INSIDER THREAT INCIDENTS REPORT
FOR
August 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

TABLE OF CONTENTS

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 31** 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 AUGUST 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

UK Government Fires 50 Employee For The Unauthorized Access Of Taxpayers Records / 354 Others Disciplined For Data Security Breaches - August 16, 2025

HM Revenue and Customs (HMRC) has revealed that hundreds of staff have accessed the records of taxpayers without permission or breached security in other ways. HMRC dismissed 50 members of staff last year for accessing or risking the exposure of taxpayers' records.

354 tax employees have been disciplined for data security breaches since 2022, of whom 186 have been fired - and some were dismissed for accessing confidential information. HMRC holds sensitive data including salary and earnings, which staff cannot access without a good reason.

96 staff were disciplined last year for data breaches and 50 were dismissed. The year before, 138 employees were disciplined, and 68 were dismissed. As well as accessing records, data breaches can include changing records without permission, losing documents and not properly disposing of equipment that contains sensitive data.

One employee was dismissed after sending the data of 100 people to his personal email address — including their salaries and National Insurance numbers. He printed the information on his home computer and was dismissed for gross misconduct. (Source)

Senior Executive Embezzled $2.35 Million By Creating Fraudulent Work Orders - August 20, 2025

GungHo Online Entertainment (Japanese Video Game Developer), the company that produces Puzzles & Dragons, has claimed that a former senior executive embezzled ¥346 million ($2.35 million) by creating fake work and outsourcing orders to misappropriate company funds.

In a statement released on August 14, 2025 (via Automaton), GungHo Online Entertainment alleged that a former senior executive, who was dismissed for disciplinary reasons, had "engaged in misconduct" over the last few years, including the "misappropriation of company funds through the place of fictitious work orders" (via Google Translate).

"The company became aware of the suspicion of fraudulent activity by the former employee and conducted an initial investigation with the support of forensic teams from external law and accounting firms to determine whether the former employee had engaged in fraudulent activity and to clarify the facts of the matter," GungHo Online Entertainment wrote in the statement.

GungHo Online Entertainment goes on to allege that, as a result of this initial investigation, it "confirmed" the former employee had embezzled approximately ¥246 million ($1.67 million) of company funds by using a third-party job-ordering service to create "fictitious work orders" which named the company as the client and the former employee as the contractor. (Source)

India Call Center Employees Involved In Massive Credit Card Scam - August 16, 2025

The Delhi Police have arrested 18 individuals for duping State Bank of India (SBI) credit card holders of nearly ₹2.6 crore in a nationwide fraud. The operation, which ran for six months, relied on insider leaks at a Gurugram-based call centre and a sophisticated money-laundering network that spanned cash deals and cryptocurrency transactions.

According to Deputy Commissioner of Police (IFSO) Vinit Kumar, the gang gained access to confidential SBI customer data with the help of insiders at Teleperformance, a call centre in Gurugram responsible for handling sensitive Card Protection Plan (CPP) data. The insider leak was allegedly orchestrated by call centre employees Vishesh Lahori and Durgesh Dhakad, who siphoned off SBI credit card data.

Using this leaked information, the fraudsters posed as SBI executives, contacting unsuspecting customers and tricking them into sharing one-time passwords (OTPs) and card verification values (CVVs). Armed with this information, the gang purchased high-value electronic gift cards from online platforms, particularly travel booking websites. (Source)

New Zealand Military Soldier Found Guilty Of Espionage - August 19, 2025

A military court has convicted a New Zealand soldier of attempted espionage for a foreign power – the first spying conviction in the country's history. The soldier was caught offering to pass military base maps and photographs to an undercover officer posing as an agent for the foreign nation, the court martial heard.

The court accepted the soldier's guilty plea on Monday but the hearing continued to allow the panel to determine a sentence, which is expected within days.

The soldier was the first person to be convicted of spying by a New Zealand court and only the second to be tried after a former public servant was acquitted of espionage in 1975. He admitted to attempted espionage, accessing a computer system for a dishonest purpose, and knowingly possessing an objectionable publication.

The man had copies of a live streamed video of the March 2019 killing of 51 worshippers at two mosques in Christchurch by white supremacist Brenton Tarrant. The soldier became a person of interest in the aftermath of the Christchurch attack as police cracked down on rightwing extremist groups, the court heard. While monitoring him, the New Zealand government became aware he had "made contact with a third party, indicating he was a soldier who was wanting to defect", according to an agreed summary read out by the prosecution.

