



**INSIDER THREAT INCIDENTS REPORT
FOR
July 2025**

**Produced By
National Insider Threat Special Interest Group
Insider Threat Defense Group**

TABLE OF CONTENTS

	<u>PAGE</u>
Insider Threat Incidents Report Overview	3
Insider Threat Incidents For July 2025	4
Insider Threats Definitions / Types	34
Insider Threat Impacts, Damaging Actions / Concerning Behaviors	35
Types Of Organizations Impacted	36
Insider Threat Motivations Overview	37
What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations	38
2024 Association Of Certified Fraud Examiners Report On Fraud	39
Fraud Resources	40
Severe Impacts From Insider Threat Incidents	41
Insider Threat Incidents Involving Chinese Talent Plans	63
Sources For Insider Threat Incidents Postings	65
National Insider Threat Special Interest Group Overview	67
Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview	69

INSIDER THREAT INCIDENTS OVERVIEW

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 **6,500+** 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 is 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 32** 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 JULY 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

Amtrak Employee Sentenced To Prison For \$998,000+ Million COVID Jobless Benefits Fraud Scheme With Husband - July 17, 2025

A former Amtrak employee (Lizette Lathon) was sentenced to federal prison for conspiring with her husband to steal nearly \$1 million in COVID-19 pandemic-related unemployment insurance (UI) benefits and for also fraudulently obtaining more than \$63,000 in sickness benefits while she worked at the passenger railroad company.

Previously, in July 2024, a judge sentenced Lathon's husband, Kenneth Lathon to federal prison and ordered him to pay \$998,630 in restitution.

From 2014 until at least September 2022, Lizette Lathon, in addition to her one-time duties as a service attendant for Amtrak, operated at least three tax preparation businesses: Miracle Tax Service, Hardcore Corp., and Lathon LLC.

Lizette Lathon submitted fraudulent applications with the California Employment Development Department (EDD) for UI benefits using names, Social Security numbers, and dates of birth that she obtained from former clients of her tax preparation businesses without the permission of those former clients. On the applications, she falsely asserted inflated income for the named claimants – many of whom had never lived in California – to receive the maximum benefit amount.

As a result of the fraudulent claims she filed, EDD authorized Bank of America to issue debit cards in the names of Lizette Lathon's former clients, but the cards were mailed to addresses she and her family controlled. She and her husband then used the debit cards to make cash withdrawals at ATMs and to make purchases at retail stores.

During the conspiracy, which lasted from the spring of 2020 until March 2021, Lathon and her husband caused at least 44 fraudulent unemployment claims to be filed, resulting in losses to EDD and the United States Treasury of approximately \$998,630.

Lizette Lathon, who was employed at Amtrak from 2000 to 2021, also schemed to defraud the Railroad Retirement Board out of sickness benefit payments by filing forged and false claims that stated she was being treated by a medical professional for pain and anxiety. Through this scheme, which lasted from September 2014 to January 2020, she fraudulently obtained approximately \$63,047 in sickness benefit payments.

Amtrak is a corporation owned by the United States federal government. While it operates as a for-profit company, the government holds all of its preferred stock and appoints its board of directors. This means the government essentially owns and controls Amtrak. ([Source](#))

U.S. Postal Employee Pleads Guilty To \$19,000+ Of COVID Relief Fraud - July 31, 2025

Between March 18 and April 1, 2021, Kenneth Jackson devised a scheme to defraud the Small Business Administration (SBA) by applying for a Paycheck Protection Program (PPP) loan with false representations.

Jackson claimed that he owned a landscaping business that made \$99,675 in 2019, which was not true. Jackson also provided the SBA with a fraudulent IRS tax form as proof of this reported income. Based on his false representations, Jackson fraudulently received a \$19,333 loan from the SBA. ([Source](#))

U.S. Postal Employee Pleads Guilty To \$10,000 Of COVID Relief Fraud - July 31, 2025

Between June 28 and 30, 2020, Marina Brooks devised a scheme to defraud the Small Business Administration by electronically applying for an Economic Injury Disaster Loan (EIDL) advance and providing false representations in her application. Based on her false representations, Stewart fraudulently received a \$10,000 EIDL advance. ([Source](#))

U.S. Postal Service Employee Pleads Guilty To Intentionally Causing \$42,000+ In Damage To USPS Vehicles - July 15, 2025

On January 16, 2025 mail carrier Lolita Brickhouse, 31, had concluded her work shift and began looking for her cellphone. Brickhouse began accusing other USPS employees and supervisors of stealing her cell phone. Brickhouse proceeded to violently knock over and throw objects around the postal facility. She personally insulted her supervisors and coworkers and taunted them to call the police.

Without authorization, Brickhouse took a set of vehicle keys, walked to the parking lot, and entered a USPS vehicle. She then deliberately rammed the vehicle into another USPS vehicle with such force that the second vehicle collided with and damaged a third USPS vehicle. Brickhouse exited the USPS vehicle and used her metal water bottle to break and shatter a driver-side window. As a result of the violent crash, Brickhouse totaled the second USPS vehicle. ([Source](#))

U.S. Post Office Employee Pleads Guilty To Stealing \$19,000+ / Used Funds For Personal Expenses & Gambling - July 30, 2025

Bethany LeBlanc served as the Postmaster of the Seekonk Post Office from November 2023 to about February 2025. Prior to holding this position, she worked for the United States Postal Service in a variety of roles including carrier, window clerk and customer service manager.

As Postmaster of the Seekonk Post Office, LeBlanc had the authority to issue and approve “no fee” money orders. Money orders are generated by the USPS and serve as a safe alternative to sending cash or a check through the mail. “No fee” money orders are issued solely for the purpose of paying USPS-related expenses and, thus, no fee is charged.

LeBlanc generated a total of 25 no fee money orders to herself, totaling approximately \$19,917. To avoid detection, LeBlanc presented false invoices for USPS expenses to clerks at the Seekonk Post Office, who would then issue LeBlanc the money orders. For two money orders, she entered “Fire Dept. Box” in the memo section to give the appearance that these money orders were used to pay for Post Office related expenses. For many money orders, LeBlanc entered the names of her relatives and associates to make it appear as if the funds were coming from sources other than the USPS. LeBlanc used the stolen proceeds for personal expenses, including thousands of dollars spent at casinos. ([Source](#))

U.S. Postal Worker Pleads Guilty To Role In [Drug Trafficking Through U.S. Mail For Payments](#) - July 10, 2025

USPS received a package in June 2024 which postal inspectors suspected of containing narcotics. A federal search warrant was obtained to open the parcel and resulted in the seizure of two suspicious substances. A forensic laboratory later performed a chemical analysis which confirmed the substances to be approximately 2.2 pounds of powder cocaine, and 1 pound of heroin mixed with fentanyl

Marcus Gaines was employed by USPS as a letter carrier at the time the package in question was seized.

Investigators found that the intended delivery address for the parcel containing the narcotics was on his assigned mail delivery route. Investigators repackaged the seized parcel with a sham substance and placed it back into the mail stream. Gaines collected the parcel, and it was transported along his delivery route with other U.S. mail and packages. The defendant then drove to a parking lot along his route and met with a co-conspirator where an exchange occurred.

During the investigation, federal agents learned that the co-conspirator paid Gaines \$500 for each package he delivered which contained narcotics. Each delivery occurred at a location selected by the co-conspirator which fell within the delivery route traveled by Gaines during his shift. When Gaines identified parcels labeled with fictitious names addressed to locations along his route, he knew to deliver those packages to the co-conspirator rather than the listed address. ([Source](#))

Social Security Administration (SSA) Employee Charged With Fraudulently [Obtaining \\$30,000+ COVID-19 Related Benefits While Employed With SSA](#) - July 2, 2025

In July of 2020, Tiffanie Foster applied for unemployment benefits through the state of Michigan even though she was a resident of Missouri and fully employed by SSA.

In total, she received over \$30,000 in unemployment benefits during 2020 and 2021. In early 2021, Foster applied for a PPP loan for her business. As part of her application, she also provided an altered tax form 1040 Schedule C and an altered bank statement for her business showing an inflated balance amount. ([Source](#))

Federal Employee Charged With [Simultaneously Working As A U.S. Government Federal Employee & Federal Contractor](#) - July 2, 2025

Evester Edd allegedly engaged in a scheme to defraud the U.S. government by simultaneously working as a federal employee and federal contractor. Edd is accused of falsifying his timecards submitted to multiple federal agencies and misrepresenting the amount of work he performed for the government. This scheme involved the use of wire communications to submit false time and attendance reports resulting in double billing for tens of thousands of dollars.

Additionally, Edd is accused of making false statements. When completing documentation for a security clearance, Edd allegedly misrepresented the nature of his ties to individuals overseas. Also, during an interview with federal agents investigating the case, Edd was allegedly dishonest about electronic accounts he created, actions he took, and money he sent to foreign nationals in exchange for explicit content. According to the affidavit, Edd also allegedly abused his government access to computers and systems on more than 1,000 occasions to access, save, and transmit Privacy Act information and agency sensitive information. He sent protected government information via commercial email accounts to commercial email servers and his mobile devices. ([Source](#))

U.S. Department of Energy Official Agrees To Pay \$59,000 To [Resolve Conflict Of Interest Allegations](#) - July 17, 2025

Andrew L. Horn, a former Senior Advisor to the Secretary of Energy at the Department of Energy (DOE), has agreed to pay \$59,000 to resolve allegations that he violated conflict-of-interest rules prior to his departure from the agency in 2021.

Among other things, the Ethics Reform Act of 1989 prohibits executive branch employees from participating personally and substantially in particular matters that will affect their own financial interests or the financial interests of certain parties with whom they have ties outside the government, including any organization with whom they are negotiating prospective employment.

The United States alleges that in January 2021, Horn worked personally and substantially on a particular matter affecting the financial interests of a private company with which he was simultaneously negotiating contract terms to serve as a paid senior advisor following his upcoming separation from federal service.

As part of the settlement, Horn has agreed to pay a civil penalty to resolve allegations that his conduct violated conflict-of-interest prohibitions for federal employees. ([Source](#))

Former Security Guard Working At U.S Embassy In Norway [Charged With Espionage](#) - July 23, 2025

A former security guard who used to work at the US embassy in Oslo has been charged with spying for Russia and Iran. Oslo prosecutors accuse the man, a Norwegian national, of serious espionage activities related to the US and Norway.

The security guard is said to have passed on a blueprint of the embassy, addresses and other information to Iranian and Russian contacts. ([Source](#))

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Department Of Veterans Affairs Employee Sentenced To Prison For [\\$565,000+ Fraudulent Invoices And Shell Company Scheme](#) - July 15, 2025

From approximately 2013 through October 2017, Ahmed Hassan schemed to defraud the VA by drafting and submitting for payment, false invoices of a shell company called HT Mechanical. But unbeknownst to Medical Center management, and in violation of Hassan's duties to the VA, HT Mechanical was a fraudulent entity that Hassan had secretly set up with his then-paramour (Secret Lover), Lynn Hanrahan, who was social worker with no knowledge of, or expertise in, HVAC or mechanical systems. This was done in order to defraud the VA.

