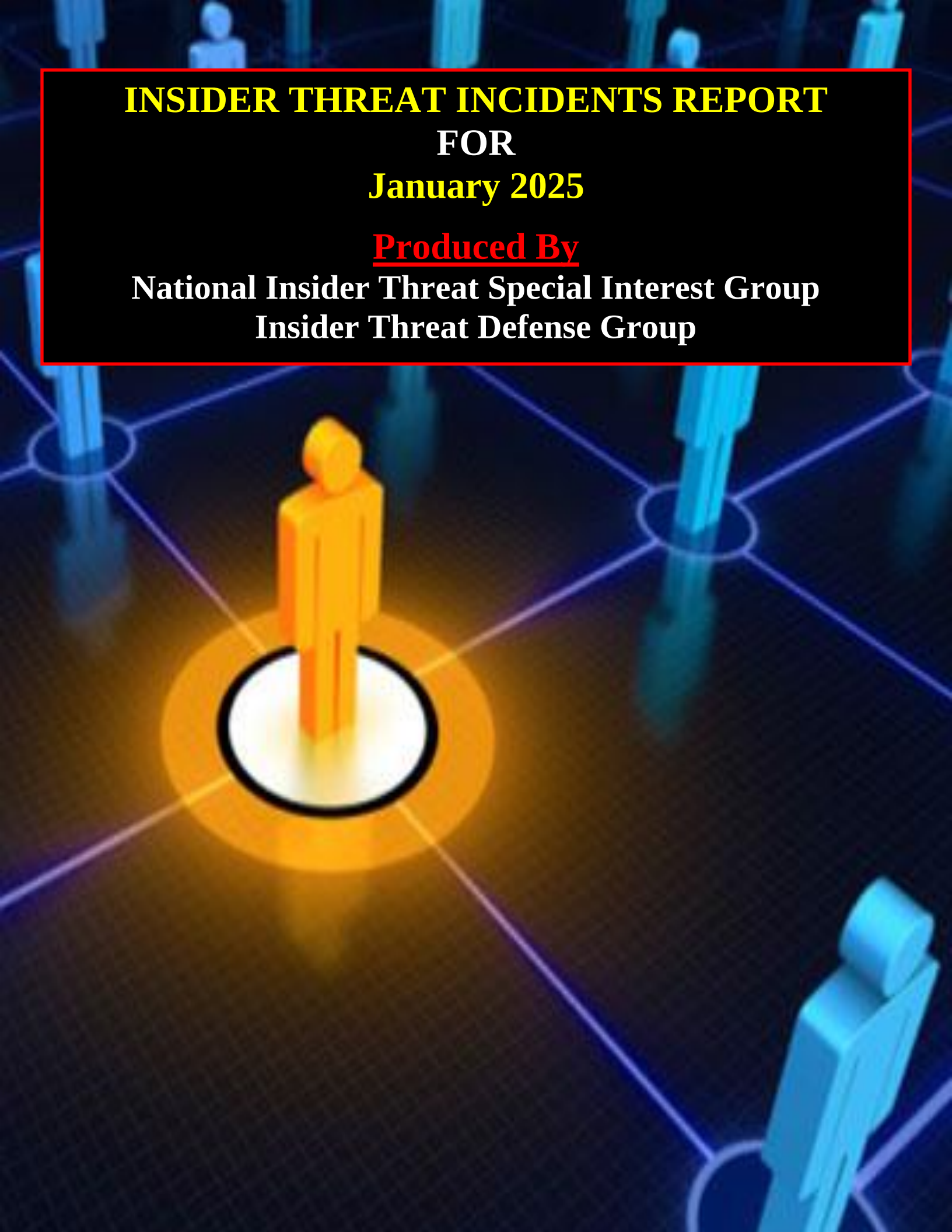

INSIDER THREAT INCIDENTS REPORT

FOR

January 2025

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 **5,900+** 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 20** 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 JANUARY 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Former Employees Accused Of Stealing Confidential Data And Providing To Rival Company - January 28, 2025

Catalyst Services Solutions Partners, a company managing canteens and employee catering services across India, has accused several former employees, including senior officials, of stealing confidential data and violating their non-disclosure agreements (NDA). The stolen information is alleged to have been used to benefit a rival company, causing significant financial losses to Catalyst Services.

According to a complaint filed by Sachin Shivajirao Desai, the company's Chief Human Resource Officer, at Chatuhshrungi Police Station, the data theft involved Chief Growth Officer Sushobhan Sarkar and other employees who resigned between April and November 2023. The accused reportedly transferred sensitive information to Axon Corporate Services India, a rival firm based in Malad, Mumbai, where Sarkar joined after resigning. (Source)

U.S. GOVERNMENT

U.S. Government Official Pleads Guility To Accepting $630,000 In Bribes To Ensure Products Were Purchased From Contractor - January 14, 2025

On Nov. 7 and 13, 2024, Brandon Glisson, a government contractor, and Lawrence Eady, a federal government official, both pleaded guilty to separate counts of bribery.

Between August 2019 and October 2020, Glisson paid approximately $630,000 in bribes to Eady from Glisson's company, Alpha Greatness Omega (AGO). In exchange for the bribe payments, Eady ensured that the U.S. government purchased IT products from one of their co-conspirators' companies at artificially inflated, non-competitive prices, and then diverted the inflated portion of the payments to AGO, which Glisson used for personal luxury purchases and to pay Eady bribes. (Source)

Former Los Alamos National Laboratory Employee Agrees To Repay $67,000+ For Unauthorized Time & Expenses Claimed For Business Trips - January 14, 2025

A former employee of Los Alamos National Laboratory has agreed to pay the United States a total of $67,500 to resolve allegations that he violated the False Claims Act by submitting false claims for payment for time allegedly worked and expenses allegedly incurred during business trips.

The settlement resolves allegations that William Wood submitted 23 false claims between July 12, 2016, and December 20, 2017, for trips to various locations in California, including Oakland, Livermore, and Santa Barbara. The United States contends that these claims were for time not actually worked and expenses not actually incurred or without a legitimate business purpose during the period from June 19, 2016, to December 9, 2017.

