United States — Senbol knowingly facilitated the illegal export of these drawings.

Once Ozcan and Simsek manufactured the components in Turkey, they shipped them to Senbol, who repackaged them — making sure to remove any reference to their Turkish origin. The conspirators then lied about the origin of the parts to the U.S. government and a U.S. government contractor to receive payment for the parts. Senbol then laundered hundreds of thousands of dollars in criminal proceeds back to Turkey through international wire transfers. (Source)

Navy Chief Petty Officer Pleads Guilty To Stealing & Selling $164,000+ Of Military Equipment - October 28, 2024

Shawn Crowell was assigned to Helicopter Sea Combat Wing Atlantic at Naval Station Norfolk from December 2022 to September 2024. Crowell had access to and was responsible for the inspection and inventorying of the military equipment belonging to the Command.

From at least January through June 2023, Crowell stole numerous government items, including seven sets of Night Vision Goggles (NVGs, or NODs), two Matbock Tarsier Eclipse lenses, and eight NVG battery packs. The value of the items stolen by Crowell was at least $164,646.

Between February and May 2023, Crowell used online advertisements to sell five sets of the stolen NVGs to third-party purchasers for $19,947. On March 8, 2023, Crowell listed for sale the two Matbock Tarsier Eclipse lenses, which are regulated by the International Trafficking in Arms Regulations (ITAR). Crowell sold the stolen lenses for $300. On April 1, 2023, Crowell sold the eight NVG battery packs for $500. (Source)

Defense Contractor Acting As Front Company Sentenced To Prison For Fraudulently Selling Military Components To DoD & Money Laundering - October 24, 2024

Yuksel Senbol was sentenced to 15 months in prison for conspiracy to defraud the United States, conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, money laundering, conspiracy to violate the Export Control Reform Act, violating the Export Control Reform Act, and violating the Arms Export Control Act. Senbol entered an order of forfeiture in the amount of $275,430.90, the proceeds of Senbol's fraud and money laundering scheme.

Beginning in approximately April 2019, Senbol operated a front company in the Middle District of Florida called Mason Engineering Parts LLC. She used this front company to assist her co-conspirators, Mehmet Ozcan and Onur Simsek, to fraudulently procure contracts to supply critical military components to the Department of Defense. These components were intended for use in the Navy Nimitz and Ford Class Aircraft Carriers, Navy Submarines, Marine Corps Armored Vehicles, and Army M-60 Series Tank and Abrahams Battle Tanks, among other weapons systems.

In order to enable Ozcan and Simsek to manufacture the components in Turkey, Senbol assisted them in obtaining sensitive, export-controlled drawings of critical U.S. military technology. Using software that allowed Ozcan to remotely control her computer — and thus evade security restrictions that limited access to these sensitive military drawings to computers within the United States — Senbol knowingly facilitated the illegal export of these drawings.

Once Ozcan and Simsek manufactured the components in Turkey, they shipped them to Senbol, who repackaged them — making sure to remove any reference to their Turkish origin. The conspirators then lied about the origin of the parts to the U.S. government and a U.S. government contractor to receive payment for the parts. Senbol then laundered hundreds of thousands of dollars in criminal proceeds back to Turkey through international wire transfers. (Source)

United States Army Reservist Pleads Guilty To Stealing $11,000+ Of Government Funds - September 30, 2024

United States Army Reservist Cody Francis pled guilty to conspiracy to commit theft of government funds. Francis stole $11,378.27 from the United States Department of the Army, by claiming reimbursement for performing military funeral honors ceremonies that never actually happened. (Source)

Department of Defense Employee Pleads Guilty To Mishandling Classified Materials - October 23, 2024
Starting in March 2020, Margaret Ashby was a civilian employee of a Department of Defense component agency located in the Southern District of Georgia, and during this time held a top secret security clearance as required for her employment.

From February 2022 to May 2022, Ashby, without authority, knowingly removed documents and materials containing classified information "concerning the national defense or foreign relations of the United States . . . with the intent to retain them at unauthorized locations, including her residence in the Southern District of Georgia and in digital files saved via a personal computing device located in the Southern District of Georgia." (Source)

Naval Officer Sentenced To Prison For Afghan Visa Bribery Scheme - October 28, 2024
Cmdr. Jeromy Pittmann, a U.S. Navy Reserve officer was sentenced to more than two years in prison for his role in a years-long bribery scheme involving Special Immigrant Visas (SIVs) for Afghan citizens.

Pittmann served as a civil engineer corps officer who deployed to Afghanistan with NATO Special Operations Command.

Pittmann received several thousands of dollars in bribes from Afghan nationals in exchange for drafting, submitting and verifying fraudulent letters of recommendation for Afghan citizens who applied for SIVs with the State Department.

To avoid detection, Pittmann received the bribe money through an intermediary and created false invoices showing that he was receiving the funds for legitimate work unrelated to his military service.

The State Department offers a limited number of SIVs to enter the United States. Pittman signed more than 20 letters stating he knew and supervised Afghan national applicants while they worked as translators in support of the U.S. military and NATO. (Source)

12 U.S. Department Of Veterans Affairs Employee Under Investigation For Unauthorized Access To The Medical Records Of Both Vice Presidential Nominees - September 30, 2024
At least a dozen staffers at the U.S. Department of Veterans Affairs improperly accessed the medical records of both vice presidential nominees, Republican Sen. JD Vance, of Ohio, and Democratic Minnesota Gov. Tim Walz, over the summer.

Those employees are under criminal investigation for potentially violating federal health privacy laws. The unauthorized views were uncovered by Veterans Affairs investigators, who notified the Vance and Walz campaigns.

Law enforcement officials stated that the VA Inspector General Michael Missal's office shared evidence with federal prosecutors related to several health system employees, including a physician and a contractor who

"spent extended time" viewing the medical files of former President Donald Trump and Vice President Kamala Harris' running mates.

The VA employees under investigation, including the physician and contractor, accessed the medical records using their VA computers and did so mostly from their government offices.

Some of the staffers in question reportedly told investigators they were simply curious to see the files of Vance and Walz given both candidates have defended their military records on the campaign trail. (Source)

CRITICAL INFRASTRUCTURE

Pennsylvania Water Authority Manager Pleads Guilty To Diverting $1 Million+ Into Personal Bank Account - October 9, 2024

Michael Dominick is the former manager at the Ambridge Water Authority (AWA). He defrauded AWA of money and property totaling approximately $1,073,185 during the period of January 2020 through August 2022.

As manager of AWA, Dominick was responsible for overseeing all daily business and financial activity and thus had access to AWA's bank accounts and cash and check payments made to AWA for water and related services. Dominick admitted that he secretly diverted AWA's money into his own personal bank accounts by writing checks to himself, depositing cash and checks issued to AWA into his personal bank accounts, using an AWA debit card to make purchases of personal items, and adjusting or failing to report the true location of AWA's funds on critical financial records. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

FBI Special Agent Charged In $1 Million+ Foreign Currency Trading Scam - October 17, 2024

Jeffrey Royer was a Special Agent with the FBI from approximately 1996 to 2001.

In 2005, Royer was convicted of federal securities fraud, among other charges, and was released from federal prison in 2012 after serving his sentence of imprisonment.