An undercover officer then made contact with the would-be spy, claiming to be from that foreign nation. The soldier said he could provide "mapping and photographs, and he could possibly get a covert device into Army Headquarters". He provided telephone directories of several military camps, including information classified as restricted. The man offered an assessment of vulnerabilities at Linton Military Camp, as well as access codes and information that would allow for unauthorised access to the camp and nearby Ohakea airbase.

In an affidavit written by the soldier and read out by his lawyer in court, he admitted to being a member of extremist groups Action Zealandia and the Dominion Movement. (Source)

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES

Microsoft Fires 2 Employees For Breaking Into The Office Of The CEO / Employees Opposed To The Israeli Military's Use Of Azure Software As Part Of Its Invasion Of Gaza - August 28, 2025

Microsoft said that it had terminated two employees who broke into President Brad Smith's office.

The news comes after 7 current and former Microsoft employees held a protest in the company's building in Redmond, Washington, in opposition to the Israeli military's alleged use of the company's software as part of its invasion of Gaza.

The protesters, affiliated with the group No Azure for Apartheid, gained entry into Smith's office and had demanded that Microsoft end its direct and indirect support to Israel.

"Two employees were terminated today following serious breaches of company policies and our code of conduct," a Microsoft spokesperson said in a statement, noting unlawful break-ins at the executive offices.
"These incidents are inconsistent with the expectations we maintain for our employees. The company is continuing to investigate and is cooperating fully with law enforcement regarding these matters," the statement added. In the aftermath of the protests, Smith claimed that the protestors had blocked people out of the office, planted listening devices in the form of phones, and refused to leave until they were removed by police.

It was reported that earlier this month, that the Israeli military had used Microsoft's Azure cloud infrastructure to store the phone calls of Palestinians, leading the company to authorize a third-party investigation into whether its technology has been used in surveillance.

Smith said on Tuesday that the company would "investigate and get to the truth" of how services are being used. According to Smith, No Azure For Apartheid also mounted protests around the company's campus last week, leading to 20 arrests in one day, with 16 having never worked at Microsoft.

Microsoft's actions come after tech giant Google fired 28 employees last year following a series of protests against labor conditions and the company's contract with the Israeli government and military for cloud computing and artificial intelligence services. In that case, some employees had gained access to the office of Thomas Kurian, CEO of Google's cloud unit. (Source)

U.S. GOVERNMENT

U.S. State Department Employees Left Sensitive Papers In Hotel Printer With Details About Meeting Between President Donald Trump & Russian President Vladimir Putin In Alaska - August 16, 2025

Papers with U.S. State Department markings, were found in the business center of an Alaskan hotel. They revealed previously undisclosed and potentially sensitive details about the Aug. 15 meetings between President Donald Trump and Russian President Vladimir V. Putin in Anchorage.

Eight pages, that appear to have been produced by U.S. staff and left behind accidentally, shared precise locations and meeting times of the summit and phone numbers of U.S. government employees.

3 guests at Hotel Captain Cook, a four-star hotel located 20 minutes from the Joint Base Elmendorf-Richardson in Anchorage where leaders from the U.S. and Russia convened, found the documents left behind in one of the hotel's public printers. NPR reviewed photos of the documents taken by one of the guests, who NPR agreed not to identify because the guest said they feared retaliation. (Source)

23 FEMA Employees Terminted After Discovering Massive Cyber Security Failures And For Failing To Fix Critical Vulnerabilities - August 29, 2025

Homeland Security Secretary Noem terminates inept FEMA employees after uncovering massive Cyber Security failures.

FEMA Chief Information Officer (CIO) Charles Armstrong, Chief Information Security Officer (CISO) Gregory Edwards, and 22 other FEMA IT employees directly responsible were immediately terminated.

While conducting a routine cybersecurity review, the DHS Office of the Chief Information Officer (OCIO) discovered significant security vulnerabilities that gave a threat actor access to FEMA's network. The investigation uncovered several severe lapses in security that allowed the threat actor to breach FEMA's network and threaten the entire Department and the nation as a whole.

The entrenched bureaucrats who led FEMA's IT team for decades resisted any efforts to fix the problem. Instead, they avoided scheduled inspections and lied to officials about the scope and scale of the cyber vulnerabilities.

Failures included: an agency-wide lack of multi-factor authentication, use of prohibited legacy protocols, failing to fix known and critical vulnerabilities, and inadequate operational visibility.