As part of the settlement, Wood has agreed to pay $67,500, of which $38,549.83 is restitution. In addition to the monetary settlement, Wood has agreed to never seek employment with, or work for, the federal government, its contractors or subcontractors in any capacity funded by or through the federal government, and to never seek a federal government security clearance. (Source)

U.S Postal Service Mail Carrier Sentenced To Prison For Stealing Credit Cards From Mail And Making $27,000 In Charges - January 10, 2025

Lakeatra White stole credit cards belonging to two victims, in which she tried to rack up personal charges estimated at nearly $27,000. During the investigation, White turned over 115 pieces of mail she had stolen to law enforcement. (Source)

U.S. Postal Service Mail Carrier Sentenced To Prison For Stealing Collector Coins & Items From Packages Valued At $5,000+ - January 16, 2025

William Paige worked as a mail carrier with USPS in Whitinsville, Massachusetts. Between January and February 2022, Paige stole collector's coins and other items from packages he was entrusted to deliver, collectively valued at over $5,000. Paige was also ordered to pay $5,119 in restitution to the victims. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing Gift Cards, Cash, Checks & Money Orders Totaling $8,600+ - January 27, 2025

From around September 2022 through July 2023, Michael Murray worked as a USPS postal clerk at the Beach Street Post Office in Revere and the Melrose Post Office in Massachusetts.

From around April 2023 through July 2023, Murray used his official position to steal the contents of hundreds of pieces of mail entrusted to him, including gift cards, cash and checks totaling approximately $3,422. During the same time period, Murray stole and fraudulently negotiated USPS money orders by generating them for postal customers for his own use totaling approximately $5,131. (Source)

Shipyard Contractor Must Pay $1 Million+ To Settle False Claims Involving Billing The U.S. Coast Guard For Employees Ineligible To Work In The U.S. - January 15, 2025

Bollinger Shipyard LLC (Bollinger), a Lockport, Louisiana, based company, has agreed to pay $1,025,000 to resolve allegations that it violated the False Claims Act by knowingly billing the U.S. Coast Guard for labor provided by workers who were not eligible to work in the United States.

Bollinger manufactures ships for the United States, including the Coast Guard's Fast Response Cutter (FRC).

The United States alleged that, from 2015-2020, Bollinger knowingly billed the Coast Guard for labor prohibited under the FRC contracts. Specifically, the United States alleged that Bollinger was contractually required to confirm that its employees were eligible to work in the United States. The United States further alleges that Bollinger failed to comply with this requirement and, as a result, several ineligible employees worked on the contract. Further, the United States alleged that Bollinger billed the Coast Guard for the labor provided by the ineligible employees and received payment for those bills. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Army Veteran Sentenced Prison For $779,000+ Of Disability Benefits Fraud - January 13, 2025

For nearly 14 years, Kevin McMains received over $779,000 in government disability benefits by providing false information to the Department of Veterans Affairs (VA).

McMains submitted fraudulent documentation and made false statements to medical professionals and in his applications claiming that post-traumatic stress was affecting his life to the extent he was unable to work, do normal daily activities, or care for himself, knowing that was not true. In addition, he also falsely claimed he was awarded a Purple Heart as proof of his service-connected injuries.

As a result of his fraud, McMains also qualified for and received Social Security disability benefits and Medicare coverage to which he would not have otherwise been entitled.

In addition to a 33-month prison sentence, McMains was ordered to pay restitution of $378,380.82 to the VA, $357,847.80 to the SSA, and $43,451.56 to the Centers for Medicare and Medicaid Services. (Source)

U.S. Army Soldier Posing As Cyber Criminal Charged For Selling Customer Call Records Stolen From AT&T & Verizon - December 30, 2024

Federal authorities have arrested and indicted a 20-year-old U.S. Army soldier on suspicion of being Kiberphant0m, a cybercriminal who has been selling and leaking sensitive customer call records stolen earlier this year from AT&T and Verizon. (Source)

U.S. Army Officer Sentenced To Prison For Deleting JAG School Training Materials - January 16, 2025

A former Army officer and attorney assigned to the United States Army Judge Advocate General's Legal Center and School (JAG School) in Charlottesville, Virginia, was sentenced to 54 months in federal prison on multiple federal charges related to his destruction of U.S. Army property and subsequent false statements to federal investigators.

In February 2022, Manfredo Madrigal was assigned to a staff position at the JAG School in the Training Developments Directorate, whose mission was to design and develop training products for the JAG Corps and the Army. Madrigal possessed an active security clearance and previously served overseas on sensitive operations.

In early 2022, Madrigal was under investigation by the U.S. Army and the JAG School for failing to report a previous arrest for driving under the influence (DUI). While his Army investigation was pending, Madrigal deleted, without authorization, online JAG training materials and filmed himself doing so while graphically describing his ill-will towards the Army. The FBI's investigation also revealed that Madrigal made a phone call to the Russian embassy in Washington, D.C. the same night that he deleted the training materials and then texted a witness that Russia wanted to know what he knew.

On February 22, 2022, Madrigal was discharged from the JAG School and claimed in his exit paperwork that he had no unreported contact with a foreign national. In April and May 2022, Madrigal was interviewed by the FBI about his actions. In these interviews, Madrigal made multiple false statements regarding his actions, including denying any involvement in the deletion of materials and that he only learned of the deletion from a coworker, as well as falsely denying his contact with a foreign national at the Embassy. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

FBI Employee Sentenced To Prison For $37,000+ COVID Paycheck Protection Program Fraud - January 29, 2025

Christopher Phillips formed Phillips Global Realty LLC on Dec. 20, 2019 and submitted a PPP application on May 29, 2020, using his FBI-issued credentials to confirm his identity. In his application, Phillips represented that he employed two individuals and had an average monthly payroll of $15,000.

Additionally, he submitted an IRS Form 941 (Employer's Quarterly Federal Tax Return) for the fourth quarter of 2019, claiming a payroll of $50,000 over the three-month period. IRS records indicate that Phillips did not file such a form any time between 2019 and 2022, meaning the Form 941 he submitted as part of his PPP loan application was fraudulent and the representations were false.

Phillips also certified that PPP funds would be spent only on authorized expenses, to include payroll, utilities, rent and mortgage interest. On June 2, 2020, he received $37,500 in PPP funds. Six days later, on June 8, Phillips wired $25,000 to a personal trading account and subsequently lost all of it due to trading activities. On June 9, 2020, he made a $5,117 payment toward his personal auto loan. On June 16, 2020, he paid approximately $8,500 toward his home mortgage. (Source)

Former High-Ranking FDNY Official Pleads Guilty To $190,000 Bribery Conspiracy For Inspections - January 29, 2025

From 2021 to 2023, Anthony Saccavino repeatedly abused his position as a Chief of the 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, Saccavino used his authority within the BFP to improperly "expedite" BFP inspections and plan reviews for Santiago's customers. Saccavino personally profited $57,000 as part of this scheme. To carry out this conspiracy, Saccavino lied to his BFP subordinates to justify otherwise improper expediting requests. (Source)

Justice Department To Pay Nearly $116 Million To 103 Women Who Were Sexually Abused By Federal Prison Correction Officers - December 18, 2024

The Justice Department has been ordered to pay almost $116 million to 103 women who say they were abused at the now-closed Federal Correctional Institution in Dublin, California, dubbed the "rape club."