From early 2020 through June 2023, Royer executed an investment fraud scheme involving his personal forex trading account. As part of the scheme, Royer fraudulently solicited and accepted over $1 million from various investors in the Eastern District of Michigan and elsewhere. He then misappropriated the money or lost it trading forex. Royer did not disclose the misappropriation or the extent of his trading losses. Instead, Royer concealed the truth from investors, including by providing investors with false monthly account statements that showed investment gains rather than the trading losses that Royer actually incurred. (Source)

Customs & Border Protection Officer Sentenced To Prison For Receiving Bribes From Drug Cartel To Allow Drug-Laden Vehicles Into U.S. - October 28, 2024

During the trial, several witnesses testified that Leonard George agreed to allow drug-laden vehicles to enter the U.S. through his lane in late 2021. George would notify members of a drug trafficking organization when he was at work, what lane he was on, and that they had one hour to reach his lane. However, in February 2022, after an alert placed by law enforcement agents on a suspected drug smuggling vehicle was flagged entering George's Lane, George was forced to send the vehicle to secondary inspection, later revealing approximately 222 pounds of methamphetamine.

Undeterred, George allowed a second drug-laden vehicle affiliated with the drug trafficking organization and traveling directly behind the flagged vehicle to enter the U.S. with over 200 pounds of drugs. Text messages sent by George the following day reveal he received approximately $13,000 for the vehicle he allowed to enter the U.S. On the same day he received his bribe payment, George purchased a 2020 Cadillac CT5 for an associate of the drug trafficking organization as a gift. George delivered the Cadillac CT5 to the associate in Ensenada on Valentine's Day.

Over the course of six months, George continued to allow vehicles containing undocumented individuals to enter the U.S. through his lane. George repeatedly omitted passengers and the true names of drivers coming through his lane, instead entering the names of others to conceal his criminal activities. Law enforcement agents and prosecutors identified approximately 19 crossings associated with the criminal organizations during the six-month time period. Text messages confirmed George agreed to allow vehicles through his lane for $17,000 per vehicle, $34,000 for two vehicles, $51,000 for three vehicles, or $65,000 for four vehicles. One text message confirmed that George received $68,000 after he allowed four vehicles from one organization to enter his lane in June 2022.

Testimony from a witness confirmed that George purchased vehicles, motorcycles, and jewelry with the proceeds of his illicit activities. On George's days off, he travelled to Tijuana to visit Hong Kong Gentlemen's Club where he spent approximately $5,000 per trip. He would stand on the second level of the club and throw cash over the balcony to the dancers below, "showering" them with money. He would also buy bottles of alcohol, and occasionally gifts, for dancers. (Source)

Customs & Border Protection (CBP) Employee Pleads Guilty To Stealing $67,000+ Worth Of Laptop And Attempting To Sell - October 22, 204

On Dec. 13, 2023, Xavier Mittakarin removed the 27 laptops, valued at a total of over $67,000, from the facility, intending to sell them. On March 22, 2024, Mittakarin sold one of the laptops via eBay to a purchaser in California, who paid $2,803.26. On May 22 and May 27, Mittakarin sold eight more laptops via eBay to another purchaser in California, who paid a total of $16,706.76.

On Aug. 1, Mittakarin attempted to sell 18 laptops to another purchaser, who was actually an undercover officer, for approximately $28,000. Mittakarin brought the laptops to a prearranged meeting place and time, where he was arrested and the laptops were recovered from his vehicle. (Source)

Former Drug Enforcement Administration Employee Pleads Guilty To Embezzling $75,000+ - October 25, 2024

In September 2023, after 16 years of employment with the DEA, Scott Knox embezzled over $75,000 from a DEA vault to which he had access and control by virtue of his position as a Mission Support Specialist and Account Technician with the DEA in Phoenix.

In this role, his responsibilities included safeguarding the DEA Imprest Fund, which is a designated cash reserve for managing recurring DEA expenses, including operational funds utilized by agents in the field. Knox admitted that he deliberately stole $75,546 in cash from the Imprest Fund secure room. Knox attempted to conceal his actions from the DEA, but his embezzlement was uncovered during an internal audit the DEA conducted in March 2024. (Source)

Former High-Ranking New York City Fire Department Official Pleads Guilty To $190,00 Bribery Conspiracy - October 8, 2024

From 2021 to 2023, Brian Cordasco repeatedly abused his position as a Chief of the New York Bureau of Fire Prevention (BFP) by participating in a scheme to solicit and receive $190,000 in total bribe payments from a former FDNY firefighter named Henry Santiago, Jr.

In exchange for those bribe payments, Cordasco used his authority within the BFP to improperly "expedite" BFP inspections and plan reviews for Santiago's customers. Cordasco personally profited $57,000 as part of this scheme.

To carry out this conspiracy, Cordasco lied to his BFP subordinates to justify otherwise improper expediting requests. Cordasco also lied to law enforcement when interviewed about his involvement in the scheme. (Source)

Former Correctional Officers Sentenced To Prison For Using Inmates Stolen Identities In $331,000+ Fraud Scheme - October 28, 2024

Between on or about 2015 and their arrest date in January 2019, Martins Chidiobi and Lawrence Onyesonwu worked as Correctional Officers at the New Castle Correctional Facility, a privately managed prison within the Indiana Department of Corrections.

During that time, Chidiobi and Onyesonwu stole at least five inmates' personally identifiable information, including names, dates of birth, and social security numbers. The defendants used the stolen identities of the victim inmates to open at least nine accounts at various Indiana banks using fraudulent passports. The fraudulent passports were purportedly issued by Nigeria, Liberia, and Ghana, and included pictures of the defendants, but the names and other information of the identity theft victims.

The accounts opened by the defendants with the stolen identities were then used to receive the proceeds of broader fraud schemes. A total of at least $331,282 was deposited into the defendants' fraudulent bank accounts from at least 11 sources. Investigators worked to identify and contact individuals who deposited funds into fraudulent accounts. Of the eleven depositors able to be identified, each was themselves the victim of a "romance scam" or other fraud scheme. Further investigation revealed that the defendants also received deposits of apparent fraud proceeds into their own personal bank accounts.

The vast majority of the over $331,282 in apparent fraud proceeds received by the defendants was withdrawn as cash. A large portion of the money was transferred into Nigerian bank accounts. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

County Supervisor Plead Guilty To Accepting $550,000 In Bribes For $10 Million COVID Relief Funds Fraud Scheme - October 22, 204

The supervisor on the Orange County Board of Supervisors (Andrew Hoang Do) has agreed to plead guilty to a felony federal charge for accepting more than $550,000 in bribes for directing and voting in favor of more than $10 million in COVID funds to a charity affiliated with one of his daughters, Rhiannon Do.

Andrew Hoang Do admitted that in exchange for more than $550,000 in bribes, beginning in 2020, he voted in favor of and directed millions of dollars in COVID-related funds to Viet America Society (VAS), a charity

affiliated with his daughter. Andrew Hoang Do directed and worked together with other county employees to approve contracts with – and payments to – VAS.