FEMA spent nearly half a billion dollars on IT and cybersecurity measures in Fiscal Year 2025 alone and delivered virtually nothing for the American people. Despite burning hundreds of millions of taxpayer dollars, FEMA's IT leadership still neglected its basic duties and exposed the entire Department to cyberattacks. "This unacceptable behavior will not be tolerated in the Trump administration," added Secretary Noem. (Source)

FAA Contractor Sentenced To Prison For Illegally Acting As An Agent Of The Iranian Government - August 26, 2025

From at least December 2017 through June 2024, Abouzar Rahmati conspired with Iranian government officials and intelligence operatives to act on their behalf in the United States, including by meeting with Iranian intelligence officers in Iran, communicating with coconspirators using a cover story to hide his conduct, obtaining employment with an FAA contractor with access to sensitive non-public information, and obtaining open-source and non-public materials about the U.S. solar energy industry and providing it to Iranian intelligence.

From June 2009 to May 2010, Rahmati served as a First Lieutenant in the Islamic Revolutionary Guard Corps (IRGC), an Iranian military and counterintelligence organization under the authority of the Supreme Leader of Iran. After being discharged from the IRGC, Rahmati lied to the United States government regarding his military service with the IRGC in order to, among other things, gain employment as a U.S. government contractor.

In August 2017, Rahmati offered his services to the Iranian government through a senior Iranian government official who previously worked in Iran's Ministry of Intelligence and Security and with whom Rahmati had previously attended university.

Four months later, in December 2017, Rahmati traveled to Iran, where he met with Iranian intelligence operatives and government officials and agreed to obtain information about the U.S. solar energy industry, to provide that information to Iranian officials, and to conduct future communications under a cover story based on purported discussions about research with fellow academics.

Upon returning to the United States in early 2018, Rahmati obtained various private and open-source materials related to the U.S. solar energy industry and provided them to an official from the office of Iran's Vice President for Science and Technology in response to tasking from Iranian government officials.

In response to tasking from Iranian officials, and in furtherance of his role as an agent of the Government of Iran, Rahmati exploited his employment as an FAA contractor by downloading at least 172 GB of the company's files. Rahmati stored those files on removable media, which he took to Iran, where he provided sensitive documents to the Government of Iran in April 2022.

At the April 2022 meeting in Iran, Iranian intelligence officers told Rahmati and his brother that they were seeking information, including new ideas and technology not available in Iran. They further explained that if Rahmati brought such information to Iran, the Government of Iran could provide Rahmati with financial incentives, including free or low-interest loans and grants.

Later in April 2022, also in response to tasking from Iranian government officials, Rahmati sent additional information relating to solar energy, solar panels, the FAA, U.S. airports, and U.S. air traffic control towers to his brother, who lived in Iran, so that he would provide those files to Iranian intelligence. (Source)

Small Business Administration Employee Pleads Guilty To $550,000 Fraudulent COVID-19 Pandemic Loan - August 12, 2025

Rena Barrett, 45, became a Small Business Administration (SBA) employee in October 2020.

In May 2021, she submitted a fraudulent Economic Injury Disaster Loan (EIDL) application for $170,000. SBA initially declined to approve this loan, but in July 2021, Barrett approved the loan herself.

SBA shortly thereafter discovered that Barrett had abused her position by approving that loan and other loans she or her relatives submitted. Barrett received nearly half of the approximately $550,000 she sought to obtain and resigned from the SBA after her wrongdoing was discovered. (Source)

U.S. Postal Inspector Charged With Stealing $330,000+ In Cash From Elderly Victims / Used Fund For Home Improvements, Travel & Escorts - August 29, 2025

Scott Kelley is a former U.S. Postal Inspector. He was arrested and charged for allegedly stealing over $330,000 in cash from packages mailed by elderly victims and then laundering the cash. Kelly used the stolen cash to pay for a pool patio and lighting, granite countertop for his outdoor bar, Caribbean cruise expenses and escorts. He also is alleged to have stolen cash from an evidence locker and then blamed a direct report for the missing cash.

Kelley was a Postal Inspector at the Boston Division headquarters of the U.S. Postal Inspection Service, the law enforcement arm of the Postal Service. From 2015 until June 2022, he was the Team Leader of the Mail Fraud Unit, which, among other things, investigated lottery and other scams that targeted senior citizens and other vulnerable populations. In June 2022, Kelley was transferred to serve as the Team Leader of the Mail Theft Unit, a position he held until August 2023.

Between January 2019 and Aug. 11, 2023, Kelley used deceptive emails to cause unwitting postal employees to intercept packages that a USPIS algorithm had flagged as scam, and send them to him. In total, Kelley allegedly requested that approximately 1,950 packages be intercepted and mailed to him. It is alleged that Kelley opened intercepted parcels that looked or felt like they might contain cash, and that he stole any cash inside.