For years, the Hassan made up fake work, drafted false invoices on HT Mechanical letterhead, submitted them for payment to the VA under the VA purchase card program, and lied to the VA, claiming that the work had been done, when the so-called jobs did not exist, and no work was performed. After the VA made payment to HT Mechanical based on the Hassan's lies, his paramour returned the payments to the Hassan, either by check or by giving the defendant envelopes of cash.

Hassan was ordered to pay \$565,058.70 in restitution, with \$150,000 of that restitution due in 30 days, and a \$2,200 special assessment. ([Source](#))

U.S. Air Force Employee Pleads Guilty To [Disclosing Classified Information On Dating Platform](#) - July 10, 2025

A civilian employee (David Slater) of the U.S. Air Force assigned to the U.S. Strategic Command (USSTRATCOM) at Offutt Air Force Base pleaded guilty today to conspiring to transmit classified information relating to the national defense (National Defense Information) on a foreign online dating platform beginning in or around February 2022 until in or around April 2022.

Slater after retiring as a Lieutenant Colonel from the U.S. Army, worked in a classified space at USSTRATCOM and held a Top Secret security clearance from in or around August 2021 until in or around April 2022. ([Source](#))

Texas National Guard (NG) Soldier [Convicted Of Alien Smuggling & Discharged From NG](#) - July 21, 2025

Mario Sandoval was deployed to the U.S.-Mexico border with the Texas National Guard as part of Operation Lonestar. Following release from his orders, Sandoval remained in the Rio Grande Valley began smuggling aliens in July 2024.

The jury saw Sandoval's text messages discussing that drivers were needed for trips from the Rio Grande Valley to destinations north of the immigration checkpoint. Surveillance would later show him at the immigration checkpoint at the same time he was sending text messages about the presence of law enforcement and K-9 patrols.

Sandoval was discharged from the Texas National Guard in October 2024. ([Source](#))

CRITICAL INFRASTRUCTURE

Airport Services Worker International Airport Pleads Guilty To [Smuggling Cocaine For \\$54,000+ Payment](#) - July 31, 2025

Joes Rojas, 43, was employed by an airport services company at Washington Dulles International Airport (IAD). Castillo Rojas held a Special Access Seal that provided him unescorted access to customs security areas within the airport, including access to international flights and secure baggage areas.

On April 24, Castillo Rojas arrived at IAD on COPA Airlines Flight 404 from Tocumen International Airport in Panamá City, Panamá, with one cargo bag and one backpack. During an authorized inspection of Castillo Rojas' cargo bag, Customs and Border Patrol officers discovered multiple packages of cocaine, totaling 1.95 kilograms and more than \$54,000 in counterfeit U.S. currency. An inspection of his cellphone revealed a text message conversation in which Castillo Rojas discussed retrieving the cargo bag from an individual in Peru and payment for delivering the bag to an individual in the United States. ([Source](#))

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 U.S. Customs Border & Protection Officers Plead Guilty To [Accepting Bribes To Allow Drugs To Enter The U.S. Through Their Inspection Lanes](#) - July 28, 2025

Customs and Border Protection Officers Jesse Clark Garcia and Diego Bonillo have pleaded guilty to conspiring with members of a Mexican-based poly drug trafficking organization (DTO) to allow drug laden vehicles to enter the United States free from inspection. As part of the scheme, Garcia, working at the Tecate, California Port of Entry, and Bonillo, working at the Otay Mesa, California Port of Entry, would let members of the DTO know what time and lane they were assigned by utilizing a secret emoji-based code.

The DTO would then send the drug-laden cars through Garcia and Bonillo's lanes knowing that Garcia, nor Bonillo, would inspect these vehicles.

Bonillo admitted that as part of the conspiracy he allowed at least 75 kilograms of fentanyl, 4.5 kilogram of methamphetamine, and over 1 kilogram of heroin, into the United States. The United States has alleged that both defendants profited handsomely, funding both domestic and international trips as well as purchases of luxury items and attempts to purchase real estate in Mexico. ([Source](#))

Park Police Officer Found Guilty For Role In [Committing Extortion, Impersonating An ATF Agent And The Unauthorized Seizure Of Marijuana - July 11, 2025](#)

Joseph Huffaker, 40, was employed between 2012 and 2019 with the City of Rohnert Park Department of Public Safety (RPDPS) in California as a police officer.

Huffaker conspired with his co-defendant, fellow police officer Brendan Tatum, to pull over drivers they suspected of possessing significant amounts of marijuana and extorting the drivers' marijuana by falsely claiming to be ATF agents and threatening arrest if the drivers contested the property seizures.

The jury also found that Huffaker conspired with Tatum to obstruct justice by creating a false police report two months after their extortions and sending that report to the FBI.

The RPDPS previously operated an interdiction team between 2014 and early 2017 that conducted traffic stops on vehicles along Highway 101 between Cloverdale and Rohnert Park in an effort to seize illegal drugs.

In December 2017, 11 months after the interdiction team had been disbanded, Huffaker and Tatum extorted significant quantities of marijuana from individuals, declaring to the individuals that their property would be seized, and at times threatening to arrest and charge the individuals. These seizures occurred while the officers were not on duty and not wearing their uniforms or body-worn cameras. ([Source](#))

Former FBI Procurement Official Pleads Guilty To [Bid-Rigging Scheme Involving Sister To Obtain \\$350,000 In Electronics Contracts - July 2, 2025](#)

A former electronics technician at the FBI's Los Angeles Field Office and his sister were charged with conspiring to defraud the United States to obtain at least \$350,000 in low-bid electronics equipment contracts from the FBI.

Jeffrey Spencer, 51, and Christy Evereklian, 43, were charged and both agreed to plead guilty to the felony offense, which carries a statutory maximum sentence of five years in federal prison.

From August 2015 through August 2020, Spencer and Evereklian conspired to defraud the United States by impeding the solicitation of competitive bids for electronic equipment by deceitful and dishonest means. Spencer, who was an FBI procurement official and solicited bids for electronic equipment, conspired with Evereklian to submit purportedly independent and competitive bids from Evereklian's several companies for FBI contracts.

In fact, Spencer and Evereklian already had decided which company would submit the lowest – and presumably winning – bid for a contract. Evereklian submitted bids from her own companies to the FBI using the names of her relatives to conceal her control over bidding companies, and she used a random number generator to create the fraudulent bids. ([Source](#))

Federal Correctional Officer Sentenced To Prison For Accepting \$43,000+ In Bribes To Smuggle Contraband Into Prison For Inmates - July 30, 2025

Samuel Smith was a correctional officer with the Federal Bureau of Prisons (BOP) and worked at the Coleman Federal Correctional Complex (FCC Coleman) in Sumter County, Florida. As an employee of a government agency, Smith was a “public official” under federal law.

Between December 18, 2023, and September 4, 2024, Smith received \$43,901 in bribes to smuggle contraband into FCC Coleman for inmates. On September 4, 2024, when Smith reported to work at FCC Coleman, staff members searched him and found 668 grams of marijuana and other controlled substances hidden within his duty vest. Smith was smuggling this contraband into the facility with the intent to distribute it to federal prisoners in exchange for monetary payments. ([Source](#))

County Sheriff’s Office Employee Arrested For Stealing \$230,000 For Personal Use - July 1, 2025

A former employee with the Fannin County Sheriff’s Office in Texas has been arrested after being indicted on a theft charge. The employee, Krystal Wilson, 31, was indicted for theft between \$150,000 and \$300,000.

The district attorney’s office said that the charges came from a Texas Ranger investigation that was initiated by the Fannin County Sheriff’s Office in May after it found that cash that had been deposited into kiosks for inmate commissary accounts was missing. Investigators said that \$230,000 in cash deposits had gone missing between 2021 and 2025 while they were under the sole control of Wilson, who was a records clerk.

Wilson allegedly admitted to embezzling money for personal use during an interview with law enforcement. She was fired from her job with the sheriff’s office, and on Monday she was arrested and booked into the Collin County Jail. ([Source](#))

Los Angeles County Sheriff’s Deputy Pleads Guilty To Heroin Possession And Attempting To Smuggle Drugs Into Jail For inmates / Was Paid \$15,000 - July 10, 2025

A Los Angeles County Sheriff’s Department (LASD) deputy pleaded guilty today to possessing more than one pound of heroin that he admitted to attempting to smuggle inside a county jail in the Santa Clarita Valley last year.

In April 2024, Michael Meiser was working as an LASD deputy at the North County Correctional Facility in Castaic. He had agreed with inmates to smuggle narcotics into the jail in exchange for cash and payments via the Cash App digital wallet that inmates would arrange for Meiser and one of his relatives to receive.

LASD investigators arrested Meiser and searched the other deputy’s truck, where they found the green backpack containing \$15,000 in cash, Meiser’s loaded handgun, and his badge and LASD identification. ([Source](#))

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

City Civil Engineer Charged With \$30,000 Bribery, Theft By Deception And Forgery Scheme - July 10, 2025

A former civil engineer for the City of South Fulton in Georgia has been arrested and charged with multiple crimes as part of an ongoing corruption investigation, police announced. Police have not ruled out additional arrests in connection with the scheme.

Hal Moon, who previously worked in the city’s Planning and Zoning Department, faces charges of bribery, theft by deception, and forgery.

Authorities say Moon used his position to steer developers away from the official city process and toward personal contacts, bypassing city protocols and misappropriating public funds.

The City of South Fulton Police Department's Corruption Unit launched the investigation after receiving a tip. Officials say approximately \$30,000, much of it intended for the city's tree fund, was misdirected during Moon's tenure. ([Source](#))

City IT Director Arrested For [Stealing \\$17,000 Worth Of Electronic Devices And Selling For His Profit](#) - July 10, 2025

SELMA, Ala. (WSFA) - A Selma city employee has been terminated from his position and arrested for allegedly pawning off items that belonged to the city, according to the Dallas County Sheriff's Office.

Investigators opened a probe after LEADS Online, a program that checks pawns and sales across Alabama, noticed suspicious activity where someone had pawned about 40 "pricey" items since 2023.

Investigators found the seller in question was John Louis Kinnerson, who worked as the IT Director for the City of Selma at the time. When they checked the serial numbers of the items Kinnerson had pawned, it was discovered that 36 of those items belonged to the city.

The total estimated value of the pawned items was over \$17,000, but Kinnerson only received about \$4,000 from pawning them, according to Sheriff Mike Granthum.

Kinnerson has since been removed from his position as IT Director, arrested, and charged with first degree theft of property and using public office for personal gain. ([Source](#))

County Employee Arrested For [Stealing \\$4,000](#) From County Using Purchase Card On Cell Phone - July 16, 2025

Investigators report receiving information that 31-year-old Eli Herbert Patterson was given a county-issued Government Purchase Card in August 2024 to make purchases in relation to an upcoming drill. He was employed as a part-time radio programmer / maintenance technician with Oconee Co. Emergency Services, officials said.

The investigation revealed that Patterson had downloaded the P-Card's information to his Apple Pay app on his phone. County officials in October 2024 discovered suspicious charges that had been made to the P-Card totaling around \$4,014.02, officials said.

Patterson's employment with emergency services ended on April 3, according to officials. ([Source](#))

County Clerk Of Courts Employee Charged With [Stealing \\$3,800+](#) - July 10, 2025

Victoria Elsenpeter is accused of embezzling \$3,801.60 from the Santa Rosa County Clerk of Courts & Comptroller's Office. The arrest report states the crime took place between June 13-16.