Some of the bribe funds that had been funneled to his daughters were spent for his direct benefit. For example, during 2022, a total of $14,849 of funds that had been funneled to Do's daughters was used to make property tax payments for properties in Orange County owned by Do and his wife. Approximately $15,000 was used to pay for one of Do's credit card bills. (Source)

Massachusetts Department Of Housing & Community Development Employee Pleads Guilty To $443,000+ Fraud Scheme - September 30, 2024

In 2022, Alihea Jones worked remotely for the Massachusetts Department of Housing and Community Development (DHCD) for six months where she worked with the Residential Aid to Families in Transition (RAFT) program, which provides funds to assist low-income Massachusetts residents facing eviction and other housing emergencies.

Immediately after she was terminated, Jones, who was still logged into the RAFT database, accessed the files of four RAFT program participants and authorized electronic payments to their landlords in the amounts of $7,500, $8,800, $6,925 and $10,000. However, Jones changed the routing and bank account numbers from the landlords' accounts to four unauthorized accounts in Georgia: an account in the name of Jones's business, Beauty Concepts by Alihea, LLC (Beauty Concepts); Jones's personal account; and the accounts of persons identified in the charging document as "Friend A" and "Friend B" – all without knowledge or permission from DHCD. After these transfers went through, Friend A and Friend B each paid Jones a $2,000 kickback.

Earlier, in 2021, Jones also fraudulently obtained a $187,000 PPP loan from a Massachusetts lender, which the SBA later forgave. (Source)

Employee Sentenced To Prison For Stealing $430,000+ From San Diego Regional Economic Development Corporation Over 5 Years - October 17, 204

Katherine Lu Acquista, the former Director of Operations and Accounting for the San Diego Regional Economic Development Corporation (EDC), was sentenced in federal court to 12 months in prison for stealing approximately $433,275.89 from her then-employer. She was also ordered to pay a fine of $50,000.

While employed at EDC, Acquista used her access and authority to put personal expenses on EDC credit cards and pay those expenses using EDC funds.

She also directed other employees to issue checks to her from the EDC company bank account. She then caused false entries about these transactions to be made in the EDC's accounting system to disguise her ongoing theft. In addition, she stole from EDC's flexible spending and payroll system. All told, she exploited her position of trust to steal more than $430,000 over at least a five-year period, between August 2017 and August 2022. (Source)

Las Vegas City Councilwoman Convicted In $70,000+ Charity Fraud Scheme / Used Funds For Rents Payment, Etc. - October 4, 2024

Michele Fiore while serving as a Las Vegas city councilwoman, solicited donors for money to build statues honoring two Las Vegas police officers who had been killed in the line of duty.

The evidence at trial demonstrated that Fiore promised donors that "100% of the contributions" would be used towards the construction of memorials for the fallen officers. However, Fiore did not use any of the more than $70,000 in charitable donations she raised for the memorials. Instead, Fiore spent the money donated by the victims on a variety of personal and political expenses, including political fundraising bills, personal rent payments, and payments to family members. (Source)

Real Estate Developer Sentenced To Prison For Paying $85,000+ In Bribes To Mayor - October 24, 2024
Between 2016 and 2018, Shady Awad provided a steady stream of bribes to a Mayor (Richard Sollar) in Michigan. The bribes were in the the form of cash, home improvements to Sollars' home and lake house, appliances, and other items of value.

Awad also agreed to charge more than $19,000 to his credit cards, and then convert the charges to cash for Sollars. In total, Awad provided Sollars with goods and services valued at $85,011.73, in exchange for being permitted to acquire tax-foreclosed properties to redevelop through the City of Taylor's Right of First Refusal (ROFR) program. This was a program designed to allow Taylor to acquire tax-foreclosed properties from Wayne County for redevelopment. As a result of the bribes Awad paid to Sollars, Sollars recommended to City Council that Awad be awarded the vast majority of the City's ROFR properties. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Employee Pleads Guilty To Embezzling $135,000+ From School District - October 29, 2024
Linda Johnson admitted guilt to embezzling more than $135,000 as a former employee of Dupo Community Unit School District #196.

Johnson committed the embezzlement while employed in an administrative support role in the superintendent's office between 2020 and 2022. In this role, Johnson was responsible for depositing cash and checks into the district's activities account intended to support student athletics, clubs, and extracurriculars.

To conceal her crime, she would prepare bank deposit slips reflecting the correct amount of cash and checks received, but later she prepared a second set of fraudulent deposit slips that only accounted for the checks, while she kept the cash. (Source)

School Janitor Allegedly Used Artificial Intelligence To Create Child Pornography With Students' Faces - October 11, 2024
Daril Gonzales worked as a janitor for the Anson Independent School District in Texas. Gonzales also moonlighted as a school sports and cheerleading photographer, taking pictures of middle and high school students for free.

Without the children's consent, he allegedly used artificial intelligence (AI) to superimpose the faces of pre-pubescent students onto the faces of adult subjects in sexually explicit videos or to attach AI-generated nude bodies to the faces of the girls.

According a police report admitted into evidence at the detention hearing, Mr. Gonzales allegedly described his crimes as a "power trip" and admitted to viewing child pornography for up to six hours per day for the past 20 to 25 years. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Union Treasurer Sentenced To Prison For Embezzling $44,000+ - October 2, 2024

Donald Byers was the treasurer of the Brotherhood of Locomotive Engineers Division 287. From

June 2017 through December 2020, Byers used his position to embezzle over $44,000 of union money by issuing more than 50 unauthorized checks to himself. Byers also falsified a financial report filed with the Department of Labor's Office of Labor-Management Standards and forged the signature of a union officer on many of the checks.

Prior to imposing sentence, Judge Colville stated that Byers's crime was serious and that incarceration was warranted because of Byers's criminal history, among other factors. (Source)

Chairman For D.C. Department Of Corrections Union Pleads Guilty To Embezzling $30,000 / Used Funds Himself & Friends - October 30, 2024

Andra Parker is a former D.C. Corrections officer, who served as Chairman of the Labor Committee, an organization that represents all members of the D.C. Department of Corrections.

As Chairman, Parker had full access to the Labor Committee's bank accounts to carry out his official duties and was issued a debit card.

As part of his guilty plea, Parker admitted that he misappropriated more than $30,000 of union funds to pay for unofficial travel, lodging, and entertainment for him and his friends. Parker spent more than $7,000 on a trip to New York city for his friends and him, including $4,000 on rooms and expenses at a Times Square hotel, more than $370 on tickets to a New York Knicks game, and an additional $616 on tickets to Summer: The Donna Summer Musical. He also spent more than $2,000 in union funds to purchase four tickets to a Diana Ross concert in North Bethesda, Maryland. (Source)

BANKING / FINANCIAL INSTITUTIONS

TD Bank Pleads Guilty To Money Laundering Conspiracy By Bribed Employees / FINED $1.8 BILLION - October 10, 2024

TD Bank failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than $670 million through TD Bank accounts between 2019 and 2023.

Between January 2018 and February 2021, one money laundering network processed more than $470 million through the bank through large cash deposits into nominee accounts. The operators of this scheme provided employees gift cards worth more than $57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over $10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports.

In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million through shell accounts before TD Bank reported the activity.