7 victims who were scammed into mailing cash in parcels that Kelley allegedly intercepted, and that he opened the parcels and stole the cash. The average age of the victims was 75, with the oldest victim being 82. The victims mailed between $1,400 and $19,100 cash. It is alleged that Kelley met with one victim in person and told them that that he did not know what had happened with their package and that their loss was their own fault because they had mailed cash. None of the victims recovered their packages or their cash. (Source)

U.S Postal Service Employee Pleads Guilty To Role In Stealing $156,000 Of Checks From Mail - August 28, 2025

Kierra Blount, at times while employed by the U.S. Postal Service in Stamford Connecticut stole mail and obtained stolen mail for the purpose of obtaining checks that were payable to other individuals.

In approximately November 2021, Blount opened a bank account using the name and social security number of an individual without the identity theft victim's knowledge. Blount and others fraudulently changed the payee names on stolen checks to the name of the identity theft victim, forged the victim's signature on the back of the checks, and deposited them into the bank account Blount opened. From November 2021 until the account was closed in April 2022, Blount and others deposited approximately $156,000 in fraudulent checks into the account. Some check deposits were reversed by the bank, and Blount and others used approximately $81,000 for their own purposes.

On June 20, 2023, investigators conducted a court-authorized search of Blount's Stamford residence and seized a significant amount of stolen mail and other items related to this scheme, including debit cards in the names of other individuals, checks totaling more than $285,000, and sheets of paper containing personal information of other individuals, including names, dates of birth, addresses, email addresses, and security question answers. Subsequent analysis of cell phones seized from Blount on that date revealed images of stolen checks, personal identifying information for more than 50 individuals, and communications using the Telegram app with unknown individuals involved in the scheme. (Source)

U.S. Postal Service Mail Carrier Pleads Guilty To Role In Stealing 100+ Checks - Credit Cards From Mail / Used Funds For Trips, Luxury Good, Etc. - August 11, 2025

Mary Ann Magdamit formerly worked as a letter carrier for the United States Postal Service in Torrance, California.

She pleaded guilty to stealing checks and debit and credit cards from the mail then selling them to her accomplices for three years, using the illicitly obtained funds to take international trips and buy luxury goods, and then flaunting the cash on Instagram.

From at least 2022 until July 2025, Magdamit stole mail containing checks, personal identifying information (PII), and debit and credit cards. She then activated the stolen bank-issued cards online, used the cards to make purchases, and sold some stolen cards to her co-conspirators.

She also arranged to have her co-conspirators cash the stolen checks, usually by people using counterfeit identity documents in the name of the check's payee. Federally insured banks and credit unions were victimized in this scheme.

Law enforcement searched Magdamit's apartment in December 2024, and seized 133 stolen credit and debit cards,16 U.S. Department of Treasury checks, and a loaded, un-serialized Glock gun.

Agents also discovered luxury goods purchased with cards she stole from the mail. She also used stolen cards on international trips she took to Turks and Caicos and Aruba. Magdamit posted on Instagram her luxury purchases and vacations, and flaunted stacks of hundred-dollar bills. Magdamit has agreed to forfeit a Rolex watch and other luxury goods. (Source)

Department Of Labor Employee Charged For Fraudulently Obtaining $45,000+ In COVID Unemployment Assistance Benefits - August 26, 2025

Mo Yuong Kang worked as an Industrial Hygienist with the Occupational Safety and Health Administration, an agency of the DOL, from June 2016 until July 2023. In 2020 and 2021, Kang was a full-time employee of the DOL and earned $86,667 and $90,738, respectively.

In April 2020, Kang allegedly submitted a false PUA application to the Division of Unemployment Assistance (DUA). Kang claimed that he was "self-employed, an independent contractor, or a gig worker and COVID-19 has severely limited his ability to perform his normal work," and that he had not earned more than $89 a week since March 8, 2020. The DUA approved Kang's claim, and through September 2021 Kang subsequently submitted weekly certifications to the DUA allegedly claiming that he did not work and did not receive any income during those weekly periods. Based upon his application registration and those weekly certifications, Kang allegedly received $45,868 in PUA benefits he was not entitled to. (Source)

U.S. Embassy Employee Extradited To U.S. To Face Charges For Cocaine Import Conspiracy - August 6, 2025

Jairo Eliezer Arias Caceres allegedly orchestrated a cocaine smuggling scheme while employed as a security officer at the U.S. Embassy in the Dominican Republic and as a former security officer at the airport in Santo Domingo

Since April 2023 through December 2023, Caceres while employed as a security officer by the U.S. Embassy in the Dominican Republic operated a transnational conspiracy to import cocaine into the United States.