The settlement was approved on Tuesday and will average $1.1 million for each woman who sued the prison for mistreatment and staff-on-inmate sexual abuse.

The prison's former warden, Ray Garcia, and seven other employees are now in prison themselves for sexually abusing inmates. The eighth remaining correctional officer, Darrell Wayne Smith, is awaiting trial on 12 counts of sexual abuse.

The California Coalition of Women Prisoners has filed a separate class-action lawsuit in which approximately 500 women who were housed at FCI Dublin could possibly benefit from court-ordered reform in the future.

The Bureau of Prisons shut down the facility in April and made its closure permanent last month. (Source)

Police Lieutenant And Son Sentenced To Prison For Drug Trafficking Crimes - January 15, 2025

Charles Page, age 52 and his son Treyvon Ladonte Page, age 29, were sentenced to 48 months and 120 months in prison, respectively, for their drug trafficking crimes in 2021 and 2022. At the time of Charles Page's crimes, he was a law enforcement officer with the Ayden Police Department in North Carolina.

This police lieutenant, a 13-year veteran of the force, used his official position to access confidential databases and share intelligence to advance his son's drug trafficking," said U.S. Attorney Michael F. Easley, Jr.

In July of 2021, law enforcement received information that Treyvon Page was distributing cocaine, heroin, fentanyl, and marijuana in Pitt County.

Law enforcement launched an investigation that included conducting 15 controlled purchases from Treyvon Page between November 2021 and August of 2022. The purchases consisted of varying amounts of heroin and fentanyl, cocaine, and methamphetamine.

In 2022, surveillance showed that Treyvon Page was visiting a residence in Grifton, close in time to the controlled purchases occurring. The residence belonged to his father, Charles Page, who was serving as a lieutenant with the Ayden Police Department at the time.

On September 20, 2022, law enforcement executed several search warrants across Pitt County in conjunction with the ongoing investigation. A search warrant was executed at Charles Page's house and the following items were seized: 167 grams of pure methamphetamine; 72 grams of cocaine; 15 grams of cocaine base (crack); and three shotguns. (Source)

Police Officer Sentenced To Prison For Stealing Cocaine From Crime Scenes & Police Evidence Room / Sold Cocaine And Made $130,000 - January 8, 2025

In February 2020, Joel Mefford and the other officer were investigating a drug crime and unlawfully gained access to a detached garage belonging to the subject of the investigation. Without a warrant, they entered the garage and discovered two kilograms of cocaine in the rafters. They unlawfully seized one of the kilograms and left the other to be found during the execution of a search warrant the next morning. The other officer gave the stolen narcotics to another individual to sell.

Similarly, in February and March 2020, Mefford and the other officer were investigating drug-trafficking activity at houses in Columbus, Ohio. On March 7, 2020, the officers took a bag containing multiple kilograms of cocaine from the house on Ambleside Drive and arrested an individual there. They then traveled to the house on Kilbourne Avenue and removed a kilogram of cocaine. That same day, Mefford turned in one kilogram of cocaine to evidence, and the officers stole the other kilograms to be sold.

In April 2020, Mefford and the other officer stole between 10 and 20 kilograms of cocaine from the Columbus police property room and replaced it with fake cocaine.

Mefford transported the stolen cocaine in a police cruiser and the other officer later gave the drugs to another individual to sell. The drug proceeds were then given to the other officer, who provided Mefford his cut. Mefford personally received a total of approximately $130,000 from cocaine sales.

Mefford deposited more than $72,000 of the cash derived from the cocaine sales into his personal bank account. (Source)

Police Sergeant Charged With Stealing & Selling Stolen Duty Weapons - January 27, 2025

Thomas Fry was charged with 3 counts of possession and sale of a stolen firearm.

Fry stole at least 3 9mm Sig Sauer pistols were stolen from a Dallas Police Department substation. Fry then allegedly pawned the firearms through a pawn shop in Oklahoma. If convicted of the federal charges, he faces up to 30 years in federal prison. (Source)

Corrections Officer Sentenced To Prison For Providing Firearms And Body Armor Vests To Felon - January 22, 2025

Brian Mills admitted that at various times during summer 2022, he traded a New England Firearms Company Model Pardner-SP1 .410-gauge shotgun, an Armalite rifle, ammunition, an ammunition magazine and two body armor vests to Dustin J. Manor at Manor's apartment in Plattsburgh, New York, knowing that Manor was a felon.

On October 20, 2022, the Plattsburgh Police Department seized the shotgun, one (1) .44 magnum round of ammunition, shotgun rounds, and a set of RTS Tactical Level IV ceramic body armor from Manor's Plattsburgh apartment after responding to a domestic incident there. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former State Government Employee And Her Former Boyfriend Plead Guilty To Fraudulently Obtaining $750,000+ Of COVID Jobless Benefits - January 8, 2025

A former employee of the California Employment Development Department (EDD), which administers the state's unemployment insurance (UI) program, pleaded guilty to fraudulently obtaining more than $750,000 in COVID jobless relief.

Phyllis Stitt and Kenneth Riley had been in a relationship as domestic partners with each other for over a decade at the beginning of the COVID-19 pandemic when Stitt was employed by the EDD as an employment program representative. Her job duties included determining claimant eligibility for unemployment insurance (UI) benefits and performing claim processing activities.

From March 2020 to September 2021, while using the access and information available to her in her position with the EDD, Stitt acquired the names, dates of birth, Social Security numbers, and other personal identifying information of victims that were used to submit fraudulent claims.

Stitt then filed fraudulent applications for UI benefits without the victims' knowledge or consent, and then increased the amount of UI benefits paid out by backdating the fraudulent requests to maximize the claims.

Stitt certified the fraudulent applications alleging that the victims had submitted their employment history and driver's license information, and she confirmed they were unemployed because of the pandemic and actively were searching for work.

Many of the victims were ineligible to receive these benefits because they were currently employed, not unemployed because of the pandemic, or were deceased at the time.