In a third scheme, money laundering networks deposited funds in the United States and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately $39 million. The Justice Department has charged over two dozen individuals across these schemes, including two bank insiders. (Source)

Bank Manager Sentenced To Prison For Coordinating Multistate $5 Million COVID-19 Relief Program Fraud Scheme - October 21, 2024

In 2020 and early 2021, Tommy Hawkins worked as the Branch Manager of the Conshohocken, Pennsylvania, branch of a national bank that was accepting Paycheck Protection Program (PPP) loan applications.

Hawkins worked with Eric Rivera, Lisa Smith, and others to recruit individuals who owned companies with little or no operations to open bank accounts at Hawkins' branch and apply for PPP loans. Hawkins helped the recruited individuals submit PPP loan applications that contained materially false representations about the companies' number of employees and payroll expenses. The applications also included false documentation, including tax forms.

Based on these applications, Hawkins' bank approved at least 38 PPP loans and disbursed approximately $5 million.

Hawkins received incentive compensation through the bank for opening business bank accounts for the companies that received fraudulent PPP loans and also had an agreement with Rivera and Smith for them to pay Hawkins $5,000 of the loan proceeds for each PPP loan that Hawkins helped to obtain.

Lisa Smith has pleaded guilty to her role in the scheme. Charges remain pending against Rivera and Wessels, and they are presumed innocent unless and until proven guilty. (Source)

Bank Loan Officer For Credit Union Sentenced To Prison For Creating $134,000 Of Fraudulent Loan Applications - October 8, 2024

Between December 2019 and August 2021, Nadaje Hendrix and co-conspirator Glenroy Miller agreed to defraud the credit union where Hendrix worked as a loan officer and assistant branch manager, by obtaining loans in the names of other individuals, including inmates at a Massachusetts prison where Miller was incarcerated.

While in prison, Miller allegedly gave Hendrix information about fellow inmates for Hendrix to use in creating fraudulent loan applications, and then arranged to have other co-conspirators go into the credit union to pretend

to be the inmates, sign loan forms and obtain loans from the credit union through Hendrix. The scheme also involved obtaining loans in the names of individuals whose identities were stolen. In total, Hendrix and Miller stole about $134,000 from the credit union in about two months in 2021. (Source)

Bank Employee Sentenced To Prison For Role In $100,000+ Bank Fraud Conspiracy - October 22, 2024

Between February 2022 and October 2022, Allahson Allah together with codefendant Evan Cutler, managed a conspiracy targeting SEFCU in which the conspirators obtained customer personal identifying information and impersonated people to fraudulently obtain cash and credit from SEFCU.

Caeshara Cannon was a Member Service Representative at SEFCU and provided Allah and Cutler with customer account information to use in creating counterfeit checks that were presented for negotiation at SEFCU branches all over the Capital Region. The conspirators also applied for loans at SEFCU in the names of individuals whose identities they had stolen and withdrew the proceeds in cash. In total, the conspiracy netted the conspirators $88,800, with intended losses of over $100,000. (Source)

HSBC Bank May Have To Compensate 329 Customers Robbed By Scammers Posing As Bank Employees - October 15, 2024

Banking giant HSBC may have to compensate customers robbed by scammers after a consumer watchdog found a victim should not have been held responsible for their $47,000 loss.

In a landmark ruling, the Australian Financial Complaints Authority rejected HSBC's claim it was not liable when a sophisticated scammer masqueraded as a bank worker to raid the victim's account, an argument it has used to deny compensation to other victims.

Over at least 10 months in 2023 and 2024, fraudsters were able to infiltrate genuine text message chains from HSBC to make victims believe their accounts had been compromised and scare them into handing over pass codes to a fake bank worker.

The Australian Financial Complaints Authority has received 329 complaints related to the HSBC impersonation scam, of which 121 are still open.

Even when customers realised they were being scammed as they were still speaking with the scammer, HSBC was unable to retrieve their money because criminals quickly changed the victim's daily transfer limits and moved money into new accounts and cryptocurrency. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Siemens Energy Pleads Guilty To Stealing Confidential Competitor Information / Agrees To Pay $104 Million Resolution / Corporate Executive & Others Sentenced To Prison - September 30, 2024

Siemens Energy, Inc. pleaded guilty today and has agreed to pay $104 million to resolve the Justice Department's criminal investigation into violations related to the misappropriation of confidential competitor information. Additionally, Siemens has agreed to a three-year term of organizational probation. (Source)

2 Employees Working For Roadside Assistance Provider Given Suspended Sentences For Illegally Copying & Selling Personal Data On 29,000+ People Involved In Accidents - October 11, 2024

Debbie Okparaver, and Maliha Islam had worked as customer services specialists at RAC's call center.

The RAC had installed unspecified security monitoring software, which showed Okparavero accessing and copying personal information relating to people involved in road traffic accidents" A search of Okparavero's mobile phone revealed the data was then shared with Islam in a WhatsApp chat.

Some 29,500 lines of personal information were exposed. The chat messages shared between the pair suggested an unknown third party was paying for that data.

RAC employees have been involved in similar criminal activities before. In 2021, an ex-staffer pleaded guilty to charges of unsanctioned access to computer systems and selling that data to an accident claims management company, while in February last year, the ICO highlighted another former RAC worker involved in a copycat incident. (Source)

CHINESE / NORTH KOREA FOREIGN GOVERNMENT ESPIONAGE / THEFT OF TRADE SECRETS INVOLVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

10 Pharmaceutical Distributor Executives, Sales Representatives & Brokers Charged With Unlawful Sales Of Nearly 70 Million Opioid Pills Worth $1.3 BILLION - October 3, 2024

Charges against 5 pharmaceutical distributor executives and 5 pharmaceutical sales representatives and brokers have been unsealed as part of a larger enforcement action related to the unlawful distribution of nearly 70 million opioid pills and over 30 million doses of other commonly abused prescription drugs to alleged Houston, Texas pill-mill pharmacies. 3 Houston area pharmacy operators were also charged in the Southern District of Texas for their role in the schemes. Nine individuals have pleaded guilty.

The opioids allegedly distributed were oxycodone, hydrocodone and hydromorphone.

They were available in numerous strengths and forms, but the distributors allegedly sold the drugs almost exclusively in their most abused, most powerful immediate-release pill forms — i.e., the ones that sold for the most money on the black market. The distributors also allegedly sold prescription drug potentiators alprazolam, carisoprodol, and promethazine with codeine syrup, known for their reputation of enhancing the high from the opioids.

The distributors allegedly charged their Houston customers far more for the drugs than what a legitimate pharmacy could or would pay.

This is the largest ever criminal enforcement action targeting distributors of pharmaceutical opioids and commonly abused prescription drugs with estimated street value of $1.3 BILLION. (Source)

Chief Executive Officer Of Hospital Charged For Role In $19 Million Corruption And Embezzlement Scheme - October 11, 2024

A 45-count, second superseding indictment accuses former CEO George Miller, of conspiring with the hospital's then-Chief Financial Officer, Anosh Ahmed, to corruptly steer vendor contracts and other hospital business to certain medical supply companies in exchange for cash from the companies' owner, Sameer Suhail.

Ahmed, Suhail, and the hospital's former Chief Transformation Officer, Heather Bergdahl, were originally indicted earlier this year on fraud, embezzlement, and money laundering counts. The charges accused them of causing the hospital to issue payments to purported vendor companies for goods and services that they knew had not been provided. Many of the purported vendor companies were created by Suhail and Ahmed under various names to conceal their association with the fraudulent payments, the charges alleged. Bergdahl allegedly opened bank accounts in the names of two legitimate hospital vendors and caused the hospital to deposit fraudulent payments into those accounts.