Caceres devised a scheme through which couriers smuggled cocaine into various airports in the New York area by disguising the cocaine in the packaging of items purchased from the Santo Domingo Airport Duty Free store.

Before working for the U.S. Embassy, where he was employed from 2018 through 2025, Caceres also worked for at least seven years as security officer at the Santo Domingo Airport. Caceres exploited his former positions of authority at the Embassy and the Airport in order to operate this narcotics importation scheme. (Source)

DHS Inspector General Report (August 2025) On Problems With TSA Insider Threat Program And Coordinating Investigations - August 13, 2025

The Transportation Security Administration (TSA) did not clearly assign law enforcement roles to its program offices, which led to internal disagreements and friction between TSA's Law Enforcement / Federal Air Marshal Service (LE/FAMS) Insider Threat Section (ITS) and TSA Investigations related to referring and investigating allegations of misconduct. TSA's conflicting management directives resulted in impeded collaboration and deconfliction of investigations into risks to the Nation's transportation system, potentially jeopardizing TSA's ability to mitigate insider threats.

We found that ITS did not consistently refer to or deconflict with TSA Investigations cases involving alleged TSA employee misconduct as required. Because ITS and TSA Investigations receive allegations from sources available to both offices, ITS' lack of deconfliction risks inadvertently compromising the integrity of investigations.

Based on our analysis of 177 case records, we found ITS did not refer to TSA Investigations 21 allegations of criminal misconduct involving TSA employees that originated from sources available to both offices. Of those 21 non-referrals, ITS opened a case on 12 allegations to gather additional information without coordinating with TSA Investigations.

We also found that ITS did not have an approved, documented standard operating procedure or a formalized training plan to ensure ITS' personnel process and refer allegations of TSA employee misconduct consistently. (Source)

U.S. Forest Service Law Enforcement Officer Sentenced To Probation For $13,000+ Of Time & Attendance Fraud - August 27, 2025

Nathan Snead documented his regular and overtime hours on his Time and Attendance Record for each pay period and signed a certification they were correct.

On May 2, 2023, based on information Snead was not working his claimed hours, agents installed a GPS tracker on his government-issued patrol vehicle to monitor his movements. The tracker data showed Snead's patrol vehicle was stationary at his house during hours he claimed to be working.

On several occasions, Snead certified on his Time and Attendance Record he worked an 8-hour regular shift. However, his patrol vehicle remained stationary at his house for the entire 8 hours. Additionally, Snead claimed overtime hours when his patrol vehicle was stationary at his house for much of his regular shift and for the entire period of claimed overtime.

Agents also evaluated Snead's law enforcement statistics from 2021 through 2023. His productivity levels, measured via incident reports and the issuance of violation notices, were much lower than other similarly situated LEOs. Snead was ordered to pay restitution in the amount of $13,923.77. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Army Sergeant Shoots 5 Soldiers / Co-Workers At Fort Stewart In Georgia - August 6, 2025

The man accused of shooting five soldiers at Fort Stewart in Georgia on Wednesday morning has been identified as U.S. Army Sergeant Quornelius Radford. Radford, who has been apprehended, is 28 years old and serves as an automated logistics sergeant assigned to the ABCT.

The soldiers were shot in the 2nd Armored Brigade Combat Team (ABCT) area of the base, according to a social media post by the U.S. Army. All the soldiers were treated on-site and then transported to Winn Army Community Hospital. No motive for the shooting has been released by the Army. (Source)

U.S. Navy Veteran Charged With Defrauding Navy Of $9 Million+ By Bid-Rigging And False Billing With Help Of Navy Employee Who Was Paid Kickbacks - August 20, 2025

A Navy veteran has been charged with defrauding the Navy out of more than $9 million through a bid-rigging and contract steering scheme that involved paying kickbacks and other benefits to a co-conspirator, who was a Navy insider at the time, the Justice Department announced today.

Cory Wright was enlisted in the Navy from February 1997 until his retirement in May 2017. At various points from 2005 to 2017, Wright worked for the Navy's Mobile Utilities Support Equipment division (Muse), located at the naval base in Port Hueneme in Ventura County California.

Muse was responsible for providing management, technical, and logistics support for power systems, including large generators, for U.S. Department of Defense operations around the world, including active combat zones.

To accomplish its mission, Muse engaged with prime contractors to procure goods and services, typically by tasking orders to subcontractors.