A Santa Rosa County Clerk of Courts employee reported to police on June 20 that three money bags were missing. One contained \$2,542.31, another held \$1,150 and another had \$109.29.

Upon review and some internal investigation, it was determined that those money bags were likely or potentially misplaced by someone who had direct access," Milton Police Chief Jennifer Frank said.

"Direct access to the safe and to what we call 'behind the doors within' that led to an internal investigation of employees." Elsenpeter is no longer employed by the county. ([Source](#))

Department Of Motor Vehicles Employee Charged In Stolen Vehicle Title Laundering & Bribing Scheme - July 10, 2025

The Harris County District Attorney's Office has filed five felony charges against a local Texas Department of Motor Vehicles (DMV) employee and another person in connection with a car title laundering scheme.

DMV employee Carlisha Haywood was charged with bribery and two counts of tampering with a government record. Her co-conspirator, Xavier Goodwin Washington, was also charged with two counts of tampering with a government record.

According to the DA's office, an auto theft operation was uncovered, in which people would steal vehicles and then sell the stolen vehicles to a good-faith purchaser. Before making the sale, the thieves would swap the Vehicle Identification Number (VIN) of the stolen vehicle with a "clean" VIN from a different vehicle of the same make and model.

Investigators said Goodwin Washington would then bribe Haywood and exploit her ability to access and print official records as a DMV employee to obtain certified copies of car titles in order to commit the fraudulent sale. ([Source](#))

SCHOOL SYSTEMS / UNIVERSITIES

Texas Mayor Sentenced To Prison For Role In Cocaine Drug Distribution That Involved The Use Of School Building - July 24, 2025

The former Mayor of Progreso Texas has been sentenced to prison for his role in a conspiracy to possess with intent to distribute cocaine.

The investigation determined that from 2020 to 2022, conspirators would smuggle kilograms of cocaine into the United States from Mexico. The drug trafficking organization would then re-package and conceal the cocaine in hidden compartments built into 18-wheelers. Other involved in the conspiracy would transport it to other states, specifically Illinois, Tennessee and North Carolina.

At the hearing, the court heard additional evidence that described the use of a school building to store and re-package cocaine. ([Source](#))

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Employee Who Sold Login Credentials To Hackers Leads To \$140 Million Theft From Brazilian Banks -

July 4, 2025

On Wednesday, a significant cybersecurity breach occurred when hackers infiltrated the software system of C&M Software, a service provider that connects Brazil's Central Bank to local banks and other financial institutions. The attack resulted in the theft of 800 million Brazilian reais, equivalent to approximately \$140 million, from six institutions connected to the central bank.

The breach was facilitated by an employee of C&M who allegedly sold his login credentials to the threat actors for roughly \$2,700. This unauthorized access allowed the hackers to infiltrate the software system and steal funds held in reserve accounts.

The stolen funds were then converted into cryptocurrencies, with an estimated \$30 million to \$40 million being laundered through Latin American exchanges and over-the-counter (OTC) trading platforms. ([Source](#))

Former Banker Arrested For Role In Obtaining \$2.7 Million In COVID Business Relief Funds Scheme / Used Funds For Gambling, Luxury Cars, Jewelry, Etc. - July 10, 2025

A former Wells Fargo & Co. banker (Norayr Madadi) and his brother (Vazrik Madadi) have been arrested on an eight-count federal grand jury indictment alleging they schemed to fraudulently obtain more than \$2.7 million in taxpayer-funded COVID-19 relief funds and federally-guaranteed small business loans, including by submitting applications using the stolen identities.

Norayr Madadi was a banker at Wells Fargo and opened fraudulent accounts in the names of shell companies and persons including using stolen and fictitious identities.

From March 2020 through April 2021, the defendants obtained millions in Paycheck Protection Program and Economic Injury Disaster Loan Program loans by submitting loan applications with false statements about revenues, operations, and employees.

The defendants used fake and stolen identities to further the fraudulent scheme, including the stolen identities of two victims who are developmentally disabled and live in long-term care facilities.

The Small Business Administration (SBA) and PPP participating lenders disbursed the loans into bank accounts controlled by the defendants, including the Wells Fargo bank accounts opened by Norayr Madadi. The Madadi brothers allegedly spent the loan proceeds at casinos, paying for luxury cars and jewelry, and cash withdrawals. ([Source](#))

Employee Of Bank Contractor Sentenced To Prison For Role In \$8 Million Debit Card Fraud Scheme -

July 22, 2025

Jaysha Victorian worked for a bank contractor from late 2020 to early 2021 and used her access to load prepaid debit cards with fraudulent funds, including unemployment benefits for California. She credited at least 187 cards with nearly \$8.6 million. Recipients withdrew or spent over \$7.6 million before the bank could freeze the cards.

She admitted to using some funds herself, including a \$1,000 ATM withdrawal in Houston, and received about \$300,000 in cash proceeds from her role in the scheme. ([Source](#))

Former Loan Officer Pleads Guilty To Defrauding His Employer Out Of Almost [\\$1 Million](#) - July 8, 2025

Brian Socha hacked into co-workers' computers on over 20 occasions to covertly raise the credit limit and lower the interest rate on the home equity line of credit (HELOC) on the home he owned with his wife. Over a period of six years, Socha allegedly increased the HELOC credit limit from \$135,500 to \$995,000 and adjusted the HELOC interest rate from 7.25% to 1.99%. ([Source](#))

Bank Employee Charged For Role With [Illegally Accessing Customer Accounts And Stealing \\$477,000+](#) - July 7, 2025

In August 2024, a Rochester New York area bank reported to the FBI that, over a couple of weeks in July and August, someone accessed the online accounts of approximately 12 customers and transferred funds out of those accounts.

Following an internal review, the bank determined that Damani Brown, a bank employee, used his employee credentials to look up each of the victim accounts around the time that the accounts were unlawfully accessed.

Brown was able to see whether the victim customers had ever registered their online accounts, their bank member number and social security number. Shortly after Brown performed a lookup, a co-conspirator registered the victim customer's online account.

In total, Brown and/or his co-conspirator transferred approximately \$477,000 from the 12 accounts without the knowledge or consent of the customers.

The money was transferred to other, third-party accounts at the bank, and ultimately, approximately \$327,000 was withdrawn as cash from various local branches or funds were transferred through CashApp.

Within a few days of these fraudulent transfers, a number of the victims contacted the bank to report the unauthorized activity on their accounts.

In January 2025, the FBI obtained a warrant to search Google Accounts associated with the thefts.

Investigators recovered verification emails sent from the bank containing one-time password codes and notification emails sent from the bank with updates regarding the online accounts, including email updates, password resets, and account freezes. ([Source](#))

Credit Union Branch Manager Sentenced To Prison For [Embezzling \\$330,000+](#) / [Used Funds For Personal Gain](#) - July 1, 2025

An auditor with Doches Credit Union In Texas, requested a sample of loans from the Hemphill branch for review. The review showed missing paperwork and unusual transactions on loans that were approved by Haley Maxine Snodgrass. Snodgrass had been employed by the Doches Credit Union since 2016, first as a teller and then as a branch manager.

An investigation conducted by a third party revealed that Snodgrass used a variety of schemes to take money from the credit union for personal gain. This included creating fraudulent loans, refinancing legitimate loans without the consent of the credit union member, misappropriating loan payments, and conducting unauthorized transactions on member accounts. Snodgrass admitted that she embezzled and willfully misapplied approximately \$281,097.97 in money, funds, and assets belonging to Doches Credit Union with the intent to defraud the credit union. She also admitted that the amount of restitution owed was \$330,351.39. ([Source](#))

Former Bank Employee Pleads Guilty To [Stealing \\$255,000+ From Vault - July 22, 2025](#)

Jennifer Lamanna worked for an FDIC-insured financial institution. As a result of reduced in-branch staffing due to the COVID-19 pandemic, Lamanna had sole access to and exercised control over a branch bank vault located in Venice, Florida. In 2020, Lamanna began using a contingency cash bag to steal cash from the vault, then physically removed the cash from the branch until the contingency cash bag program was discontinued. After the cash bag program ended, Lamanna continued to embezzle cash from the vault and deposited \$255,362 in stolen funds into a bank account she controlled.

To balance out the vault and conceal her embezzlement, Lamanna made multiple large withdrawals and subsequent matching deposits out of a customer's account. To make the sham transactions appear legitimate, Lamanna filed fictitious Currency Transaction Reports. On June 8, 2023, Lamanna made a materially false statement to the Financial Crimes Enforcement Network, a sub-agency of the U.S. Treasury Department, when she completed and submitted a Currency Transaction Report falsely stating that a bank customer deposited \$160,100 in cash into his account knowing that no such deposit took place. ([Source](#))

Truist Bank Employee Pleads Guilty To [Stealing \\$195,000 From 70 Customer Accounts - July 22, 2025](#)

In 2023, Ahshah Martin began improperly using her access to Truist computer systems to gather Truist account holders' banking information. Then, she initiated fraudulent debits and withdrawals from these accounts for her own benefit. For instance, Martin repeatedly initiated payments from customer bank accounts to a child support payment processor, through which Martin paid herself. In all, Martin used her access to sensitive customer financial information to steal \$195,000 from at least 70 separate Truist customer accounts.

Martin stole from the Truist accounts of individuals and entities, including multiple churches, a children's museum, an eye tissue bank non-profit organization, manufacturing and construction companies, a small business making customized holsters, and the North Carolina Wing of the Civil Air Patrol. Martin spent stolen funds on cosmetic products, clothing, travel expenses, dining, and at a hookah bar.

On April 15, 2024, Martin was terminated by Truist. Despite repeated attempts to retrieve her Truist laptop, Martin retained access to her work computer. To conceal her wrongdoing and prevent the return of her Truist laptop, Martin faked her own death. On April 17, 2024, in response to an email from Truist asking for the computer, Martin responded, "Sorry to inform you, she has passed away." ([Source](#))

Bank Officer Sentenced To Prison For [Embezzling \\$170,000+ / Used Funds For Gambling, Debts, Etc. - July 22, 2025](#)

Edward Jenkinson has been sentenced to prison for theft, embezzlement, or misapplication of funds by a bank officer. As part of his sentence, the court also entered an order of forfeiture in the amount of \$122,000, the proceeds of the charged criminal conduct.

Jenkinson was employed as a bank officer at a Federal Deposit Insurance Corporation insured institution. As a bank officer, Jenkinson was responsible for managing a financial center located in Tampa, Florida. One of Jenkinson's duties was to oversee the Automated Teller Machine (ATM) and teller cash drawers at the financial center.

Between March and November 2024, Jenkinson embezzled FDIC-insured funds. As part of his embezzlement scheme, Jenkinson redeemed certificates of deposit without customers' knowledge or consent. He then prepared deposit tickets and deposited the redeemed funds in customer checking accounts. Subsequently, Jenkinson embezzled the funds from the victim customers' accounts and drafted cashiers' checks payable to himself, which he deposited into his own bank accounts.

Jenkinson depleted most of the embezzled funds through cash withdrawals. Jenkinson also embezzled \$52,000 from the ATM at the financial center he managed and spent the funds on gambling, paying off debts, and retail purchases. ([Source](#))

Credit Union Employee Charged With [Stealing \\$75,000 - July 14, 2025](#)

A credit union employee in Orgeon faces charges after being accused of stealing nearly \$75,000 from six members over the past six months.