The newly returned indictment alleges that from 2018 to 2021, Suhail paid Miller and Ahmed a share of $19 million in payments that he received from the hospital, in return for Miller and Ahmed steering those contracts and business to him. The payments to Miller and Ahmed were in addition to the millions of dollars in fraudulent payments charged in the prior indictment. (Source)

Operator Of Medicaid Call Center Agrees To Pay $11.3 Million To Resolve Payment Of False Claims / 2 Former Employees Plead Guilty To $8 Million+ Of Wire Fraud - October 3, 2024

Conduent State Healthcare, LLC, headquartered in New Jersey, has agreed to pay $11,358,767 to resolve False Claims Act allegations arising from Conduent's fraudulent reporting of call center performance metrics and false claims for payment to the South Carolina Department of Health and Human Services (SCDHHS).

2 former employees of Conduent, Richard Kirchner and Brian Devanney pleaded guilty for their role in fabricating performance metrics and adjusting invoices to SCDHHS.

In connection with the settlement, the United States acknowledged that Conduent took significant steps in cooperating with the government's investigation, entitling it to credit.

Between Jan. 1, 2018, and Feb. 28, 2023, Kirchner and Devanney supplied fake reports to SCDHHS with inflated numbers for call volumes and misrepresented metrics to avoid penalties under the contract. SCDHHS paid Conduent an excess of $8,113,405 as a result of the fraudulent reports and invoices submitted by Devanney and Kirchner. Those payments benefited Conduent. (Source)

Physician Assistant Sentenced To Prison For Role In $10 Million+ Telemedicine Fraud Scheme - October 4, 2024

In 2018 and 2019, Colby Joyner was a physician assistant in the Charlotte North Carolina area who worked as an independent contractor for a physician staffing and telemedicine company.

Joyner signed fraudulent prescriptions for medically unnecessary genetic testing, specifically cancer genomic and pharmacogenetic testing, for over 600 Medicare beneficiaries residing in North Carolina. Joyner had never met, seen, or treated the beneficiaries, and only had brief telephone conversations with them or no interactions at all.

Joyner received from the telemedicine company and its clients pre-populated prescription forms and related records for patients who were pre-selected for genetic testing, which he then electronically signed and returned, in exchange for $12 – and later $15 – for each purported consultation that he performed.

To conceal that Joyner was not the beneficiaries' treating physician and that he did not conduct medical evaluations or examinations of the beneficiaries, Joyner falsified medical records in connection with the unnecessary prescriptions and falsely certified that the genetic tests were medically necessary. Joyner's scheme resulted in the submission of more than $10 million in fraudulent reimbursement claims to Medicare, and more than $3.6 million in payments. (Source)

Chief Financial Officer For Pharmaceutical Wholesaler Sentenced To Prison For Falsifying Loan Documentation / Caused Lenders To Sustain Loss Of $1.3 Million - October 10, 2024

Theodore Toloff served as the Chief Financial Officer of the Frank W. Kerr Company (Kerr), a now-defunct pharmaceutical wholesaler that was based in Novi, Michigan.

Kerr had a revolving credit agreement with two large financial institutions under which the company borrowed funds up to $60 million pursuant to a calculation dependent on the company's eligible accounts receivable and inventory. Toloff admitted that he submitted false documentation to the financial institutions that included $18 million in ineligible accounts receivable and that Kerr borrowed additional funds after this false documentation was submitted. The Court found that Toloff's criminal conduct caused Kerr's lenders to sustain a loss of $1.3 million, which Toloff was also ordered to pay back to the lenders as restitution. (Source)

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

Company Accounting Specialist Pleads Guilty To $532,000+ Fraud Scheme - October 1, 2024

Between March 2021 and July 2022, Rhonda Canidate was employed as an Accounting Specialist at Henry Molded Products Company in Lebanon, Pennsylvania.

Between October 2021 and June 2022, Canidate entered false payment entries for former Henry Molded employees into Henry Molded's third-party payroll software, causing the software to issue direct deposit payments from Henry Molded's bank account to bank accounts controlled by Canidate in the name of the former employees. This fraud not only financially injured Henry Molded; it also harmed the former employees by creating an overpayment for tax purposes. Canidate caused a loss of $532,050 and has agreed to pay restitution. (Source)

Pharmaceutical Executive Pleads Guilty To $250,000+ Of Insider Trading - October 8, 2024

Dishant Gupta worked as the Director of Strategy and Operations in the Boston office of a global pharmaceutical company (Company A). In the spring of 2022, during the course of his employment at Company A, Gupta learned that Company A was negotiating to acquire certain assets of a smaller pharmaceutical company based in Boston (Company B), including its leading cancer drug, and that Company A later agreed to acquire Company B outright.

While in possession of this material non-public information, and in violation of his fiduciary duties to Company A, Gupta acquired shares of Company B in his own and his wife's brokerage accounts – in an effort to profit from the eventual public announcement of the transaction.

Gupta purchased more than 300,000 shares of Company B over approximately two and a half months. Gupta then sold all the shares he had acquired after Company A announced the acquisition of Company B, earning more than $250,000. (Source)

Office Manager For Car Dealership Pleads Guilty To Embezzling $191,000 - October 28, 2024

Between 2001 and January 2024, Jennifer LaBonte was employed by automobile dealerships located in Burlington, Vermont. From about 2012 until her termination, LaBonte served as Office Manager for the dealerships, a position that gave her oversight over all accounting matters. LaBonte had check-signing authority.

Beginning no later than 2013, LaBonte began embezzling from the dealerships. LaBonte stole cash receipts that had been paid by dealership customers, but she also issued checks to herself for non-business-related purposes. LaBonte tried to cover up her thefts by manipulating and falsifying entries about individual transactions in the dealerships' computerized accounting systems. An officer at the dealerships uncovered the fraud in January 2024, and LaBonte was immediately fired. The total loss resulting from her embezzlement is about $191,000. In court, the parties announced that LaBonte has provided the dealerships with a check that repaid them in full for the stolen funds. (Source)

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

Chief Financial Officer Pleads Guilty To Stealing $4.8 Million+ / Used Funds To Purchase Vehicles, Gambling, Etc. - October 8, 2024

John Raine was arrested related to his alleged embezzlement of funds from his former employer, the Virginia Birth-Related Neurological Injury Compensation Program (Birth-Injury Program).

Raines was the Chief Financial Officer and Deputy Director of the Birth-Injury Program.

The Birth-Injury Program is a fund administered by the Virginia Workers' Compensation Commission, paying monetary compensation to families of infants who suffer from brain or spinal cord injuries resulting from the birth process that render the infant developmentally and/or cognitively disabled. According to Court documents, Raines' role required that he oversee the finances of the Birth-Injury Program, including approximately $650 million in investments in 2023.