When Wright neared retirement in late 2016, he and an individual Co-Conspirator 1 agreed to create a Georgia-based company, C&C Power Solutions LLC (CCP). Co-Conspirator 1 was a fellow Navy enlistee who ultimately retired from the Navy in 2021 and held various positions at Muse, including supervisory positions that allowed him to exercise considerable influence over naval contracts. The scheme lasted from December 2016 to August 2022.

Wright and Co-Conspirator 1 created the company with the understanding that Co-Conspirator 1 would be a 50% partner in the business once he retired from the Navy. Co-Conspirator 1 told Wright that he would ensure CCP received Navy contracts, including task orders from a prime contractor. In exchange for directing the Navy contracts to CCP, Wright paid Co-Conspirator 1 thousands of dollars in kickback payments and other benefits, including payments to a sporting club operated by Co-Conspirator 1.

To provide initial funding for CCP's business operations, Co-Conspirator 1 caused a prime contractor and subcontractors to issue payments to CCP for products and services that CCP did not provide.

Once CCP was operational, Wright and Co-Conspirator 1 engaged in a bid-rigging scheme to ensure CCP received subcontracts from a prime contractor. For example, in connection with a 2017 task order worth approximately $790,496, Wright and Co-Conspirator 1 caused the submission of multiple fake contract bids that contained estimated project costs that were significantly higher than the bid that CCP submitted.

Wright also generated false and fraudulent invoices that represented CCP had completed work and delivered products to Muse when, in fact, CCP had not completed its contractual obligations.

In turn, this caused the prime contractor to submit invoices containing Wright's false information, causing the Navy to issue payments on the invoices.

Starting in September 2017, Wright and Co-Conspirator 1 conspired to secure CCP as Muse's next prime contractor, which they knew would be worth tens of millions of dollars to their company. Wright and Co-Conspirator 1 worked together to generate bogus documents – including a fraudulent past performance questionnaire – to obtain the contract. They also hid from the Navy Co-Conspirator 1's role and financial interest in CCP, including his direct involvement in the company's successful bid proposal for the prime contract with the Navy.

From the time the Navy awarded CCP this lucrative contact in July 2019 until it terminated three task orders awarded to the company in late 2022 and early 2023, Wright continued to submit false documents, including invoices, to the Navy for obtaining money that his company and he were not entitled to receive.

In total, Wright and his co-schemers defrauded the Navy out of approximately $9,128,515. (Source)

U.S. Army Soldier Charged With Espionage For Attempting To Send U.S. Defense Information To Russia's Ministry Of Defense - August 6, 2025

Taylor Lee is an active-duty service member in the U.S. Army stationed at Fort Bliss, and holds a Top Secret (TS) / Sensitive Compartmented Information (SCI) security clearance.

From approximately May 2025 through the present, Lee sought to establish his U.S. Army credentials and send U.S. defense information to Russia's Ministry of Defense. In June 2025, Lee allegedly transmitted export-controlled technical information on the M1A2 Abrams Tank online and offered assistance to the Russian Federation, stating, "the USA is not happy with me for trying to expose their weaknesses," and added, "At this point I'd even volunteer to assist the Russian federation when I'm there in any way."

In July, at an in-person meeting between Lee and who he believed to be a representative of the Russian government, Lee allegedly passed an SD card to the individual. Lee proceeded to provide a detailed overview of the documents and information contained on the SD card, including documents and information on the M1A2 Abrams, another armored fighting vehicle used by the U.S. military, and combat operations.

Several of these documents contained controlled technical data that Lee did not have the authorization to provide. Other documents on the SD card were marked as Controlled Unclassified Information (CUI), and featured banner warnings and dissemination controls. Throughout the meeting, Lee stated that the information on the SD card was sensitive and likely classified. (Source)

U.S. Navy Sailor Convicted Of Spying For China / Chinse Intelligence Officer Paid $12,000 Sailor For Sensitive Ship Information - August 21, 2025

Patrick Wei was a machinist's mate for the amphibious assault ship U.S.S. Essex. He also held a U.S. security clearance and had access to sensitive national defense information about the ship's various systems.

Wei was approached in February 2022 via social media by someone who claimed to be a naval enthusiast. The individual was in reality a Chinese intelligence officer. Between February 2022 and his arrest in August 2023, as their relationship developed, Wei, at the request of the officer, sent extensive information about the Essex, including photographs, videos, and about its weapons. He also sent detailed information about other U.S. Navy ships that he took from restricted U.S. Navy computer systems. In exchange for this information, the intelligence officer paid Wei more than $12,000 over 18 months. (Source)

U.S. Army Captain Pleads Guilty To Theft And Sale Of $150,000+ Of Government Property - August 25, 2025

Jacob Suenkel stole valuable equipment from various units at Fort Stewart on multiple occasions extending from late 2024 through May of 2025, all while serving as a captain in the United States Army. The stolen equipment included costly items such as skid-steer loaders, UTVs, trailers, generators, welders, commercial grade hand tools, and a tractor. After stealing these items, Suenkel would then market them for sale on social media and sell them to unsuspecting buyers.