The alleged thefts came to light when Gateway Credit Union staff contacted Springfield police on July 4. Authorities were provided with documents and surveillance footage that reportedly showed employee Laila Payne making unauthorized withdrawals and transfers between member accounts, resulting in cash withdrawals totaling \$74,700. ([Source](#))

TD Bank Teller Arrested For [Stealing Debit Card Information From Customers And Making \\$995 Of Purchases From Costco - July 3, 2025](#)

Katelyn Lang was arrested for stealing credit card information and then using it the next day to shop at the Costco for purchases totaling about \$995.

A follow-up investigation found that there were four additional victims stemming from the initial investigation, all of which Lang had linked their debit card and bank account information to a digital wallet in her role as a bank teller at TD Bank, police said. Lang then used that digital wallet to make various purchases from businesses in Stafford and nearby towns. ([Source](#))

Bank President & Contractor (Brother In Law) Plead Guilty [To Loan Fraud Scheme For 9 Years - July 3, 2025](#)

A former bank president (Francis Eversman) and contractor (Gregg Crawford) admitted to committing bank fraud by conspiring together to falsify loan applications and obtain funds. The fraud scheme was from 2011 to 2020.

Eversman was a senior loan officer at former Tempo Bank in Trenton. Crawford was the owner of construction companies in southern Illinois.

Eversman and Crawford admitted that Crawford recruited straw purchasers to act as nominal loan applicants on what were often highly overvalued properties.

His brother-in-law, Eversman, steered these loans through the approval process. Crawford then used the loan proceeds for other purposes.

In some cases, Crawford provided fake lease agreements to purport to show rental income from subject properties. When at audit by the Office of the Comptroller of the Currency discovered the suspect loans, Crawford instructed a straw purchaser to provide investigators with false information. ([Source](#))

PHARMACEUTICAL COMPANIES / PHARMACIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES

National Health Care \$14.6 BILLION+ Fraud Takedown Results In 324 Defendants Charged / Includes 96 Doctors, Nurse Practitioners, Pharmacists & Other Licensed Medical Professionals - June 30, 2025

The Justice Department announced the results of its 2025 National Health Care Fraud Takedown, which resulted in criminal charges against 324 defendants, including 96 doctors, nurse practitioners, pharmacists, and other licensed medical professionals, in 50 federal districts and 12 State Attorneys General's Offices across the United States, for their alleged participation in various health care fraud schemes involving over \$14.6 billion in intended loss.

The government seized over \$245 million in cash, luxury vehicles, cryptocurrency, and other assets as part of the coordinated enforcement efforts.

The Centers for Medicare and Medicaid Services (CMS) also announced that it successfully prevented over \$4 billion from being paid in response to false and fraudulent claims and that it suspended or revoked the billing privileges of 205 providers in the months leading up to the Takedown. Civil charges against 20 defendants for \$14.2 million in alleged fraud, as well as civil settlements with 106 defendants totaling \$34.3 million, were also announced as part of the Takedown. ([Source](#))

2 Hospital CEOs Charged For \$12 Million Healthcare Fraud Scheme - July 28, 2025

Jose Huerta, 58, was the Chief Executive Officer for two Long-Term Acute Care hospitals located in El Paso, Texas. Israel Navarro, 47, owned one of the hospitals and was financially connected to the other.

Huerta and Navarro conspired together and with others to knowingly devise a scheme to engage in illegal pass-through billing of urine drug tests (UDTs).

Huerta's and Navarro's hospitals allegedly submitted false insurance claims to Blue Cross Blue Shield, indicating in those claims that the individuals tested were patients in their hospitals when they were not. The claims further indicated that UDT samples were taken from the patients and forwarded to a lab in the Dallas area. None of this was true. Over a six-month period, Huerta and Navarro submitted \$16 million dollars in claims for the laboratory testing of UDTs. The actual loss to Blue Cross Blue Shield attributed to Huerta's and Navarro's alleged fraud scheme totals more than \$12 million. ([Source](#))

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Company Awarded \$59 Million For Trade Secret Theft By Vice President - July 10, 2025

A nearly decade-long legal battle in the U.S. District Court for the Northern District of Illinois recently concluded with a significant jury verdict, underscoring the potentially severe consequences of trade secret theft claims. In Sonrai Systems, LLC v. Anthony M. Romano and The Heil Co. d/b/a Environmental Solutions Group, a jury awarded Sonrai Systems, LLC (Sonrai) nearly \$29 million in actual damages and an additional \$30 million in punitive damages after determining that its confidential information had been misappropriated.

The conflict began with a failed business relationship between Sonrai, a technology company specializing in automation and data collection for the waste hauling industry, and The Heil Company (Heil), a manufacturer of garbage trucks.

In 2014, the two companies entered into a confidentiality agreement to explore integrating Sonrai's proprietary "Vector" technology into Heil's fleet. Vector is a vehicle information tool that allows a garbage truck fleet operator to monitor relevant data from trucks in real time. After negotiations, Heil and Sonrai were unable to reach a deal for use of the technology.

Instead, Heil acquired another company, which it used to develop and launch a competing product called “Enhance.” Sonrai alleged that this new product was developed using its confidential information.

During the negotiations, the then-Executive Vice President of Sonrai worked with Heil to evaluate and demonstrate Sonrai’s technology. He later resigned from Sonrai and joined Heil, where Sonrai claimed he used misappropriated confidential information to aid in the development of Heil’s competing product. ([Source](#))

Hulk Hogan's Alcohol Brand Is Involved In A \$10 Million Lawsuit Against 2 Former Employees - July 11, 2025

WWE icon Hulk Hogan’s alcohol brand, “Real American” beer, is at the center of a \$10 million lawsuit involving a licensing company and two former employees.

Carma HoldCo Inc. filed the lawsuit in Illinois and alleges that its former president, Chad Bronstein, chief legal and licensing officer Nicole Cosby, and their company, Rahm Inc, violated state and federal trade secret laws by using proprietary information and intellectual property belonging to Carma when they launched the wrestler-themed beer company.

The lawsuit claims that Cosby and Bronstein violated their employment agreements by misappropriating and making use of its proprietary information and its marketing tactics and concepts when developing Rahm Inc. In other words, Carma is accusing its former executives of swiping its ideas and strategies and poaching Hogan away from them in order to launch their own beer using his name and likeness.

Carma frequently partners with celebrities to license their likenesses out to other companies, which are then used for a variety of products. It claims in the suit that it had entered into a deal with Hogan to be one of its brand ambassadors back in February 2023. ([Source](#))

Apple Sues Former Employee For Stealing Thousands Of Documents Before Joining Snap - July 1, 2025

Apple has accused a former engineer for its Vision Pro headset computer of stealing company trade secrets before starting a new job at Snap. In the June 24, 2025 court filing, Apple accuses Di Liu, a senior design engineer, of downloading thousands of documents in his final days at the Cupertino company last year and saving them to his personal cloud accounts.

Apple alleges that Liu didn’t inform the company when he resigned late last year that he was headed to Snap, a competitor and maker of smart glasses. As a result, Apple did not shut off his access to accounts and allowed him a customary two-week transition period, which he used to download company files, according to the lawsuit.

Many of the files downloaded by Liu had codenames for Apple projects and described the company’s technology, product design and supply chain, according to the lawsuit.

Apple says that all employees agree to keep Apple files confidential and that Liu broke confidentiality agreements he made when he joined. Liu worked for Apple between 2017 and 2024.

Apple is seeking damages and for Liu to have his devices inspected by a forensic examiner to make sure all the trade secrets are deleted.

The iPhone maker has sued several former employees in recent years for taking files when they left the company. Apple settled with former engineer Simon Lancaster in 2022 over providing information to a journalist. Apple also sued a former employee, Andrew Aude, in 2024 over leaking details to the media.

That lawsuit was dismissed after Aude apologized. The Cupertino company sued Rivos, a chip startup staffed by former Apple semiconductor employees, over its intellectual property, and settled in 2024.

Additionally at least three former Apple employees have also been arrested and accused by the government of taking company secrets and giving them to China-linked organizations. One pled guilty and was sentenced to four months in prison, and two are still in proceedings. ([Source](#))

Mercer Global Advisors [Suing 3 Former Employees For Stealing Trade Secrets](#) - July 16, 2025

Mercer Global Advisors continues to keep up the legal pressure and has sued 3 employees who left to work with a smaller, venture capital-backed company Savvy Wealth.

Mercer's complaint names Brian Jellig, Sandra Mapp and Sean O'Connor, who joined Savvy on July 3. All three worked at Epstein & White, which was managing around \$740 million when it was purchased by Mercer in early 2021.

On Friday, Mercer filed a lawsuit against the 3 former employees and Savvy, alleging they illegally conspired to steal client information and trade secrets. The advisors also resigned "abruptly" on the same day they joined Savvy, in violation of an agreement to provide 30 days notice, according to Mercer's complaint, which was filed in California Superior Court.

Mercer alleged that O'Connor downloaded "highly confidential information" from its systems "without authorization" one month before their departure and gathered information on more than two dozen clients the day before. It further accuses all three of attempting to poach Mercer clients in the days leading up to their resignation and after they had left.

Savvy allegedly aided the team's alleged breach of contract and client solicitation. The suit is seeking unspecified compensatory and punitive damages along with an injunction.

Mercer has a history of filing similar lawsuits against departing advisors. They currently have two pending lawsuits against former employees. ([Source](#))

Private International Investment Firm [Suing Former Employee For Trade Secret Theft](#) - July 10, 2025

Sun Valley Investments AG (Sun Valley) a leading private international investment firm, announced that it filed a lawsuit in the United States District Court for the Northern District of California on July 9, 2025, against former consultant Onil Gunawardana and his company, Akalytic Advisors, LLC for misappropriation of trade secrets, and other claims.

According to the lawsuit, Mr. Gunawardana, during his tenure as a consultant for Sun Valley Investments A.G., stole valuable trade secret source code from Sun Valley.

Sun Valley alleges that Mr. Gunawardana and Akalytic Advisors, LLC, are unlawfully using that source code for their own benefit, without Sun Valley's permission, and in violation of Mr. Gunawardana's legal obligations as a former consultant." ([Source](#))

Former Executive Accused Of Leaking Trade Secret To New Employer Using Personal E-Mail Accounts - July 28, 2025

Over the course of nearly five years, Lisa Chi, who served as Arhaus' Chief Marketing Officer for a furniture company, regularly sent proprietary information to her personal Gmail and Google Drive accounts. Among the emails listed in the suit is one with the subject line "5 year LRP" that Chi allegedly forwarded to her personal email on April 27, 2021. Attached was a presentation detailing "Arhaus' 4 Year Plan," which included information regarding sales, inventory and strategy. Chi also forwarded herself another email on Aug. 5, 2024, that discussed Arhaus' business strategy and referenced RH pricing, the lawsuit says."

On May 20, Restoration Hardware (RH), another furniture company, announced in a news release that Lisa Chi would be joining the competing company as president, co-chief merchandising and creative officer. RH, which is valued at \$4 billion, highlights Chi's accomplishments at Arhaus in the release, praising her work during "a period of rapid growth" where Arhaus also crossed the billion dollar threshold. Arhaus currently has a market cap of \$1.37 billion.