In filing the fraudulent applications, Stitt used mailing addresses that Riley had access to. Debit cards and accounts created as a result of these fraudulent applications were then accessed by Riley and others, who made cash withdrawals at ATMs, bank transfers and retail purchases. (Source)

New York City Housing Authority Superintendent Sentenced To Prison For Accepting $300,000+ In Bribes / 70 Other NYCHA Employees Charged - January 31, 2025

Juan Mercado is former superintendent for the New York City Housing Authority (NYCHA). He was sentenced to 48 months in prison for soliciting and accepting hundreds of thousands of dollars in bribes from contractors in exchange for awarding those contractors no-bid contracts or approving payment on previously awarded contracts at NYCHA developments.

From at least 2014 through at least July 2023, Mercado served as a superintendent at multiple NYCHA housing developments in Queens. For approximately nine years, Mercado demanded and received hundreds of thousands of dollars from multiple contractors in exchange for arranging for those contractors to receive contract work at developments where Mercadowas employed. Mercado initially demanded that contractors pay him 10% of the contract value in order to receive the work, Mercado eventually doubled the amount that contractors had to pay from 10% to 20% of the value of the contract. The contractors typically paid Mercado between $500 and $2,000 for each contract on hundreds of occasions. In total, Mercado accepted approximately $329,300 in bribes in connection with at least $1,886,000 in contract work at NYCHA developments.

Of the 70 individual NYCHA employees charged with bribery and extortion offenses in February 2024, 60 have pled guilty, and three have been convicted after trial. (Source)

Former City Official Charged For Embezzling $55,000+ And Using Funds To Pay 153 Pounds Of Bourbon Steak Ttips, Music Studio Recording & Toyota Prius - January 8, 2025

Thomas Clasby was the Director of the Quincy Department of Elder Services (Elder Services) from approximately 1999 and April 2024.

Beginning in 2019, Clasby allegedly used the City's purchasing process to pay personal expenses and generate cash for himself.

For example, Clasby allegedly arranged for the City to pay $8,950 to a music studio to produce recordings of Clasby singing songs; $2,236 to food service vendors for 153 pounds of bourbon steak tips; $4,800 for a Toyota Prius; and $1,658 for a signature, lacquered, mounted, and framed self-portrait, all of which were personal expenses.

The indictment further alleges that Clasby arranged for the City pay over $38,000 to a New York consulting company owned by Clasby's friend.

The consulting company never provided goods or services to any City department. Instead, Clasby's friend allegedly cashed the City checks and delivered the cash to Clasby at a rest stop in Framingham, Mass., a ferry terminal in Bridgeport, Conn. and at the friend's New York apartment. The indictment further alleges that, starting in June 2021, Clasby stole the vast majority of cash receipts generated by Elder Services at the Kennedy Center in Quincy. (Source)

Mayor Of Gary, Indiana Sentenced To Prison For Using $26,000+ Of Campaign Committee Funds For Financing The Purchase Of His Personal Residence - January 16, 2025

Jerome Prince, who served from 2020 to 2023 as Mayor of Gary, Indiana, illegally used approximately $26,750 of his campaign committee funds for a non-campaign purpose of financing the purchase of his personal residence. (Source)

Texas State Office Fires 7 Employees After The Unauthorized Access To 61,000+ Texas Residents Personal Identifying Information - January 21, 2025

The personal identifying information of more than 61,000 Texans may have been compromised in a data breach, and some of the state's most vulnerable residents are at highest risk.

The Texas Health and Human Services Commission (HHSC) publicly notified the public about an incident that it learned about Nov. 21, 2024. Then, the HHSC learned that, allegedly, employees from within its own office improperly accessed the information of 61,104 Texans who receive public assistance including Medicaid and food stamps.

This isn't the first break of trust from within the HHSC, however. The Texas Tribune reports that earlier in the year, an employee said she illegally possessed the information of 3,392 Texans. Plus, two other employees were found to have allegedly stolen $270,000 from around 500 food stamp accounts. The HHSC fired all seven employees accused in the various incidents. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

University IT Director Sentenced To Prison For Role In $3.9 Million IT Equipment Theft & Fraud Scheme - January 16, 2025

As Director of Information Technology for the university, Ronald Simpson was responsible for repairing and replacing defective IT equipment used at his employer's multiple locations

Beginning about Nov. 29, 2018, Simpson devised a scheme to enrich himself at the expense of the University and their equipment supplier. After receiving approval to purchase hundreds of items of IT equipment by falsely claiming the equipment would be used or installed at university locations, Simpson sold that equipment to a third-party. Simpson misappropriated at least a million dollars from the university with this part of the scheme.

He also fraudulently obtained 56 items from the university's IT supplier by falsely claiming that the equipment they originally had supplied was defective. Simpson then sold both the original equipment and the replacement gear.

The supplier sent a total of $780,233 worth of replacement IT equipment to the university based on Simpson's misrepresentations. The judge ordered Simpson to pay $3.19 million to the university and $780,233 to the IT supplier. (Source)

Former University Employee Sentenced To Prison For Staging Hoax Explosion - January 14, 2025

Jason Duhaime in September 2002 was employed as the New Technology Manager and Director of the Immersive Media Lab (Lab) at Northeastern University.

At approximately 7:00 p.m. on Sept. 13, 2022, Duhaime called the Northeastern Police Department and reported that he was injured by sharp objects expelled from a plastic case he opened inside the Lab that evening.

Specifically, Duhaime told an emergency police dispatcher that he and a Northeastern student who was working in the Lab that evening had collected several packages—including two plastic "Pelican cases"—from a mail area and brought them into the Lab. Duhaime said that when he opened one of the cases inside a storage closet, "very sharp" objects flew out of the case and under his shirt sleeves, causing injuries to his arms. Duhaime also reported that the case contained an anonymous "violent note" threatening to "destroy the lab" and stating: "In the case you got today we could have planted explosives but not this time!!! Take notice!!! You have two months to take operations down or else!!!!! WE ARE WATCHING YOU."

Duhaime's report and concern about a second, unopened Pelican case triggered a significant law enforcement response that included, among other things, the assistance of the Boston Police Department's bomb squad, the assistance of multiple federal and state law enforcement agencies, and the evacuation of a portion of the Northeastern campus.

During a search of Duhaime's office at Northeastern on Sept. 14, 2022, several laptop computers were found. A subsequent forensic examination of one of the computers revealed a word-for-word electronic copy of the anonymous threat letter that Duhaime claimed was inside the Pelican case.