Suenkel admitted that the total amount of financial loss caused by his actions exceeded $150,000, produced an initial payment of $50,000 to go toward the monetary component of his sentence, and agreed to be discharged from the Army with an adverse characterization of service, which will result in the loss of veterans' benefits. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Police Officer Sentenced To Prison For Smuggling Firearms To Criminals - August 14, 2025

Michael Nieto, a sworn law enforcement officer, repeatedly purchased and resold firearms. Among others, Nieto supplied firearms to Ernesto Vazquez, a key member of a criminal conspiracy that smuggled hundreds of firearms to the Dominican Republic, Puerto Rico, and Haiti. In addition, to benefit the conspiracy, Nieto used police databases to provide sensitive and confidential information to Vazquez.

Between June 6, 2022, and September 4, 2024, Nieto purchased at least 58 firearms. Many of the firearms were identical and were purchased together or close in time to one another.

On October 17, 2024, FBI and ATF agents executed a search warrant at Nieto's residence, during which 12 firearms were still in Nieto's possession.

On October 17, 2024, Nieto was interviewed by FBI and ATF agents. He admitted to repeatedly buying and reselling guns to individuals, including Vazquez, despite knowing that Vazquez was transferring these guns to third parties, in violation of federal law. Nieto also admitted that Vazquez had provided him with illegal items, including a machinegun conversion device. (Source)

County Sheriff Charged For $50,000 Extortion Scheme Involving Business Owner - August 8, 2025

Sheriff Steven Tompkins, who serves as the Sheriff for the Suffolk County Sheriff's Department in Massachusetts, has been charged with extortion involving the purchase of an equity interest in a Boston-based cannabis company (CC).

The FBI took Tompkins into custody for allegedly extorting $50,000 from the owner of a national cannabis retailer seeking to do business in Boston. We believe what the Sheriff saw as an easy way to make a quick buck on the sly is clear cut corruption under federal law," said Ted Docks, Special Agent in Charge of the Federal Bureau of Investigation, Boston Division.

It is alleged that Tompkins pressured an individual at the CC for stock, reminding the individual that Tompkins had the CC with its licensing efforts. (Source)

Federal Corrections Officer Admits To Taking $40,000 In Bribes To Smuggling Contraband Into Prison - August 7, 2025

Hector Lopez is a former federal correctional officer at Federal Corrections Institution Gilmer In West Virginia.

Lopez, age 41, pled guilty to bribery of a public official. According to the plea agreement, Lopez accepted $40,000 in payments from or on behalf of inmates as payment for smuggling contraband into the prison. (Source)

Police Detective Charged For Purchasing & Using Stolen Data From Illegal Online Website - August 21, 2025

Since August 2018, the FBI has been investigating an illicit online marketplace known as Genesis Market, whose operators compile stolen data, such as computer and mobile device identifiers, email addresses, usernames, and passwords, from malware-infected computers around the globe and package it for sale on the market. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.

Between March and August 2020, Terrance Ciszek, a Buffalo Police Detective, purchased 11 packages on Genesis Market that included 194 stolen account credentials.

In March and April 2020, Ciszek is accused of attempting to use the stolen credit cards to make purchases. In addition, on April 15, 2020, Ciszek is accused of possessing and using the identification, including name, address and credit card, of another person. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former Department of Vehicle Regulation Employee Fired Because She Reported Co-Workers Selling Driver's Licenses To Illegal Immigrants - August 13, 2025

Melissa Moorman is a former Kentucky Transportation Cabinet (KYTC) clerk working for the Department of Vehicle Regulation.

Moorman discovered in 2024 that 2 co-workers from the Department of Vehicle Regulation were selling documents to nonresidents without proper immigration screenings or testing. Her lawyers argued that she knew of the crime after being invited to participate. "The employees were being paid under the table, Moorman stated. I immediately let my supervisor know about it."

Moorman stated these co-workers would sell licenses for $200 per person approximately four to five times a day, for over two years. Moorman said that every case she encountered involved an illegal immigrant.

After Moorman reported the crime, the co-workers were fired, and a federal investigation was launched into KYTC. Moorman allegedly met with federal investigators in January after learning those employees were using her credentials and log-in information without her knowledge at the time.