From at least January 2022 through at least October 2023, Raines allegedly stole over $4.8 million from the Birth-Injury Program, including by using his access to the Birth-Injury Program bank account to initiate at least 59 separate wire transactions, sending funds to bank accounts in Raines' own name. Raines also allegedly used the Birth-Injury Program debit card for personal gain. According to the criminal complaint, Raines spent embezzled Birth-Injury Program money on various personal expenses. For example:

What Did Raines Do With The Money?

- Purchased numerous vehicles, including eight luxury golf carts for over $160,000 and a 2023 Chevrolet Suburban.
- Spent over $100,000 on gambling.
- Spent over $9,000 to hire private limousines, including to chauffer himself and his guests to Virginia area vineyards.
- Made numerous purchases of cryptocurrency, including Bitcoin and Dogecoin, and transferred funds to his brokerage accounts.
- Paid over $30,000 for private jet travel to take his wife and friends to Nashville, Tennessee, for three day.

- Paid over $60,000 to pay down his student loan debt, his mortgage, and other loans.
- Spent over $19,000 to purchase eight separate 2022 1-oz American Gold Eagle Bullion coins and a 100-oz silver bar.

(Source)

Employee Sentenced To Prison For Embezzling $3 Million+ / Used Funds For Gambling - October 25, 2024

From April 2019 to December 2022, Sally Elmore abused her position of trust and used her access to the payroll and banking systems of her employer to execute a scheme to fraudulently direct electronic payments, in the form of salary, bonuses, and expense reimbursements that she knew she was not entitled to receive, from her employer's bank account to her personal bank accounts.

In order to conceal her fraud, Elmore prepared and presented falsified financial statements to her employer's board, representing that the company was still in possession of funds that she had, in fact, fraudulently directed to herself. She also concealed the missing funds from the company's insurer, causing the company to lose coverage for losses from theft. In total, Elmore stole over $3 million and gambled most of it away.
(Source)

Director Of Finance & Human Resources Accused Of Embezzling $690,000 From Charity - Used Funds For Travel, Clothing, Rent, Etc. - October 15, 2024

Joelle Fouse was the Manager / Director Of Finance and Human Resources for a charity from October 2012 through December 2023, when she was terminated.

Fouse was responsible for payroll, expense reimbursement and maintaining the charity's books and records. She stole from the charity in three ways, the indictment says. Fouse provided false information to a third-party payroll processing company that caused the company to make 71 unauthorized payments totaling $139,810 to multiple bank accounts controlled by Fouse, the indictment says. The indictment also accuses Fouse of triggering 181 unauthorized expense payments into bank accounts she controlled, totaling $407,186. Finally, Fouse allegedly used her company credit card to make184 unauthorized purchases totaling $133,210.

The charity also overpaid the employer portion of payroll taxes by about $10,694 due to the inflated payroll, the indictment says.

The indictment says Fouse took cash out of ATMs and used the charity's funds for travel, clothing, entertainment, restaurant meals, rent payments and day-to-day expenses for herself and relatives. She tried to cover up her crimes by making false entries in financial and accounting records, it says. (Source)

Bookkeeper Sentenced To Prison For Embezzling $550,000+ From Employer Over 15 Years / Used Funds For Personal Use - October 4, 2024

Rebecca Willis was employed as a bookkeeper with an architecture firm for more than twenty years. She had various financial responsibilities, including handling accounts payable, accounts receivable, and payroll.

Between 2006 and 2021, Willis entered false payroll data to unjustly enrich herself. She inflated her regular hours, overtime hours, bonuses, and mileage reimbursement to cause her employer to pay her more than she was actually owed. Willis' bi-weekly pay was generally 40% fraudulent and 60% legitimate.

Additionally, Willis used the company's business account and company credit cards to make unauthorized purchases of items that she retained for her personal use and benefit, including gift cards and gasoline. In total, Willis stole approximately $570,209.47 from her employer over fifteen years. (Source)

Credit Union Employee Admits Embezzling Approximately $390,000 / Used Funds For Gambling - October 25, 2024

From about July 2023 to June 2024, Edward Nurse embezzled from his employer, Park Side Credit Union in Missoula, Montana.

In June 2024, an employee discovered $340,000 in cash in the credit union's vault had been replaced with fake funds from a company that provides fake currency as props for movies and entertainment productions. Nurse was identified as a potential suspect because his primary role was managing and balancing money in the vault. In the previous seven months, financial records showed cash deposits totaling $117,751, with each deposit for more than $10,000, into Nurse's bank account. In addition, financial information from a local casino reflected that from March 2024 to May 2024, Nurse put more than $56,000 in cash into the business and cashed out slightly more than $8,000.

After the credit union discovered the thefts, Nurse claimed to an FBI special agent that he did not usually carry much cash and, aside from a vacation to Las Vegas, Nevada, he had not made any recent large purchases or cash deposits.

The investigation determined that during the first six months of 2024, Nurse had purchased $410,000 in fake currency from a prop money company and had the money delivered to a post office box in Nurse's name. The credit union was later informed that approximately $50,000 in fake money had been received by the Federal Reserve in July 2024. Those funds were returned and determined to be fake bills from the prop money company. (Source)

Company Employee Responsible For Accounting Sentenced To Prison For Stealing $334,000+ / Used Funds For Personal Expenses - October 11, 2024

Tamarisk Mathews was responsible for accounting duties of a restaurant and music venue in Wood County, Texas. She worked in accounts receivable, accounts payable, and had access to the financial accounts of the business. Mathews also had authority to issue invoices to customers and issue checks and other payments to creditors.

Beginning in about December 2018, Mathews devised and began executing a scheme to wrongfully obtain money, funds, and assets under the custody and control of the restaurant. Among other things, she wrote checks that she was not authorized to write for personal expenditures, made charges in the business's name from vendors such as Amazon, and used business funds to make purchases through PayPal. Mathews also opened an American Express account in the name of the business and obtained an American Express credit card.

She then used the card and account to make personal purchases and expenditures and paid American Express for those purchases and expenditures using business funds and the business bank account. The scheme resulted in a loss to the business of $334,252.00. (Source)

Employee Sentenced To Prison For Making $100,000+ Of Unauthorized Charges On Company Credit Card - October 3, 2024

Stephen Higgins was to a year and a day in prison and ordered him to repay $100,485 to his former employer and an insurance company.

While working as a sales engineer at a St. Louis County company, Higgins misused his company credit card for personal purposes on multiple occasions. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Employee Charged For Stealing $589,000+ From Employer Using Fake Invoice Scheme - September 29, 2024

Kristen Levin was employed by her company from 2015 to 2020. Levin misused her position to steal funds, totaling approximately $589,729.12, from the company by using fraudulent invoices for products never received her employer. (Source)

Amazon Employee Sentenced To Prison For Role In $480,000+ For Fabricated Invoices & Expense Reports Scheme / Used Funds For Condo Payments, Vehicles, Etc. - October 17, 2024

Between approximately the summer of 2020 through at least June of 2022, Tiffany Vo worked for Amazon in a role in which she administered virtual employee programs during the COVID-19 Pandemic.

Vo devised and participated in a scheme to fabricate invoices and expense reports to claim reimbursement for approximately $483,393.58 in purported corporate event expenditures that did not occur.