According to evidence presented during the trial, this electronic copy of the threat letter was created and printed between approximately 2:50 p.m. and 3:56 p.m. on Sept. 13, 2022 – just hours before he reported the incident to the Northeastern Police Department. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Teachers Union President & Vice President For Charged For Stealing $1.2 Million+ - January 13, 2024

Teresa Brady and Ruby George were the President and Executive Vice President of Duval Teachers United (DTU), a labor union that represents Duval County Public Schools (DCPS) teachers, paraprofessionals, and office personnel. DTU has approximately 6,500 members and represents approximately 80 percent of eligible DCPS employees. DTU's annual revenue is approximately $5 million, which is comprised of funds paid by dues-paying members.

Between 2013 and 2022 Brady and George engaged in a conspiracy to steal more than $1.2 million each from the DTU by selling back leave time that they had not accrued or earned back to DTU.

Brady and George allegedly hid this activity by providing false information to DTU's auditors (Certified Public Accountants), and by signing each other's checks when distributing the unaccrued and unearned leave money, hiding those payments from the DTU Secretary/Treasurer. The indictment further alleges that Brady and George withheld this unearned compensation from the Florida Public Employee Relations Commission (PERC), responsible for public labor unions in Florida, in required annual financial statement filings, some of which were mailed to PERC.

Brady also allegedly used the fraud proceeds and engaged in two monetary transactions of more than $10,000 to pay personal credit card debt. (Source)

BANKING / FINANCIAL INSTITUTIONS

Banking Executive Pleads Guilty To Embezzling $4.2 Million From Customers Over 12 Years To Pay For Luxury Lifestyle - January 8, 2025

William Garrow was hired by the Bank of Oklahoma in August 2007 and promoted to Senior Vice President. He served as a financial advisor and provided investment and banking services to wealthy banking clients until he was terminated in March 2024.

From September 2012 through April 2024, Garrow admitted to stealing from at least 16 client accounts. Garrow fraudulently transferred funds or issued cashier checks without authorization and consent from his clients and then deposited those funds into accounts that he controlled at other financial institutions.

Garrow further admitted that his actions were wrong and that the funds were used to pay for his lifestyle. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Senior Adviser For Federal Reserve Board (FRB) Charged With Stealing FRB Trade Secrets For People's Republic Of China - January 31, 2025

John Harold Rogers, 63, is a former Senior Adviser for the Federal Reserve Board of Governors (FRB) He was arrested on charges that he conspired to steal Federal Reserve trade secrets for the benefit of the People's Republic of China (PRC).

From ay least 2018, Rogers allegedly exploited his employment with the FRB by soliciting trade-secret information regarding proprietary economic data sets, deliberations about tariffs targeting China, briefing books for designated governors, and sensitive information about Federal Open Market Committee (FOMC) deliberations and forthcoming announcements. He passed that information electronically to his personal email account, in violation of FRB policy, or printed it prior to traveling to China, in preparation for meetings with his co-conspirators. Under the guise of teaching "classes," Rogers met with his co-conspirators in hotel rooms in China where he conveyed sensitive, trade-secret information that belonged to the FRB and the FOMC.

In 2023, Rogers was paid approximately $450,000 USD as a part-time professor at a Chinese university. (Source)

Hospital Administrator Sentenced To Prison For $250,000+ Identity Theft Scheme / Used Fake Identity For 30 Years - April 1, 2024

Matthew Keirans is a former Iowa hospital administrator. He lived under a false identity for more than 30 years and caused the false imprisonment of his victim.

Evidence presented at hearings in the case established that Keirans and his identity theft victim worked together at a hotdog cart in Albuquerque, New Mexico, in the late 1980s. Keirans assumed the victim's identity and, for the next three decades, used that identity in every aspect of his life. Keirans obtained several false documents in the victim's name, including a Kentucky birth certificate.

In 2013, Keirans obtained employment as a high-level administrator in an Iowa City hospital. Keirans provided the hospital with false identification documents during the hiring process, including a fictitious I-9 form, social security number, date of birth, and other identification documents in his victim's name. After getting hired, Keirans worked for the hospital remotely from his residence in Wisconsin. Keirans' access to, and roles in, the system architecture of the hospital's computer infrastructure were the highest it could be, and Keirans was the key administrator of critical systems.

Between August 2016 and May 2022, Keirans repeatedly obtained vehicle and personal loans from two credit unions in the Northern District of Iowa using the victim's name, social security number, and date of birth. Keirans obtained nine loans with a total value of over $250,000 from the credit unions. Keirans also obtained various lines of credit from other lenders in the victim's name and with his personal identifiers.

Keirans also maintained deposits at a national bank. In 2019, the victim, who was homeless at the time, entered the branch of the national bank in Los Angeles, California, and told a branch manager that he had recently discovered that someone was using his credit and had accumulated large amounts of debt. The victim stated that he did not want to pay the debt and wished to close his accounts at the bank. The victim presented the bank with his true social security card, as well as an authentic State of California identification card.

Due to the large amount of currency in the accounts, the branch manager asked the victim a series of security questions, which the victim was unable to answer. The national bank then called the Los Angeles Police Department (LAPD).

LAPD officers spoke with Keirans on the telephone, who stated he lived in Wisconsin and did not give anyone in California permission to access his bank accounts. After faxing the LAPD a series of phony identification documents, the LAPD arrested Keirans' victim on two felony charges. The victim was charged in Keirans' name and held without bail at the Los Angeles County Jail.

In the ensuing months, Keirans contacted the LAPD and Los Angeles District Attorney (LADA) numerous times requesting updates on the victim's prosecution. Meanwhile, Keirans' victim continued to assert throughout the California criminal proceedings that he was not Keirans. A California state court judge ultimately found Keirans' victim was not mentally competent to stand trial and ordered Keirans' victim to a California mental hospital. The California state court also ordered Keirans' victim to receive psychotropic medication.

After his release from jail and hospital, Keirans' victim made numerous attempts to regain his identity. For his part, Keirans continued to make false reports and statements to law enforcement officials in Wisconsin and California.

In January 2023, after learning where Keirans was employed, the victim contacted the Iowa City hospital's security department about Keirans. The hospital referred Keirans' complaint to a local law enforcement agency, which assigned an experienced detective to investigate the victim's complaint. The detective conducted an investigation and, over the course of the ensuing months, unraveled Keirans' identity theft scheme. Among other things, the detective obtained DNA evidence that conclusively proved that Keirans was not the son of an elderly man in Kentucky, as Keirans had claimed, but that Keirans' victim was the man's son. (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

Virginia Hospital Nurse Arrested For Child Abuse & Unexplainable Injuries In Other Babies - January 3, 2025

Virginia police have arrested a registered nurse in connection with a twisted attack that left a vulnerable newborn in a hospital's neonatal intensive care unit with an "unexplainable fracture" in November and additional charges could come as detectives continue to probe a half dozen similar incidents.