Arhaus alleges that RH received confidential information and trade secrets when it hired one of its former executives Lisa Chi in May 2025. After Lisa Chi joined RH, the company's product and marketing materials started to mirror Arhaus' marketing collateral. Arhaus alleged that consequently, the losses are "ongoing and cannot be remedied by damages alone." The company is seeking punitive damages in addition to damages proven at trial, plus "costs incurred herein and its reasonable attorney's fees." ([Source](#))

Mobile Phone Retailer Fires Employee For Stealing Customer Data & Posting On Internet - July 30, 2025

Mobile phone retailer Studio 7 in Bangkok has issued a public apology after an employee at a branch was found to have stolen and leaked a customer's personal photos and data.

The company said it has also filed a police complaint against its former employee. The data theft was revealed on Tuesday and sparked widespread outrage online.

The photos were allegedly circulated in a Telegram group, prompting multiple victims to consider legal action.

The police arrested the suspect on charges of importing obscene data into a computer system accessible to the public. ([Source](#))

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

Engineer Pleads Guilty To Stealing For Chinese Government's Benefit Trade Secret Technology Designed For Missile Launch And Detection - July 21, 2025

Chenguang Gong is a former engineer at a Southern California company. He pleaded guilty to stealing trade secret technologies developed for use by the U.S. government to detect nuclear missile launches, track ballistic and hypersonic missiles, and to allow U.S. fighter planes to detect and evade heat-seeking missiles.

In January 2023, the victim company hired Gong as an application-specific integrated circuit design manager responsible for the design, development and verification of its infrared sensors.

Beginning on approximately March 30, 2023, and continuing until his termination on April 26, 2023, Gong transferred thousands of files from his work laptop to three personal storage devices, including more than 1,800 files after he had accepted a job at one of the victim company's main competitors.

Law enforcement also discovered that, between approximately 2014 and 2022, while employed at several major technology companies in the United States, Gong submitted numerous applications to ‘Talent Programs’ administered by the People’s Republic of China (PRC).

The PRC government has established these talent programs as a means to identify individuals who have expert skills, abilities, and knowledge of advanced sciences and technologies in order to access and utilize those skills and knowledge in transforming the PRC’s economy, including its military capabilities. ([Source](#))

Woman Sentenced To Prison For Role In Information Technology Worker Fraud Scheme That Generated \$17 Million+ In Revenue For North Korea - , July 24, 2025

Christina Chapman was sentenced to prison for her role in a fraudulent scheme that assisted North Korean Information Technology (IT) workers posing as U.S. citizens and residents with obtaining remote IT positions at more than 300 U.S. companies. The scheme generated more than \$17 million in illicit revenue for Chapman and for the Democratic People’s Republic of Korea (DPRK or North Korea).

North Korea has deployed thousands of highly skilled IT workers around the world, including to the United States, to obtain remote employment using false, stolen, or borrowed identities of U.S. persons. To circumvent controls employed by U.S. companies to prevent the hiring of illicit overseas IT workers, the North Korean IT workers obtain assistance from U.S.-based collaborators.

Chapman helped North Korean IT workers obtain jobs at 309 U.S. companies, including Fortune 500 corporations. The impacted companies included a top-five major television network, a Silicon Valley technology company, an aerospace manufacturer, an American car maker, a luxury retail store, and a U.S media and entertainment company.

Chapman operated a “laptop farm” where she received and hosted computers from the U.S. companies at her home, deceiving the companies into believing that the work was being performed in the United States. Chapman also shipped 49 laptops and other devices supplied by U.S. companies to locations overseas, including multiple shipments to a city in China on the border with North Korea. More than 90 laptops were seized from Chapman’s home following the execution of a search warrant in October 2023. ([Source](#))

Justice Department Announces Coordinated, Nationwide Actions To Combat North Korean Remote Information Technology Fraudulent Workers Schemes - June 30, 2025

Law Enforcement Actions Across 16 States Result in Charges, Arrest, and Seizures of 29 Financial Accounts, 21 Fraudulent Websites, and Approximately 200 Computers.

The Justice Department announced coordinated actions against the Democratic People’s Republic of North Korea (DPRK) government’s schemes to fund its regime through remote information technology (IT) work for U.S. companies.

These actions include two indictments, an arrest, searches of 29 known or suspected “laptop farms” across 16 states, and the seizure of 29 financial accounts used to launder illicit funds and 21 fraudulent websites and approximately 200 Computers.

The schemes involve North Korean individuals fraudulently obtaining employment with U.S. companies as remote IT workers, using stolen and fake identities.

The North Korean actors were assisted by individuals in the United States, China, United Arab Emirates, and Taiwan, and successfully obtained employment with more than 100 U.S. companies. ([Source](#))

8 Individuals From China & Taiwan Involved In Fraudulent Scheme To Obtain Remote Jobs At 100+ U.S. Companies / Caused \$3 Million In Damages - June 30, 2025

Nine individuals have been indicted in Boston, Mass. including one New Jersey man and eight overseas actors from China and Taiwan in connection with an alleged scheme to generate revenue for the Democratic People's Republic of Korea (DPRK) weapons of mass destruction (WMD) programs. The alleged scheme involved the dispatchment of skilled information technology (IT) workers who, using stolen identities of U.S. persons, posed as domestic workers to obtain remote IT jobs with U.S. companies, including several Fortune 500 companies and a defense contractor

From approximately 2021 through October 2024, the defendants and other co-conspirators perpetuated a massive fraud scheme resulting in the transmission of false and misleading information to dozens of U.S. companies, financial institutions, and government agencies, including the Department of Homeland Security (DHS), the Internal Revenue Service (IRS), and the Social Security Administration (SSA).

Specifically, these defendants and their co-conspirators allegedly compromised the identities of more than 80 U.S. persons; fraudulently obtained remote jobs at more than 100 U.S. companies, including several Fortune 500 companies and a cleared defense contractor; received laptops and other hardware from U.S. companies; accessed, without authorization, the internal systems of these U.S. companies, including sensitive employer data and source code; generated at least \$5 million in revenue for the overseas IT workers; and caused U.S. victim companies to incur legal fees, computer network remediation costs, and other damages and losses of at least \$3 million.

The Democratic People's Republic of Korea IT workers' scheme involved the use of pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers, and third-party enablers in the United States and abroad.

The IT workers employed under this scheme also gained access to sensitive employer data and source code, including International Traffic in Arms Regulations data from a California-based defense contractor that develops artificial intelligence-powered equipment and technologies. ([Source](#))

4 North Koreans Charged For Fraudulent IT Workers Scheme To Infiltrate American Companies / Stole Nearly \$1 Million From Company - June 30, 2025

To generate revenue for the regime, the Democratic People's Republic of Korea (North Korea or DPRK) dispatches thousands of skilled IT workers around the world to deceive and infiltrate American companies.

In October 2019, the defendants traveled to the United Arab Emirates on North Korean documents and worked there as a team. In approximately December 2020 and May 2021, respectively, Kim Kwang Jin (using victim P.S.'s stolen identity) and Jong Pong Ju (using the alias "Bryan Cho") were hired as developers by an Atlanta, Georgia-based blockchain research and development company and a Serbian virtual token company.

Both defendants concealed their North Korean identities from their employers by providing false identification documents containing a mix of stolen and fraudulent identity information. Neither company would have hired Kim Kwang Jin or Jong Pong Ju had it known the defendants were North Korean citizens. Later, on a recommendation from Jong Pong Ju, the Serbian company hired "Peter Xiao," who in fact was Chang Nam Il.

After gaining their employers' trust, Kim Kwang Jin and Jong Pong Ju were assigned projects that provided them access to their employers' virtual currency assets.

In February 2022, Jong Pong Ju used that access to steal virtual currency then worth approximately \$175,000. In March 2022, Kim Kwang Jin stole virtual currency then worth approximately \$740,000 by modifying the source code of two of his employer's smart contracts.

This scheme has involved the dispatchment of skilled information technology (IT) workers who, using stolen identities of U.S. persons, posed as domestic workers to obtain remote IT jobs with U.S. companies, including several Fortune 500 companies and a defense contractor. ([Source](#))

North Korean Operative Reveals The Inner Workings Of The DPRK Fraudulent IT Worker's Scheme That Infiltrated Fortune 500 Companies - July 2, 2025

In a Fortune interview facilitated by a Seoul, South Korea NGO that supports North Korean defectors, Mr. Kim Ji-min describes his experience as a software developer inside North Korea's IT worker scheme.

Kim uses an alias to protect the lives of his friends and family who could be in danger from the regime because he spoke to Western media about his time as a developer.

His remarks offer a rare glimpse into the way North Korea has weaponized the global remote-work economy to fund its nuclear program.

For more than a decade, Kim Ji-min served as an IT worker inside a vast global scheme devised by North Korea's authoritarian leadership to evade crushing financial sanctions. Kim has since defected to South Korea.

Now, he is sharing his experience as a cog in the IT worker conspiracy employed by the Democratic People's Republic of Korea to amass billions to fund its weapons of mass destruction program. ([More Details](#))

LARGE FINES OR PENALTIES THAT HAVE TO BE PAID BECAUSE OF INSIDER THREAT INCIDENTS

No Incidents To Report

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

Accountant For Construction Company Sentenced To Prison For **Embezzling \$1.8 Million+ - July 21, 2025**

Richard Mandarino entered false payment requests in the construction company's accounting system, causing checks to be issued to vendor companies for goods and services that Mandarino knew were never provided. Mandarino then converted those payments to his and others' personal use. He concealed the thefts by creating fictitious credits and offsets in the construction company's accounting system.

Mandarino committed the fraud from 2015 to 2017 while he resided in Canada and worked on the Chicago construction company's Canadian business projects. As a result of his conduct, Mandarino caused losses totaling more than \$1.8 million. ([Source](#))

Employee Charged For **Stealing \$90,000+ Worth Of Funds - July 26, 2025**

Authorities with the Georgia Bureau of Investigation (GBI) issued a release on Friday stating 42-year-old Jessica Steele was arrested on Monday, July 14, 2025

Steele reportedly worked at Callaway Resort and Gardens in Georgia. Investigators with the Pine Mountain Police Department reportedly called the GBI in February 2022 to conduct an investigation.

The GBI statement indicates Steele "reportedly misappropriated more than \$90,000 worth of funds" from Callaway Gardens. ([Source](#))

Harris Teeter Employee Charged For [Stealing \\$11,000+ From Store - July 16, 2025](#)

Brittany Gardner, 35, is accused of stealing \$11,170 from a Harris Teeter after it was delivered to the store.

A Harris Teeter asset protection manager advised that one of his customer service managers, identified as Gardner, stole \$11,170 from Feb. 9 through June 5. The official noted 10 separate occasions that Gardner counted money and placed it into the safe. The company then said Gardner took the money out of the safe and pocketed it.

The most recent incident happened on June 5, when Gardner allegedly counted \$15,000 for deposit; however, only \$13,000 was deposited at the bank.

Gardner was caught on camera taking the money and later admitted to taking the \$2,000 during the incident. The affidavit states that Gardner admitted to taking between \$10,000 and \$11,000 from the store but couldn't recall the exact amount and dates.