Vo spent the stolen funds on a variety of personal expenses including designer handbags and sunglasses, payments toward her condo, two vehicles, exercise equipment, and thousands of dollars of beauty products. (Source)

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

Fired Disney World Employee Arrested For Hacking Into Restaurant System And Changing Prices / Caused $150,000 In Damages - October 30, 2024

A fired Disney World employee (Michael Scheuer) is accused of hacking into an online system and altering Disney World restaurant menus by changing fonts and prices, adding profanity and manipulating the food allergy warnings, according to new federal documents.

The cyberattack caused at least $150,000 in damage and has gotten the FBI involved. Disney printed the wrong menus but realized the mistake in time. The menus were not sent to restaurants or distributed to the public.

According to the criminal complaint, authorities said Scheuer hacked into Menu Creator, which is run by a third-party Minnesota company that creates menus used only for Disney World restaurants.

Scheuer worked as a menu production manager until he was fired on June 13 for misconduct.

"Scheuer's firing was contentious and was not considered to be amicable," read the criminal complaint, which did not go into details into the situation. (Source)

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Hospital Nurse Pleads Guilty To Diverting Fentanyl From ICU Patient - October 7, 2024

On December 30, 2022, while working as a nurse at Concord Hospital in New Hampshire, Lisa Richardson removed a quantity of fentanyl from an intravenous line bag inserted in an Intensive Care Unit patient. She then replaced the fentanyl with saline. The defendant was not assigned to the patient's care as part of her duties as a nurse. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Employee Kills Co-Worker Because He Was Obsessed She Took To Many Breaks - October 21, 2024

Travis Merrill was arrested after he shot and killed his coworker Tamhara Collazo at her desk. The two both worked at an Allegiance Trucks office in Lewisville, which is roughly 30 miles north of Dallas. As she re-entered the building after lunch, he followed her to her cubicle and ambushed her, firing the gun several times. She was rushed to a hospital, but died from her injuries.

Merrill admitted to being obsessed with Collazo and was preoccupied with the breaks she took at work. Merrill said that he meticulously kept track of what days she took breaks and how lengthy they were, because he considered them to be unauthorized long breaks during work hours, as well as not paying any attention to him.

Collazo got wind of Merrill's concerning behavior and reported him to the company's human resources department. The suspect was ordered to seek counseling before he returned to work.

Merrill also told police that Collazo avoided him at work after she had reported him, which angered him. He then bought firearms, and even told police that he had brought the guns to work on several occasions. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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

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

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

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

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

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

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. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Key Findings From Report / Infographic
Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERETHE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

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

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

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

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

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

Former Company Chief Investment Officer Pleads Guilty To Role In $3 BILLION Of Securities Fraud / Company Pays $2.4 BILLION Fine - June 7, 2024

Gregorie Tournant is the former Chief Investment Officer and Co-Lead Portfolio Manager for a series of private investment funds managed by Allianz Global Investors (AGI).

Between 2014 and 2020, Tournant the Chief Investment Officer of a set of private funds at AGI known as the Structured Alpha Funds.

These funds were marketed largely to institutional investors, including pension funds for workers all across America. Tournant and his co-defendants misled these investors about the risk associated with their investments. To conceal the risk associated with how the Structured Alpha Funds were being managed, Tournant and his co-defendants provided investors with altered documents to hide the true riskiness of the funds' investments, including that investments were not sufficiently hedged against risks associated with a market crash.

In March 2020, following the onset of market declines brought on by the COVID-19 pandemic, the Structured Alpha Funds lost in excess of $7 Billion in market value, including over $3.2 billion in principal, faced margin calls and redemption requests, and ultimately were shut down.

On May 17, 2022, AGI pled guilty to securities fraud in connection with this fraudulent scheme and later was sentenced to a pay a criminal fine of approximately $2.3 billion, forfeit approximately $463 million, and pay more than $3 billion in restitution to the investor victims. (Source)

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Paying $1.6 BILLION In Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

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

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

Between approximately 2009 and 2014, Ng conspired with others to launder billions of dollars misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions it executed with Goldman Sachs, known as "Project Magnolia," "Project Maximus," and "Project Catalyze." As part of the scheme, Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite also known as "Jho Low," conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

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

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

Boeing Charged With 737 Max Fraud Conspiracy Agrees To Pay Over $2.5 BILLION In Penalties Because Of Employees Fraudulent And Deceptive Conduct - January 11, 2021

Aircraft manufacturer Boeing has agreed to pay over $2.5 billion in penalties as a result of "fraudulent and deceptive conduct by employees" in connection with the firm's B737 Max aircraft crashes.

"The misleading statements, half-truths, and omissions communicated by Boeing employees to the FAA impeded the government's ability to ensure the safety of the flying public," said U.S. Attorney Erin Nealy Cox for the Northern District of Texas.

As Boeing admitted in court documents, Boeing through two of its 737 MAX Flight Technical Pilots deceived the FAA about an important aircraft part called the Maneuvering Characteristics Augmentation System (MCAS) that impacted the flight control system of the Boeing 737 MAX. Because of their deception, a key document published by the FAA lacked information about MCAS, and in turn, airplane manuals and pilot-training materials for U.S.-based airlines lacked information about MCAS.

On Oct. 29, 2018, Lion Air Flight 610, a Boeing 737 MAX, crashed shortly after takeoff into the Java Sea near Indonesia. All 189 passengers and crew on board died.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 MAX, crashed shortly after takeoff near Ejere, Ethiopia. All 157 passengers and crew on board died. (Source)

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than $1.4 billion in loans. (Source)

Member Of Supervisory Board Of State Employees Federal Credit Union Pleads Guilty To $1 BILLION Scheme Involving High Risk Cash Transactions - January 31, 2024

A New York man pleaded guilty today to failure to maintain an anti-money laundering program in violation of the Bank Secrecy Act as part of a scheme to bring lucrative and high-risk international financial business to a small, unsophisticated credit union.

From 2014 to 2016, Gyanendra Asre of New York, was a member of the supervisory board of the New York State Employees Federal Credit Union (NYSEFCU), a financial institution that was required to have an anti-money laundering program. Through the NYSEFCU and other entities, Asre participated in a scheme that brought over $1 billion in high-risk transactions, including millions of dollars of bulk cash transactions from a foreign bank, to the NYSEFCU.

In addition, Asre was a certified anti-money laundering specialist who was experienced in international banking and trained in anti-money laundering compliance and procedures, and represented to the NYSEFCU that he and his businesses would conduct appropriate anti-money laundering oversight as required by the Bank Secrecy Act. Based on Asre's representations, the NYSEFCU, a small credit union with a volunteer board that primarily served New York state public employees, allowed Asre and his entities to conduct high-risk transactions through the NYSEFCU. Contrary to his representations, Asre willfully failed to implement and maintain an anti-money laundering program at the NYSEFCU. This failure caused the NYSEFCU to process the high-risk transactions without appropriate oversight and without ever filing a single Suspicious Activity Report, as required by law. (Source)

Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024

3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the world. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Pearce concealed the fraud scheme for many years by using these privileges to alter information about the accounts, which helped hide his creation of unauthorized license keys. Dusti Pearce handled accounting for the illegal business.

Hines operated Direct Business Services International (DBSI), a New Jersey-based business communications systems provider and a de-authorized Avaya reseller. He bought ADI software license keys from Brad and Dusti Pearce and then sold them to resellers and end users around the world for significantly below the wholesale price. Hines was by far the Pearces' largest customer and significantly influenced how the scheme operated. Hines was one of the biggest users of the ADI license system in the world.