The 26-year-old suspect, Erin Strotman, was booked into the Henrico County Jail on charges of malicious wounding and child abuse that caused serious injury.

A perplexing string of injuries to babies in the NICU at Henrico Doctors' Hospital in Richmond in November and December prompted officials to launch an internal investigation and close the unit to new patients on Christmas Eve. (Source)

Operations Manager For Medical Diagnostics Company Pleads Guilty To Fraudulent $70 Million Medicare Billing Kickback Scheme - January 4, 2025

From at least June 2013 through at least September 2020, Timothy Doyle conspired with others, including two managers for a mobile medical diagnostics company that performed transcranial doppler (TCD) scans, to enter into kickback agreements with various doctors. TCD scans are brain scans that measure blood flow in parts of the brain.

Doyle and his alleged co-conspirators agreed to offer and pay doctors kickbacks, some in cash and others by check, based on the number of TCD ultrasounds the doctors ordered.

Doyle and his alleged co-conspirators created purported rental and administrative service agreements, which on paper made it appear as if doctors were compensated for the TCD company's use of space and administrative resources of the ordering doctor's practice based on fair market value and not based on the volume or value of referrals. These agreements were shams that hid the true nature of the arrangement of paying per test.

The scheme resulted in fraudulent bills of approximately $70.6 million to Medicare. Medicare paid approximately $27.2 million to the TCD company for the fraudulent claims. (Source)

Amtrak Employee Admits Participating In $11 Million+ Health Care Fraud / Kickback Scheme - January 23, 2025

From January 2019 through June 2022, Rodolfo Rivera and his co-conspirators, who were also Amtrak employees, engaged in a scheme to obtain cash kickbacks from health care providers in return for their agreement to allow their health insurance plan to be billed for services that were never provided and were not medically necessary. As a result of the fraudulent claims submitted on behalf of Rivera, his dependent, and other Amtrak employees that he recruited into the scheme, the Amtrak health care plan paid over $2 million in reimbursements. In total, as a result of the conspiracy, the Amtrak health care plan paid over $11 million in fraudulent claims associated with providers connected to the scheme.

Rivera received thousands of dollars in cash kickbacks from health care providers in return for his participation in the scheme, including from Punson Figueroa, an acupuncturist, and Michael DeNicola, a podiatrist. Figueroa previously pleaded guilty to conspiracy to commit health care fraud and was sentenced on September 24, 2024 to 34 months in prison. DeNicola previously pleaded guilty on June 29, 2022 to conspiracy to commit health care fraud, among other offenses. His sentencing remains pending. (Source)

Hospital CEO Sentenced To Prison For Role In Taking Kickbacks For Illegal Payments To Physicians For Laboratory Referrals / Must Pay $5 Million Penalty - January 15, 2025

Jeffrey Madison was sentenced to prison and also agreed to pay $5,343,630 to resolve allegations under the False Claims Act involving illegal payments to physicians for laboratory referrals in violation of the Anti-Kickback Statute. (Source)

Senior Partner For Global Management Consulting Firm Pleads Guilty To Destroying Records Related To DOJ Investigation / Firm To Pay $650,000 Million Penalty - January 10, 2025

A former senior partner at McKinsey & Company, a global management consulting firm based in New York, N.Y., that last month agreed to pay $650 million to resolve criminal and civil investigations into the firm's consulting work with opioids manufacturers, including Purdue Pharma, L.P., pled guilty today to obstructing justice related to his work on Purdue matters.

Martin Elling, a U.S. citizen residing in Bangkok, Thailand, waived his right to be indicted and pled guilty to knowingly destroying records with the intent to impede, obstruct, and influence the investigation and proper administration of a matter within the jurisdiction of the United States Department of Justice. (Source)

Financial Coordinator For Dental Office Sentenced To Prison For Embezzling $243,000+ - January 16, 2025

Jennifer Thornton had been a financial coordinator in a dental office in Houston. The dentist had been in business for 38 years. In July 2021, he began a detailed review of his company accounts to prepare for retirement. At that time, he discovered Thornton had been stealing from him.

She had created a shell company called SGS Healthcare and had payments intended for the dental practice diverted there. Insurance companies made checks payable to the dental practice which she then deposited into her own accounts.

She also manipulated the company books to allow her to take cash she had received from patients. The victim hired a private auditor who identified $243,597 in losses. (Source)

Hospital CEO Sentenced To Probation For Stealing $34,000+ For Personal Use - January 16, 2025

Charles Hatfield was sentenced to five years of federal probation and ordered to pay $34,872.62 in restitution and a $20,000 fine for theft or bribery concerning programs receiving federal funds. Hatfield admitted that while Chief Executive Officer of Williamson Memorial Hospital, he stole $34,872.62 in hospital funds for personal use and without authorization.

Hatfield became the hospital's interim CEO in September 2018. As CEO, Hatfield had control over the hospital's finances and bank accounts, directed payments of the hospital's funds, and had custody and control of the hospital's checkbook. Hatfield was the permanent CEO when he was relieved of those duties in September 2019. Around that time, on Oct. 21, 2019, the rural, 76-bed hospital filed for bankruptcy.

On May 16, 2019, Hatfield directed that $9,197.62 in hospital funds be used to purchase a cashier's check made payable to an individual at Venice Sands Apartments-Argus Management of Venice in Florida. Hatfield admitted that he used the hospital funded-check to settle a personal lawsuit demanding the payment of delinquent real estate taxes and homeowners' fees he owed for personal condominium property he owned in Venice.

On September 25, 2019, Hatfield directed the transfer of $25,675 in hospital funds to Mid Mountain Properties, a real estate company owned and operated by Hatfield. The transaction occurred just days prior to Hatfield being relieved as CEO, and shortly before the hospital filed for bankruptcy.

Hatfield admitted that he was aware that the hospital could not appropriately fund its employee benefits programs, including retirement and healthcare plans at the time he directed the transfer. Hatfield further admitted to telling his business partners that he used the transferred funds to pay a personal obligation.