Gardner has worked for Harris Teeter since 2009 and was on shift when the theft happened, police say. ([Source](#))

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY BECAUSE OF FINANCIAL PROBLEMS, FOR PERSONAL ENRICHMENT, TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING ADDICTIONS

Jacksonville Jaguars Employee Who [Stole \\$22 Million+ To Support Gambling Habit](#) Facing New Charges - July 11, 2025

Florida authorities brought state grand theft charges this week against the former Jacksonville Jaguars employee who stole more than \$22 million from the team while feeding his gambling habit, according to state records.

Amit Patel, 32, is already serving a 6½-year sentence at Williamsburg federal prison in South Carolina after pleading guilty in December 2023 to wire fraud and illegal monetary transactions. Now, he faces six counts of grand theft in Florida. Under state law, grand theft of \$100,000 or more is a first-degree felony punishable by up to 30 years in prison.

Patel admitted to stealing from the Jaguars over 3½ years while managing the team's virtual credit card program. Federal prosecutors claimed Patel lived a "life of luxury" that included lavish vacations and the purchase of a high-end watch and sports memorabilia.

The Jaguars later sued Patel in Florida state court for \$66.6 million in damages. That case is still pending. In July 2024, Patel filed a lawsuit against FanDuel in federal court claiming the sportsbook "exploited" his gambling addiction and intentionally ignored its responsible gaming and anti-money-laundering protocols. According to court documents, he transferred approximately \$20 million to FanDuel.

Patel has said he was previously diagnosed with a gambling disorder and was preyed upon by the website operator, according to a court filing. ([Source](#))

Company Bookkeeper And Husband Sentenced To Prison For [\\$1.4 Million Embezzlement Scheme Lasting 10 Years / Used Funds For Airline Tickets, Cruises, Etc. - July 28, 2025](#)

From 2003 until August 2021, Valerie Joseph served as a bookkeeper for a wholesale greenhouse and garden center located in Caroline County, Maryland.

Beginning in January 2011 and continuing into August 2021, the couple conspired to defraud the business.

Robin and Valerie Joseph schemed to make unauthorized charges to three credit card accounts associated with the business for personal gain. This included American Express and Capital One accounts, along with a Lowes / Synchrony financial account.

Routinely, for more than a decade, Robin and Valerie Joseph used credit cards associated with the victims' accounts to make numerous unauthorized purchases. The theft included unauthorized credit-card charges for \$200,000-plus at Walmart; \$53,000-plus to AT&T for personal phone bills; \$30,000-plus at a Japanese steak and seafood restaurant; and \$116,000-plus to PayPal. Robin and Valerie Joseph charged more than \$90,000 to Easton Utilities for utility bills; \$16,000 to Chesapeake College for tuition payments; \$2,500 to the University of Hawaii for college expenses; and \$3,800 for cosmetics.

The couple also charged more than \$195,000 to the Lowes Account. Several of the unauthorized Lowes account charges were to purchase materials and supplies to renovate their previous residence in Easton, Maryland.

Additionally, Robin and Valerie Joseph paid for airline tickets, cruises, Airbnb expenses, and hundreds of retailer gift cards using the victims' account.

The couple also used the victims' account to pay more than \$33,000 in veterinary expenses and charged various items related to their pets, including high-end bird cages for their tropical birds. ([Source](#))

Company Personnel Director Sentenced To Prison For [Embezzling \\$500,000+ / Used Funds To Pay For Debts, Gambling, Vacations, Etc.](#) - July 3, 2025

Between October 2020 and March 2022, Zachary Rugen was employed as the personnel director for a small company in St. Petersburg, Florida.

Rugen exploited that role to embezzle at least \$503,372.01 from the company. He used his access to the employer's payment processing system to direct funds intended for vendors and contractors to bank accounts he controlled. Rugen also paid some of his outstanding debts with company funds. To cover the fraud scheme, Rugen electronically submitted falsified and fraudulent payment invoices.

Rugen used the ill-gotten funds to live lavishly, including taking expensive vacations and gambling, and for his personal expenses.

During the sentencing hearing, the victim-company's chief operating officer testified that the fraud caused substantial financial hardship from which it will take the company at least five years to recover.

As a result of the embezzlement, one of the company's vendors nearly went out of business. ([Source](#))

Company Bookkeeper Sentenced To Prison For [Embezzling \\$300,000 From Employer For 7+ Years / Used Funds For Cruises, Vacations, College Tuition Fees, Etc.](#) - July 2, 2025

Kayellen Inskip admitted to using the credit card issued by her employer, Mears Floral, to make unauthorized personal purchases between August 31, 2021, through August 25, 2022.

However, Inskip was sentenced under facts that were presented to the Court in which her true scope of her embezzlement occurred beginning in 2014 and continuing into 2022, only stopping after her fraud was discovered by company officials.

Inskip used the company card to pay for travel including airplane tickets, vacations that included cruises with Carnival Cruise Line, and vacations to Disney World, as well as entertainment, restaurants, clothing, utilities, medical bills, and she even paid college tuition and fees for her own daughter.

Inskip used her position as a bookkeeper and Operations Manager with the business to authorize payments for her fraudulent purchases. Inskip would then provide false financial reports to officers in the company that allowed her to both hide her embezzlement from more than 7 years and ultimately steal nearly \$300,000.

Mears Floral was a Springfield, Missouri, business that started in 1949, serving retail florists in Arkansas, Kansas, Oklahoma, and Missouri.

This hometown business was in operation for over 70 years and based on statements made to the Court, Inskip's massive embezzlement resulted in Mears Floral going out of business, closing its doors, and the firing of its employees.

When Mears Floral closed its doors, it had to layoff nearly 33 employees, who had an average of nearly 11 years of employment with Mears Floral, as well as other employees who had worked for over 50 years with this well-known local business.

The loss of Mears Floral, at the hands of Inskip, caused an unknown amount of true losses to the company, its employees, and ultimately the local community who benefited from the operations of this successful business. ([Source](#))

Company Purchasing Manager Sentenced To Prison For Embezzling \$250,000+ By Using Company Credit Card To Transfer Money To His Personal PayPal Account - July 24, 2025

Timothy Pew, 43, was sentenced to federal prison, followed by 3 years of supervised release, for seven counts of wire fraud.

Between March 2023 and January 2023, Pew committed wire fraud by engaging in a scheme to embezzle over \$250,000 from his employer. Pew, who was employed as a purchasing manager for a manufacturing company in western Kentucky, embezzled the funds from the company by using a company credit card to transfer money to his personal PayPal account. ([Source](#))

Civil Service Director For City Charged For Stealing \$124,000+ To Pay Off Credit Card Debt - July 24, 2025

Civil service director (Rosa Pedraza) for the city of McAllen has been charged with theft for using a stranger's bank account to pay off more than \$124,000 in credit card debt.

A probable cause affidavit for her arrest said the investigation began on June 13 when a man filed a report with McAllen police after receiving a call from Texas Regional Bank about several fraudulent transactions originating from Capital One Online.

"They stated they had never had a credit card with Capital One and had not authorized anyone to use their bank information".

As the investigation unfolded, the man and his wife provided police with monthly bank statements that highlighted the unauthorized statements, all of which were linked to the Capital One credit card dating from Oct. 31, 2024 to Dec. 31, 2024. The couple also learned that the fraudulent activity went back farther. The affidavit said the alleged fraud began on Feb. 16, 2022 and lasted through May 19.

In all, the money the man lost from his bank account to pay Capital One accumulated to \$124,654.71.

Detectives found transactions made at various locations, including Sam's Club in McAllen and at the Lucky Eagle Casino in Eagle Pass.

Investigators were able to work with loss prevention officers and other methods to determine that a black 2020 Lexus Series 300 and silver GMC Canyon were linked to the suspect. Detectives also learned Pedraza worked for the city of McAllen and obtained her driver's license photo which they were able to link to an image of the person who used the credit card at the Sam's Club, according to the affidavit. ([Source](#))

EMPLOYEES' WHO EMBEZZLE / STEAL THEIR EMPLOYERS MONEY TO SUPPORT THEIR PERSONAL BUSINESS

Los Angeles County Employees Retirement Association Chief Security Officer Charged For [Sending \\$20,000 Of County Business To His Own Business](#) - June 4, 2025

Carmelo Marquez is a former interim Chief Security Officer for the Los Angeles County Employees Retirement Association (LACERA). He has been charged with pocketing nearly \$20,000 via a company he created while on the job and failing to disclose the conflict of interest under penalty of perjury.

Marquez initially worked as an independent contractor doing information security work for LACERA. In February 2023, he was named LACERA's interim chief security officer.

He is accused of failing to disclose under penalty of perjury that he had launched a business that sold software products and provided technical support directly to LACERA.

Marquez allegedly used his position to illegally funnel public contracts worth roughly \$120,000 through his own firm and profited \$19,904 through those transactions. He no longer works for LACERA. ([Source](#))

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

Disgruntled IT Worker Sentenced To Prison [For Cyber Attack Against Employer After Being Suspended From Work / Caused \\$270,00+ In Damages](#) - June 27, 2025

A disgruntled IT worker who launched a cyber attack on his employer after he was suspended from work has been jailed.

Mohammed Umar Taj began to take revenge on his employer within hours of being suspended from work in July 2022. He caused significant disruption to the company causing them to lose at least £200,000 in lost business as well as reputational harm.

Taj gained access to the company's premises and unlawfully accessed computer systems to deliberately alter login credentials to disrupt the company's day to day activities.

A day later, Taj changed access credentials and the company's multi-factor authentication so that he could adversely impact the activities of the firm's clients both in the UK and overseas in Germany and Bahrain.

He kept recordings of his activities and discussed the attack on phone recordings recovered forensically by investigators. ([Source](#))

Fired Information Technology Employee Arrested For [Launching Cyber Attack Against Former Employer That Deleted & Altered Data](#) - July 11, 2025

The Florida Department of Law Enforcement (FDLE) arrested 41-year-old Richard Wozniak in Flagler County on four counts of offenses against computer users.

FDLE said the investigation began in January after The Spice and Tea Exchange Company in St. Augustine said it suffered a cyber attack on its firewall and email that deleted and altered company data.

Wozniak is a former Information Technology employee of the company. FDLE said it determined that just minutes after being fired, Wozniak made unauthorized access to the business network, removing its firewall and exposing it to further security risk. ([Source](#))

THEFT OF ORGANIZATIONS ASSETS

Former Amazon Employee Arrested For [Stealing & Selling 2,000 Pairs Of Shoes Valued At \\$224,000+](#) - July 24, 2025

A former Amazon employee is facing charges of stealing work boots and sneakers through a program meant to provide free safety footwear to new employees of the online retailer.

Asraf Mohamed allegedly created accounts in the names of new employees without their knowledge and obtained 1,838 pairs of work boots and sneakers, later reselling them online.

Mohamed worked at an Amazon facility on Grand Avenue in Maspeth, New York from July 2020 to Sept. 2023, when he was terminated. In his role, he was responsible for training new drivers and had access to a national database of new employees.

Between Nov. 12, 2022, and June 9, 2023, Mohamed allegedly created 1,838 unique accounts with Zappos.com, an Amazon subsidiary, using the information of new employees through an Amazon program called Zappos at Work. The program was designed to provide workers with a free pair of work boots or sneakers to be worn on the job.