To hide the nature and source of the money, the Pearces funneled their illegal gains through a PayPal account created under a false name to multiple bank accounts, and then transferred the money to investment and bank accounts. They also purchased large quantities of gold bullion and other valuable items. (Source)

COLLUSION – HOW MANY EMPLOYEES' OR INDIVIDUALS CAN BE INVLOVED?

193 Individuals Charged (Doctors, Nurses, Medical Professionals) For Participation In $2.75 BILLION Health Care Fraud Schemes - June 27, 2024

The Justice Department today announced the 2024 National Health Care Fraud Enforcement Action, which resulted in criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

In connection with the coordinated nationwide law enforcement action, and together with federal and state law enforcement partners, the government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication; over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

2 Executives Who Worked For a Geneva Oil Production Firm Involved In Misappropriating $1.8 BILLION - April 25, 2023

The former Petrosaudi employees are suspected of having worked with Jho Low, the alleged mastermind behind the scheme, to set up a fraudulent deal purported between the governments of Saudi Arabia and Malaysia, according to a statement from the Swiss Attorney General.

1MDB was the Malaysian sovereign wealth fund designed to finance economic development projects across the southeastern Asian nation but become a byword for scandal and corruption that triggered investigations in the US, UK, Singapore, Malaysia, Switzerland and Canada.

Low, currently a fugitive whose whereabouts are unknown, has previously denied wrongdoing. His playboy lifestyle was financed with money stolen from 1MDB, according to US prosecutors.

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 billion in financing from 1MDB, according to Swiss prosecutors. The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

The allegations cover a period at least from 2009 to 2015 and the duo have been indicted for commercial fraud, aggravated criminal mismanagement and aggravated money laundering. (Source)

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION in Health Care Fraud Scheme - June 28, 2023

The Justice Department, together with federal and state law enforcement partners, announced today a strategically coordinated, two-week nationwide law enforcement action that resulted in criminal charges against 78 defendants for their alleged participation in health care fraud and opioid abuse schemes that included over $2.5 Billion in alleged fraud. The enforcement action included charges against 11 defendants in connection with the submission of over $2 Billion in fraudulent claims resulting from telemedicine schemes.

In a case involving the alleged organizers of one of the largest health care fraud schemes ever prosecuted, an indictment in the Southern District of Florida alleges that the Chief Executive Officer (CEO), former CEO, and Vice President of Business Development of purported software and services companies conspired to generate and sell templated doctors' orders for orthotic braces and pain creams in exchange for kickbacks and bribes. The conspiracy allegedly resulted in the submission of $1.9 Billion in false and fraudulent claims to Medicare and other government insurers for orthotic braces, prescription skin creams, and other items that were medically unnecessary and ineligible for Medicare reimbursement. (Source)

10 Individuals (Hospital Managers And Others) Charged In $1.4 BILLION Hospital Pass - Through Billing Scheme - June 29, 2020

10 individuals, including hospital managers, laboratory owners, billers and recruiters, were charged for their participation in an elaborate pass-through billing scheme using rural hospitals in several states as billing shells to submit fraudulent claims for laboratory testing.

The indictment alleges that from approximately November 2015 through February 2018, the conspirators billed private insurance companies approximately $1.4 billion for laboratory testing claims as part of this fraudulent scheme, and were paid approximately $400 million. (Source)

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

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee. As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

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

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

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

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

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

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman. Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

TRADE SECRET THEFT

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)

U.S. Brokerage Firm Accuses Rival Firm Of Stealing Trade Secrets Valued At Over $1 BILLION - November 14, 2023

U.S. brokerage firm BTIG sued rival StoneX Group, accusing it of stealing trade secrets and seeking at least $200 million in damages.

StoneX recruited a team of BTIG traders and software engineers to exfiltrate BTIG software code and proprietary information and take it to StoneX, according to lawyers for BTIG.

StoneX used the software code and proprietary information to build competing products and business lines that generate tens of millions of dollars annually, they alleged in the lawsuit.

BTIG said in the lawsuit that StoneX had committed one of the greatest financial industry trade secret frauds in recent history, and that the scope of its misconduct is not presently known, and may easily exceed a billion dollars."

The complaint said StoneX hired several BTIG employees to steal confidential information that it used to develop its competing trading platform.

The complaint said that StoneX's stock price has increased 60% since it started misusing BTIG's trade secrets. (Source)

U.S. Petroleum Company Scientist Sentenced To Prison For $1 BILLION Theft Of Trade Secrets - Was Starting New Job In China - May 27, 2020

When scientist Hongjin Tan resigned from the petroleum company he had worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.

But Tan told a colleague a different story over dinner. He revealed to his colleague that he actually did have a job waiting for him in China. Tan's dinner companion reported the conversation to his supervisor. That conversation prompted Tan's employer to ask him to leave the firm immediately, and his employer made a call to the FBI tip line to report a possible crime.

Tan called his supervisor to tell them he had a thumb drive with company documents on it. The company told him to return the thumb drive. When he brought back the thumb drive, the company looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about. (Source)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners. As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

CEO Of Bank Sentenced To Prison For $47 Million Fraud Scheme That Caused Bank To Collapse - August 19, 2024

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering." The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (Source)

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

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

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

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

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (Source)

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

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

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly.

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

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

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

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

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

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy.

Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis.

From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

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

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

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

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

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

Former Controller Of Oil & Gas Company Sentenced To Prison For Role in $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)

EMPLOYEE EXTORTION

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data.

The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005.

Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021

On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank’s boardroom however the entire bank suffered smoke damage.

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day.

The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

She also admitted to using the fraudulently obtained money to fund her boyfriend’s business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million dollars. (Source)

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023
Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

Cook was fired for being intoxicated at work. She returned shortly after being escorted out of the hotel by police and set multiple fires in the hotel, displacing the occupants of more than 400 rooms. (Source)

WORKPLACE VIOLENCE

Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022
A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

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

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

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

Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022
Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

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

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU.

Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupicavaine, and lidocaine.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house.

Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

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

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

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

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

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

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

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,800+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. 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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Insider Threat Symposium & Expo

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 Insider Threat Program Managers / Insider Risk Program Managers with ***Hands On Experience***.

At the expo are many vendors that showcase their training, services and products. This link provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.

ITS&E events were not held in 2020 to 2023 because of COVID. The next ITS&E is scheduled for March 4, 2025 at the John Hopkins University Applied Physics Laboratory in Laurel, Maryland

The ITS&E provides attendees with access to a large network of security professionals for collaborating with on all aspects of IRM.

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.
https://www.nationalinsiderthreatsig.org/aboutnitsig.html

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and Insider Risk Management Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive Insider Risk Management. We will provide the training, guidance and resources to ensure that the Insider Risk Program Manager and key stakeholders are universally aligned from an enterprise / holistic perspective to detect and mitigate Insider Risks and Threats.

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training & Workshops For C-Suite, Insider Risk Program Manager / Working Group, Insider Threat Analysts & Investigators
- ✓ IRM Program Development, Management & Optimization Training & Related Courses
- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **675+** organizations. (Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Members
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org