Hatfield also admitted that he never requested or received authorization from the hospital's board of directors or anyone else at the hospital to direct the payments from the hospital to himself. (Source)

Hospital Charged For Healthcare Fraud For Allowing Doctor To Perform Unnecessary Surgical Procedures Knowing Doctor Had Been Previously Convicted For Doing So - January 8

A federal grand jury returned an indictment charging Chesapeake Regional Medical Center (CRMC) in Virginia, with healthcare fraud and conspiracy to defraud the United States and interference with government functions.

As alleged in the indictment, CRMC, formerly known as Chesapeake Regional Hospital, granted privileges to Javaid Perwaiz from 1984 until his arrest in 2019, despite knowing that Perwaiz' privileges had been terminated at another hospital for performing unnecessary surgeries and that he was convicted of two federal felonies in 1996. From 2010 to 2019, CRMC allegedly received approximately $18.5 million in reimbursements from health care benefit programs for surgical and obstetric procedures Perwaiz performed at the facility.

Beginning at least as early as January 2010 and continuing until November 2019, CRMC, Perwaiz, and others allegedly conspired to defraud the Centers for Medicare and Medicaid Services, Medicare, Medicaid,

the Virginia Department of Medical Assistance Services, and TRICARE. CRMC and Perwaiz allegedly agreed to Perwaiz continually performing surgeries and other procedures at CRMC that were in violation of the rules and regulations of the healthcare benefit programs. CRMC also allegedly defrauded Medicare, Medicaid, TRICARE, Anthem, Optima, Humana, Cigna, Aetna, United, and others to obtain reimbursements for obstetric deliveries that were elective inductions for no medical reason before 39 weeks of gestation, contrary to medical necessity and the standard of care. CRMC allegedly submitted such reimbursements itself, and aided and abetted Perwaiz to do the same.

In November 2020, Perwaiz was convicted of 52 counts of health care fraud and false statements in health care matters and was sentenced to 59 years in prison. Approximately 38 counts of the convictions were for procedures performed at CRMC, including unnecessary hysterectomies and other invasive and irreversible surgeries, elective inductions prior to 39 weeks of gestation without medical justification, and sterilizations of Medicaid patients without consent forms signed 30 days in advance.

The indictment alleges that CRMC periodically reviewed the credentials of practicing physicians, including Perwaiz, every two years. Perwaiz's re-credentialing packet allegedly contained information regarding his felony conviction, his prior hospital suspension, and notes regarding medical malpractice lawsuits resulting from procedures he performed at CRMC.

It is alleged that CRMC continually re-credentialed Perwaiz approximately every two years between 1984 and 2019. Perwaiz was last re-credentialed in June 2019, just five months before his arrest. (Source)

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

Company Bookkeeper Sentenced To Prison For Embezzling $1.3 Million+ Over 8 Years - January 16, 2025

Susan Figuerido was a bookkeeper for a Falmouth flooring company in Massachusetts. She was sentenced to prison for embezzling more than $1.3 million from her employer.

Between June 2015 and February 2023, Figuerido embezzled more than $1.3 million from her employer by writing checks to herself drawn on her employer's bank account. To conceal her scheme, Figuerido did not record the checks that she wrote to herself in her employer's accounting system.

Figuerido did not report or include the funds that she embezzled on her federal income tax filings, resulting in a tax loss of approximately $353,000. (Source)

Company Accountant Sentenced To Prison For Stealing $3.3 Million Over Span Of 20 Years - January 15, 2025

Evidence presented to the court showed that Christina Gregory defrauded her employer, Industrial Test Systems, Inc, of approximately $3.3 million over a span of 20 years from 2004 to 2023.

Gregory utilized her position as an accountant for Industrial Test Systems to deposit checks that were payable to Industrial Test Systems into her personal bank account. (Source)

Bookkeeper Charged With Embezzling $2.5 Million From 3 Companies - January 15, 2025

David Smerling was an attorney working as a bookkeeper for 3 Massachusetts companies. He has been arrested and charged with embezzling at least $2.5 million from the companies.

Between January 2016 and May 2020, Smerling allegedly embezzled from the companies by transferring funds from the companies' bank accounts to accounts in his name.

To conceal his scheme, Smerling allegedly transferred some funds through an intermediary account owned by one of the victims before transferring funds to his accounts.

The complaint also alleges that Smerling caused bank statements to be mailed to his home address, rather than the victims' addresses, to further hide his conduct. (Source)

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

Company Office Manager Sentenced To Prison For Embezzling $1 Million+ / Used Funds To Pay Bills, Purchase House, Cars, Etc. - January 10, 2025

Between 2011 and 2022, Jennifer Horton worked as the office manager for a family-owned contracting company located in Greenfield, Indiana. In that role, Horton was responsible for managing payroll, customer invoices, and company credit cards.

Beginning around January 2016, and continuing through December 2022, Horton devised and executed multiple schemes to brazenly defraud her employer of over a million dollars. First, by inflating her salary on 466 separate occasions, for a total of $515,000, without approval.

In addition, in December 2020, Horton added her husband to the company's payroll even though he had not been hired as a salaried employee. During that time, Horton stole an additional $107,000 under the guise of her husband's name.

To conceal her conduct, Horton edited the company's payroll data to make it appear that she was being paid her agreed-upon salary and to delete the payments to her husband.

After the edited data was approved, Horton reverted the payroll system to make the unauthorized payments to herself and her husband.

Horton misled her boss about the company's financial reports, resulting in significant financial strain on the company when the true information was discovered.

Horton also redirected credit card payments made by the company's customers into her own personal bank account over 185 times. She concealed the theft by altering the company's accounting records to delete invoices or falsely mark them as being paid in full to the company.

Finally, Horton abused the company credit card to pay personal bills and make personal purchases, including a house, cars, and clothes. In total, Horton stole approximately $1,116,258 from her employer. (Source)

Hotel Manager Sentenced To Prison For $61,000+ Financial Fraud Scheme - January 27, 2025

From March to October of 2023, Angelique Patterson manipulated the hotel's reservation system to alter the records of customers who had paid using cash or credit cards. Patterson retroactively changed those reservations to falsely show that the customers had used the hotel's loyalty rewards system "points" for their stay. She then added her own credit or debit card information into the system and had the customers' payments "refunded" to her.

On Oct. 4, 2023, although not on duty, Patterson tried to use the hotel's desk computer and a coworker's credentials to fraudulently refund herself an additional $61,998.