A total of 79 shoe orders were delivered to Mohamed's residential address, and another 1,759 orders were delivered to his brother's address in Queens. The footwear brands included Timberland, Dr. Martens, Wolverine, Carhartt, New Balance and Brooks.

Mohamed allegedly sold the shoes, which had a total retail value of \$224,834, on eBay. ([Source](#))

EMPLOYEE COLLUSION (WORKING WITH INTERNAL OR EXTERNAL ACCOMPLICES)

Operations Manager Charged For Role In [Embezzling \\$500,000](#) From Trucking Company - July 30, 2025

From May 2018 through May 2024, Dustin Jarrard served as an operations manager for Tribe Transportation, a large trucking business located in Gainesville, Georgia. As an operations manager, Jarrard had the authority to request expense reimbursements on truck drivers' behalf. To submit a request, Jarrard would send the company's accounting department the driver's name, the reason for the expense, and the amount of the reimbursement.

Over the course of more than three years, Jarrard sent fraudulent reimbursement requests to Tribe Transportation. In certain cases, Jarrard requested reimbursement for drivers who were not actually employed by the company, which resulted in payments Jarrard personally redeemed for his own use.

In other cases, Jarrard enlisted Tribe Transportation drivers in his scheme and falsely submitted payment requests for expenses never incurred and layover bonuses that were not earned. After receiving funds that were not owed to them, the drivers transferred some of the money to Jarrard for his personal use. Jarrard allegedly stole more than \$500,000 that was intended to help truckers on the road. ([Source](#))

Former Walgreens Manager Sentenced To Prison For Role In [7 Inside-Job Robberies That Stole \\$28,000+](#) - July 23, 2025

This incident involved Kamanye Williams, Gianni Robinson, London Teeter and Michael Robinson, the last 2 who were Walgreen's store managers.

4 co-conspirators devised a scheme to carry out armed robberies of the Chinatown Walgreens in Washington DC store, nearly once a month, beginning in July 2023, when either Robinson or Teeter were working. As a store managers, Robinson and Teeter knew the timing of cash transfers within the business.

The co-conspirators would also relay information to each other on how many armed security guards were present in the Chinatown Walgreens and how much cash was in the manager's office at any given time.

When Robinson was on duty, he gave inside information to his nephew, Gianni Robinson, who then relayed it to Williams so that Williams could more easily rob the store.

The robberies occurred on July 18, 2023, Aug. 2, 2023, Sept. 2, 2023, Nov. 10, 2023, Dec. 4, 2023, Jan. 9, 2024, and Feb. 11, 2024. In their plea agreements, the co-defendants admitted that they stole and split at least \$28,983.

In each robbery, Williams entered the Chinatown Walgreens wearing clothing selected to disguise his identity. Williams brandished a firearm at employees of the Walgreens, and at Special Police Officers assigned to guard the store, and then demanded business proceeds located in the Manager's Office. Williams forced employees into the manager's office or accessed the manager's office using a code provided by Michael Robinson or Teeter. Williams then robbed the employees and fled through a rear exit.

Michael Robinson and Teeter took turns pretending to be the "victim" manager on duty, knowing that the robberies would be captured on internal surveillance.

Michael Robinson later admitted that he and Teeter reviewed internal surveillance footage of a robbery, and discussed how to make future robberies look more authentic. Michael Robinson asked Williams to assault him during the robberies to make it look more real.

In response to the robberies, the Chinatown Walgreens hired armed Special Police Officers to protect the business.

Undeterred, the co-conspirators continued the robberies and Williams escalated to stealing the firearms from the Special Police Officers. ([Source](#))

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Hospital Nurse Sentenced To Prison For [Stealing Opioid For Personal Use](#) - July 7, 2025

Jacqueline Brewster was employed as a travel nurse at Raleigh General Hospital in Beckley from September 2021 until February 2022.

Brewster admitted that she unlawfully accessed and used individually identifiable health information of patients at Raleigh General Hospital to divert hydromorphone, an opioid, for her personal use.

To carry out her diversion scheme, Brewster fraudulently obtained the hydromorphone from automated controlled substance dispensing machines at the hospital. Brewster used her personal biometrics to access the machines and a patient's individually identifiable health information to begin the process of checking out hydromorphone for that patient. Once the machine's secure drawer opened, Brewster siphoned off a portion of hydromorphone from its vial and diluted what remained in the vial with another substance to make it appear full. Brewster then canceled or nulled the transaction to conceal her removal of the controlled substances.

Brewster admitted that she carried out her scheme to use individually identifiable patient health information and steal hydromorphone under false pretenses and for personal gain many times from on or about September 17, 2021, through on or about February 1, 2022. ([Source](#))

Hospital Nurse Sentenced To Prison For [Stealing Vials Of Medication](#) - July 29, 2025

Sean Falzarano was employed at Yale New Haven Hospital (YNHH) as a Registered Nurse. As part of his employment, Falzarano was granted access to secure locations used by YNHH to store controlled substances, including Lorazepam.

On January 31, 2022, Falzarano took vials containing Lorazepam solution that he knew were intended to be dispensed to patients. He removed a portion of the Lorazepam solution from at least one of the vials, replaced the contents with an inert solution, and returned the vial to the secure location where it was available for distribution to patients. Falzarano was confronted on that date by YNHH employees who were investigating drug tampering. A search of Falzarano's backpack revealed vials, crimping tools, saline, vial caps, and syringes. ([Source](#))

OTHER FORMS OF INSIDER THREATS

Employee Jailed For Secretly [Drugging His Coworker With 'Truth Serum'](#) - July 22, 2025

A man in Shanghai was sentenced to prison for drugging his colleague with something he thought would make him spill company secrets. A "truth serum". He wanted access to confidential work plans. So he used sedatives.

The employee named Li, invited his colleague Wang out to dinner. During three separate meals, Li slipped the "truth serum" into Wang's drinks (Beer, Wine, Tea). Wang became dizzy, nauseated, and, at one point was unconscious. After the third incident, he finally caught the pattern: he only felt sick after seeing Li.

Tests revealed clonazepam and xylazine in his system, both strong central nervous system depressants. Clonazepam is a regulated psychotropic. Xylazine is typically used to tranquilize animals. Their combined effects don't encourage honesty; they suppress motor function.

Police raided Li's home and found the bottle, which tested positive for both substances. Confronted with the evidence, he confessed to all three incidents. ([Source](#))

Former Business Vice President Charged For Attempting To [Extort His Former Employer For \\$100,000+ After Being Fired](#) - July 10, 2025

Bryan Chapman was the Vice President of a nationwide business located in the Middle District of Pennsylvania.

After he was fired, Chapman attempted to extort the business by claiming that he would expose that the company had taken trade secrets from a supplier. Chapman demanded six-months' severance in exchange for his silence, which would have amounted to over \$100,000. The company refused to be extorted. ([Source](#))

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

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

Former IHOP Employee Arrested For **Stealing \$3,300 / Conspired With Manager - July, 1, 2025**

A former IHOP employee has been arrested after warrants say he and a manager conspired and robbed the Greenville location last month. William Brown was arrested by Greenville police for robbing the IHOP.

Employees told police a man entered the restaurant, held a worker at gunpoint and demanded money. Warrant say Brown, who used to work at the breakfast chain, and IHOP manager Chico Haddock conspired to rob the restaurant. Brown stole nearly \$3,300, according to warrants. ([Source](#))

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Sports Store Employee Charged For **Setting Fire To Store Causing \$44 Million In Damages - July 14, 2025**

The Mebane Police Department in North Carolina are investigating a suspicious fire that broke out in sport store.

The Mebane Police Department responded to Sports Endeavors on Corporate Park Drive to assist the Mebane Fire Department with a reported structure fire. The fire was quickly contained by fire crews. No employees were injured, but one firefighter sustained minor injuries while responding.

Following an investigation by the Mebane Fire Department, it was found that the fire was suspicious. Through the course of a thorough investigation by the North Carolina Department of Insurance, the State Fire Marshal's Office, and the Mebane Police Department, a suspect was found.

Authorities believe Jacari Bunting started the fire, and he has been charged with 'Felony Burning of a Commercial Structure' and 'Felony Setting Fire to a Commercial Structure Resulting in Injury to a Firefighter.' Bunting was working at Sports Endeavors when he set it afire, reportedly causing \$44,000,000 in damage. ([Source](#))

Hardee's Employee Arrested For **Stabbing His Manager In The Head - June 30,2025**

Authorities arrested 31-year-old Romario Dean Monuma, who fled the restaurant after the stabbing. Police were dispatched after a caller reported the incident, saying the fleeing suspect was wearing a red hoodie and carrying the alleged weapon.

When police arrived on the scene, the manager was responsive to questions, but bleeding heavily down the entire left side of her body. The manager identified the suspect as a part-time employee of Hardee's. ([Source](#))

Burger King Employee Stabbed In Throat By Co-Worker - June 29, 2025

A Burger King employee was injured after getting stabbed in the throat by a co-worker.

Police responded to a report of a stabbing at the Burger King. There, they found an employee with a stab wound to the throat, police said. The injured employee was taken to the hospital and the current extent of their injuries is not known. Another employee of the Burger King, 18-year-old Brinley Capellan-Lopez, was arrested at the scene and charged with multiple crimes, including attempted homicide. ([Source](#))

McDonald's Manager Stabbed To Death By Another Employee - July 10, 2025

The manager of an McDonald's in Michigan was stabbed to death after getting into an argument with another employee. Jennifer Harris, 39, has been identified by her family as the McDonald's manager who was stabbed to death. Harris had been an employee of McDonald's for the past 15 years, according to her family.

Michigan State Police said they were called to McDonald's on a report of shots fired and a stabbing. They arrived and found a customer holding a gun and Harris had been stabbed.

According to MSP, the other employee had been sent home early after getting into an argument with Harris. The employee returned with a knife and stabbed Harris, police said.

During the stabbing, a customer at the McDonald's drive-through witnessing the assault fired a shot into the air to break up the fight. No one was struck. The suspect then tried to flee the scene, but the customer chased after her and held her at gunpoint before police arrived. ([Source](#))

Wegmans Warehouse Employee Facing Charges For Fatally Shooting Another Employee - July 29, 2025

Police responded to the warehouse around for a report of a shooting. J'Mere Ridley-Smith, 25, was pronounced dead at the scene from a gunshot wound.

Investigators determined the suspect, Kyshonn Green, 32, fled the scene and left the state. U.S. Marshals arrested Green in Knoxville, Tennessee. Police said he had a loaded 9mm handgun. ([Source](#))

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS

<https://nationalinsidethreatsig.org/nitsig-insidethreatreportssurveys.html>



INSIDER THREATS DEFINITION / TYPES

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 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

The information compiled below was gathered from research conducted by the National Insider Threat Special Interest Group (NITSIG), and after reviewing NITSIG Monthly Insider Threat Incidents Reports.

WHO CAN BE AN INSIDER THREAT?

- Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- Current & Former Employees / Contractors - Trusted Business Partners
- Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- Negligent Employees (1 - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (2 - Failure By Action, Behavior Or Response) (3 - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- Opportunist Employees (1 - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (2 - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (3 - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- Collusion By Multiple Employees To Achieve Malicious Objectives
- Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)
- Employees Involved In Foreign Nation State Sponsored Activities (Recruited - Incentives)
- Employees Ideological Causes (Promoting Or Supporting Political Movements To Engage In Activism Or Committing Acts Of Violence In The Name Of A Cause, Or Promoting Or Supporting Terrorism)
- Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)

INSIDER THREAT DAMAGING ACTIONS **CONCERNING BEHAVIORS**

There are many different types of Insider Threat incidents committed by employees as referenced below. While some of these incidents may take place outside the workplace, employers may still have concerns about the type of employees they are employing.

- Facility, Data, Computer / Network, Critical Infrastructure Sabotage By Employees (Arson, Technical, Data Destruction, Etc.)
- Loss Or Theft Of Physical Assets By Employees (Electronic Devices, Etc.)
- Theft Of Data Assets By Employees (Espionage (National Security, Corporate, Research), Trade Secrets, Intellectual Property, Sensitive Business Information, Etc.)
- Unauthorized Disclosure Of Sensitive, Non-Pubic Information (By Using Artificial Intelligence Websites Such as ChatGPT, OpenAI, Etc. Without Approval)
- Theft Of Personal Identifiable Information By Employee For The Purposes Of Bank / Credit Card Fraud
- Financial Theft By Employees (Theft, Stealing, Embezzlement, Wire Fraud - Deposits Into Personal Banking Account, Improper Use Of Company Charge Cards, Travel Expense Fraud, Time & Attendance Fraud, Etc.)
- Contracting Fraud By Employees (Kickbacks & Bribes That Can Have Damaging Impacts To Employer)
- Money Laundering By Employees
- Fraudulent Invoices And Shell Company Schemes By Employees
- Employee Creating Hostile Work Environment (Unwelcome Employee Behavior That Undermines Another Employees Ability To Perform Their Job Effectively)
- Workplace Violence Internal By Employees (Arson, Bomb Threats, Bullying, Assault & Battery, Sexual Assaults, Shootings, Deaths, Etc.)
- Workplace Violence External (Threats From Outside Individuals Because Of Relationship, Marriage Problems, Etc.) Directed At Employee(s))
- Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- Employees Involved In Drug Distribution
- Employees Involved In Human Smuggling, The Possession / Creation Of Child Pornography, The Sexual Exploitation Of Children

Other Damaging Impacts To An Employer From An Insider Threat Incident

- Stock Price Reduction
- Public Relations Expenditures
- Customer Relationship Loss, Devaluation Of Trade Names, Loss As A Leader In The Marketplace
- Compliance Fines, Data Breach Notification Costs
- Increased Insurance Costs
- Attorney Fees / Lawsuits
- Increased Distrust / Erosion Of Morale By Employees, Additional Turnover
- Employees Lose Jobs, Company Downsizing, Company Goes Out Of Business



TYPES OF ORGANIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

NITSIG Monthly Insider Threat Incidents Reports reveal that governments, businesses and organizations of all types and sizes are not immune to the Insider Threat problem.

- 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
- Schools, Universities, Research Institutes
- Non-Profits Organizations, Churches, etc.
- Labor Unions (Union Presidents / Officials, Etc.)
- And Others

WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

An employer - employee relationship can be described as a circle of trust / 2 way street.

The employee trusts the employer to treat them fairly and compensate them for their work.

The employer trusts the employee to perform their job responsibilities to maintain and advance the business.

When an employee feels **This Trust Is Breached**, an employee may commit a **Malicious** or other **Damaging** action against an organization

Cultivating a culture of trust is likely to be the single most valuable management step in safeguarding an organization's assets.

After new employees have been satisfactorily screened, continue the trust-building process through on-boarding, by equipping them with the knowledge, skills and appreciation required of trusted insiders.

Listed below are some of the common reasons that trusted employees develop into Insider Threats.

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

BILLIONAIRE LIFESTYLE



INSIDER THREATS

Employees' Living The Life Of Luxury Using Their Employers Money

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 prison 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](#))

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 INVOLVED?

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 Kozdema 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 bank's money to pay Ryan individually or fund Ryan's own businesses. Using bank money this way helped Ryan conceal 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 Kozdema 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

Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024

Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

Between May and August 2022, numerous patients at Surgicare North Dallas suffered cardiac emergencies during routine medical procedures performed by various doctors. About one month after the unexplained emergencies began, an anesthesiologist who had worked at the facility earlier that day died while treating herself for dehydration using an IV bag. In August 2022, doctors at the surgical care center began to suspect tainted IV bags had caused the repeated crises after an 18-year-old patient had to be rushed to the intensive care unit in critical condition during a routine sinus surgery.

A local lab analyzed fluid from the bag used during the teenager's surgery and found bupivacaine (a nerve-blocking agent), epinephrine (a stimulant) and lidocaine (an anesthetic) — a drug cocktail that could have caused the boy's symptoms, which included very high blood pressure, cardiac dysfunction and pulmonary edema. The lab also observed a puncture in the bag.

Ortiz surreptitiously injected IV bags of saline with epinephrine, bupivacaine and other drugs, placed them into a warming bin at the facility, and waited for them to be used in colleagues' surgeries, knowing their patients would experience dangerous complications. Surveillance video introduced into evidence showed Ortiz repeatedly retrieving IV bags from the warming bin and replacing them shortly thereafter, not long before the bags were carried into operating rooms where patients experienced complications. Video also showed Ortiz mixing vials of medication and watching as victims were wheeled out by emergency responders.

Evidence presented at trial showed that Ortiz was facing disciplinary action at the time for an alleged medical mistake made in his one of his own surgeries, and that he potentially faced losing his medical license. ([Source](#))

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](#)) ([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 2016, 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](#))

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

Protect America's Competitive Advantage

High-Priority Technologies Identified in China's National Policies

CLEAN ENERGY	BIOTECHNOLOGY	AEROSPACE / DEEP SEA	INFORMATION TECHNOLOGY	MANUFACTURING
CLEAN COAL TECHNOLOGY	AGRICULTURE EQUIPMENT	DEEP SEA EXPLORATION TECHNOLOGY	ARTIFICIAL INTELLIGENCE	ADDITIVE MANUFACTURING
GREEN LOW-CARBON PRODUCTS AND TECHNIQUES	BRAIN SCIENCE	NAVIGATION TECHNOLOGY	CLOUD COMPUTING	ADVANCED MANUFACTURING
HIGH EFFICIENCY ENERGY STORAGE SYSTEMS	GENOMICS	NEXT GENERATION AVIATION EQUIPMENT	INFORMATION SECURITY	GREEN/SUSTAINABLE MANUFACTURING
HYDRO TURBINE TECHNOLOGY	GENETICALLY - MODIFIED SEED TECHNOLOGY	SATELLITE TECHNOLOGY	INTERNET OF THINGS INFRASTRUCTURE	NEW MATERIALS
NEW ENERGY VEHICLES	PRECISION MEDICINE	SPACE AND POLAR EXPLORATION	QUANTUM COMPUTING	SMART MANUFACTURING
NUCLEAR TECHNOLOGY	PHARMACEUTICAL TECHNOLOGY		ROBOTICS	
SMART GRID TECHNOLOGY	REGENERATIVE MEDICINE		SEMICONDUCTOR TECHNOLOGY	
	SYNTHETIC BIOLOGY		TELECOMMS & 5G TECHNOLOGY	

Don't let China use insiders to steal your company's trade secrets or school's research.
The U.S. Government can't solve this problem alone.
All Americans have a role to play in countering this threat.

Learn more about reporting economic espionage at <https://www.fbi.gov/file-repository/economic-espionage-1.pdf/view>
 Contact the FBI at <https://www.fbi.gov/contact-us>

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

The websites listed below are updated daily and 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 (**6,500+ Incidents**).

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

<https://flipboard.com/@cybercops911/insider-threat-incident-magazine-resource-guide-tkh6a9b1z>

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

<https://twitter.com/InsiderThreatDG>

Follow Us On Twitter: @InsiderThreatDG

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

<http://www.insiderthreatincidents.com> or

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

SPECIALIZED REPORTS

Why Insider Threats Remain An Unresolved Cybersecurity Challenge

Produced By: IntroSecurity And NITSIG / June 2025

The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

This report provides detailed recommendations for mitigating Insider Risks and Threats. It outlines strategies for strengthening IRMP's and cross-departmental governance, adopting advanced detection techniques, and fostering key stakeholder and employee engagement to protect an organizations Facilities, Physical Assets, Financial Assets, Employees, Data, Computer Systems - Networks from the risky or malicious actions of employees.

The goal of this report is to provide anyone involved in managing or supporting an IRM Program with a common sense approach for identifying, deterring, mitigating and preventing Insider Risk and Threats. Through research, collaboration and conversations with NITSIG Members, and discussions with organizations that have experienced actual Insider Threat incidents, the report outlines recommendations for an organization to defend itself from the very costly and damaging Insider Threat problem.

[\(Download Report\)](#)

U.S. Government Insider Threat Incidents Report For 2020 To 2024

The NITSIG was contacted by Senator Joni Ernst's office in December 2024, and a request was made to write a report about Insider Threats in the U.S. Government for the Department Of Government Efficiency (DOGE). ([Download Report](#))

Department Of Defense (DoD) Insider Threat Incidents Report For 2024

The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. ([Download Report](#))

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. ([Download Report](#))

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>

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

<https://www.nationalinsiderthreatsig.org/critical-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>

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

The Insider Threat Defense Group (ITDG) provides organizations with the **core skills / advanced knowledge, resources and technical solutions** to identify, manage, prevent and mitigate Insider Risks - Threats.

Since 2009, the ITDG has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction. ITDG training courses and consulting services have empowered organizations with the knowledge and resources to develop, implement, manage, evaluate and optimize a comprehensive Insider Risk Management (IRM) Program (IRMP) for their organizations.

Being a pioneer in understanding Insider Risks - Threats from both a holistic, non-technical and technical perspective, the ITDG stands at the forefront of helping organizations safeguard their assets (Facilities, Employees, Financial Assets, Data, Computer Systems - Networks) from one of today's most damaging threats, the Insider Threat. **The financial damages from a malicious or opportunist employee can be severe, from the MILLIONS to BILLIONS.**

With 15+ years of IRMP expertise, the ITDG has a deep understanding of the collaboration components and responsibilities required by key stakeholders, and the many underlying and interconnected cross departmental components that are critical for a comprehensive IRMP. This will ensure key stakeholders are **universally aligned** with the IRMP from an enterprise / holistic perspective to address the Insider Risk - Threat problem.

IRM PROGRAM TRAINING & 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 Evaluation & Optimization Training Course (Develop, Management, Enhance)
- ✓ 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

STUDENT / CLIENT SATISFACTION

ITDG [training courses](#) have been taught to over **1000+** individuals. Our clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM. Our client satisfaction levels are in the **EXCEPTIONAL** range, due to the fact that the ITDG approaches IRM from a real world, practical, strategic, operational and tactical perspective. You are encouraged to read the feedback from our clients on [this link](#).

The ITDG Has Provided IRM Program 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, Verizon, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, 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 NITSIG 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 Risk Management Program Training Course Instructor / Consultant

Insider Threat Investigations & Analysis Training Course Instructor / Analyst

Insider Risk / Threat Vulnerability Assessor

[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