Patterson also used hotel customers' credit card information from August through September of 2021 to make fake charges via the entertainment company she owned, Angel Entertains LLC. She obtained or tried to obtain $109,000 that way. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Assistant Chief Engineer Pleads Guilty Defrauding Company Of $8.5 Million Through False Invoicing Scheme That Benefited His Business - January 23, 2025

John Pigsley is the former Assistant Chief Engineer of Facilities for Keolis Commuter Services (Keolis).

Pigsley pleaded guilty to defrauding Keolis of over $8 million and to defrauding the IRS.

Keolis has operated the MBTA commuter rail system since 2014 under an annual contract of $291–$349 million. Between 2014 and November 2021, Pigsley was employed as Keolis' Assistant Chief Engineer of Facilities and was responsible for the maintenance of MBTA Commuter Rail Facilities and their engineering operations, including corrective repair and project management for assets and maintenance and ordering and approving his subordinates' orders of electrical supplies from outside vendors for Keolis.

Pigsley also operated a separate construction company called Pigman Group. Rafferty was the general manager of LJ Electric, Inc., an electrical supply vendor to which Keolis paid over $17 million between 2014 through 2021.

Between July 2014 and November 2021, Pigsley and Rafferty defrauded Keolis of over $4 million through a false LJ Electric invoicing scheme. Specifically, Rafferty purchased vehicles, construction equipment, construction supplies and other items for Pigsley, Pigman Group and others, and Pigsley directed Rafferty to recover the cost of these items by submitting false and fraudulent LJ Electric invoices to Keolis.

Rafferty spent more than $3 million on items for Pigsley and others – including: at least nine trucks; construction equipment including at least seven Bobcat machines; at least $1 million in home building supplies and services; and a $54,000 camper– for which Keolis paid Rafferty more than $4 million based on false LJ Electric invoices.

In addition to the false invoicing scheme, Pigsley directed Keolis to purchase copper wire which he then stole and sold to scrap metal businesses, keeping the cash proceeds for himself. To conceal the theft, Pigsley personally picked up the copper wire orders from vendors or had the orders delivered to his Beverly home.

Pigsley then personally transported the wire to scrap yards where he traded it for thousands of dollars in cash several times a month and sometimes more than once a day. Pigsley obtained more than $4.5 million in cash by stealing and scrapping the copper wire. (Source)

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

Employee Pleads Guilty To Computer Intrusion & Attacks Against Employer After Being Terminated - January 23, 2025

Michael Scheuer conducted a series of computer intrusions or attacks directed at his former employer following his termination. These intrusions included manipulating allergen information in restaurant menus to indicate that food items were safe for customers with certain allergies, when they were not. Scheuer also altered menu information related to wine regions to reflect locations of recent mass shootings.

Further, Scheuer launched denial-of-service attacks designed to lock certain company employees out of their enterprise accounts. Scheuer agreed to forfeit the computer used to commit the offenses. (Source)

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Southwest Airlines Pilot Arrested At Airport For Showing Up To Work Intoxicated Just Before Boarding Flight - January 15, 2025

David Allsop, a Southwest Airlines pilot was arrested shortly before takeoff on in Georgia after he allegedly showed up to work intoxicated, police say. He was charged with driving under the influence.

Allsop was apprehended just before Southwest Flight 3772, bound for Chicago, was about to leave Georgia. It departed shortly before 11 a.m., nearly four hours after it was scheduled to takeoff.

Southwest told Fox News Digital that it was looking into the incident and that he has been "removed from duty." (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'

No Incidents To Report

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 WERE THE 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

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)

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 (**5,900+ 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 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

NATIONAL INSIDER THREAT SPECIAL INTEREST GROUP

INSIDER THREAT SYMPOSIUM & EXPO (TM)

March 4, 2025

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland

Are you looking for expert guidance from Insider Risk Management (IRM) Program Experts for developing, managing, evaluating or optimizing a program?

The NITSIG will be holding the Insider Threat Symposium & Expo (ITS&E) on March 4, 2025, at the Johns Hopkins University Applied Physics Laboratory (JHU-APL, Laurel, Maryland), in the Kossiakoff Center. The event runs from 8AM to 5PM. This will be the 5th ITS&E held.

This year's event will feature subject matter experts with real world experience in IRM Programs and an interactive breakout panel that will discuss a variety of IRM topics.

Confirmed Speakers

- Larry Knutsen / Retired CIA Insider Threat Program Manager
- Shawn Thompson / IRM Program Legal Expert (Former DoD Senior Litigation Attorney, FBI Assistant General Council)
- Todd Masse & Bill Smith / JHU- APL IRM Program
- Kevin Burton / Vice President, IRM Lead At Synchrony Financial
- Frank Greitzer, PhD / Chief Behavioral Scientist For Cogility Software
- Zak Lewis / EchoMark Insider Threat Leak Detection Tool
- Cyber Security & Infrastructure Security Agency (CISA)
- Deidra Bass / Director, Navy Insider Threat Program
- Department Of Defense Insider Threat Management Analysis Center (DITMAC)
- And More...

More Information Can Be Found On This Link:
www.insiderthreatsymposium.org

The ITS&E brings together individuals from the U.S. Government, Department Of Defense, Intelligence Community Agencies, Defense Contractors, Critical Infrastructure, Law Enforcement, Universities and the private sector companies, for a 1 day event that features expert speakers, engaging and interactive panel discussions, vendor technologies and solutions, and networking with IRM practitioners.

The expo will provide attendees with visibility into proven technologies and services for Insider Threat Detection and IRM. Vendors that are interested in exhibiting at this event, please see the link below.
https://www.eventbrite.com/e/insider-threat-symposium-expo-3-4-25-vendor-registration-tickets-1069852169639

The link below provides a complete overview of the NITSIG, advisory board members and the very positive comments (Page 19) from our membership and other individuals that have attended NITSIG meetings, workshops and ITS&E events.
https://www.nationalinsiderthreatsig.org/pdfs/NITSIG%20Overview%20With%20Comments.pdf

ITS&E Registration (**Cost: $69 – Includes Continental Breakfast / Lunch**)
https://www.eventbrite.com/e/insider-threat-symposium-expo-3-4-25-registration-tickets-1078741698459

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, evaluate and optimize an Insider Risk Management (IRM) 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, as well as attended our Insider Threat Investigations - Analysis Training Course and other training courses.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and IRM 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 IRM.

ITDG training and consulting services will empower individuals that manage or support IRM Programs, with the comprehensive knowledge, tools and a unified and holistic approach to identify, prevent and mitigate Insider Risks / Threats.

IRM PROGRAM TRANINING & CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Development, Management & Optimization Training Course
- ✓ IRM Program Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team 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 675 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, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(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