She has said that she was instructed by her supervisor to provide the employees with this information as they waited for their own credentials when they first started.

Moorman was also fired. Moorman filed a lawsuit in April, claiming that KYTC violated the Kentucky Whistleblower Act, which protects public whistleblowers who come forward with information about misconduct. She has asked for her job and benefits to be reinstated along with back pay.

KYTC released a statement to Fox News Digital confirming that it had "identified a number of irregularities and revoked 1,985 credentials" and terminated all employees involved, but offered no updates. (Source)

County Employee Charged With Embezzling $800,000 By Diverting Payments For Drilling & Well Permits To His Own Accounts - August 27, 2025

A 47-year-old man who worked for San Mateo County Environmental Health Services has been charged with embezzlement and other offenses for allegedly diverting applications and payments for drilling and well permits to his own accounts for an amount of nearly $800,000, prosecutors said Friday.

Kian Atkinson was hired in 2016. In January 2017, he allegedly started diverting incoming application fees for well permits to his personal work email, then issued false permits and diverted payments to his own Square account, according to the San Mateo County District Attorney's Office.

When Atkinson was transferred to another assignment this March, the alleged fraud was discovered and he was put on leave. Atkinson then ran up $20,000 in personal charges on his agency-issued credit card, prosecutors said. (Source)

Township Supervisor Pleads Guilty To Forging And Issuing $147,000+ Of Checks To Herself - August 4, 2025

Linda Tarlecki was the former Secretary/Treasurer for Conyngham Township, Columbia County in Pennsylvania. From 2013 through 2017, Tarlecki defrauded the Township and Fulton National Bank of over $147,000 by issuing forged paychecks to herself to which she was not entitled. (Source)

City Employee Sentenced To Prison For Role In Embezzling $121,000+ Of Homeless Housing Funds - August 6, 2025

Vanessa Robinson, is a former Amarillo City Texas employee. She was sentenced to prison for embezzling $121,000+ from a federal program that provided housing for homeless individuals.

Robinson was a Grant Manager for the City of Amarillo from 2013 to January 2024 in Amarillo's Community Development Department.

In this role, she was responsible for distributing funds supplied by the U.S. Department of Housing and Urban Development (HUD) to help homeless or near-homeless citizens in Amarillo, Texas with housing costs.

For approximately five years, from July 2019 to September 2024, Robinson embezzled from the program by various means.

She posed as a program recipient and took steps to live rent-free for more than two years, including enlisting a co-conspirator—another former employee who participated in a similar scheme—to act as Robinson's case worker and communicate with Robinson's landlord.

The twenty-five months of Robinson's rent-free living cost the program $34,673. Robinson admitted that she also created fraudulent lease agreements and a fictitious landlord, using her husband's identity, to receive funds from HUD's Emergency Services Grant.

Additionally, she filled out fraudulent applications in family members' names to enable them to receive housing assistance. In total, Robinson caused the program to spend $121,325 on Robinson's fraudulent applications, leases, and vouchers. (Source)

City Mayor Sentenced To Prison For Demanding $100,000 In Bribes - August 14, 2025

Patrick Wimberly served as the mayor of the City of Inkster, Michigan, from 2019 through 2023.

In the spring of 2022, Wimberly demanded $100,000 in cash payments to facilitate the sale of property owned by the City (Referred To As "Parcel 1) to an outside party (Referred To As Person A).

Over several months, Person A provided Wimberly with monthly cash bribes to secure the purchase of this property.

The monthly payments started at $5,000 but the parties agreed to eventually increase that amount. Person A did not move to increase the bribe payments immediately, leading Wimberly to complain that he was due "10 a month." As requested, Person A then increased the monthly payments to $10,000.

In total, Person A provided $50,000 in cash to Wimberly for the purpose of winning the bid for Parcel 1. The Federal Bureau of Investigation intervened before the property could be transferred to Person A. (Source)

County Department Of Corrections Employee Arrested For Stealing $50,000+ - August 22, 2025

The Georgia Bureau of Investigation said 49-year-old Lakina Gay was taken into custody and booked into the Coweta County Jail. She is facing five counts of theft by taking.

Gay, who worked as an office manager, misappropriated between $50,000 and $100,000 from the commissary account between 2019 and 2023. (Source)

City Council Member Pleads Guilty To Accepting $3,000 Bribe Payment From Business Owner - August 13, 2025

Jorge Salinas admitted that between June 2019 and March 2020, he participated in a scheme involving businesses seeking contracts with the city of Edinburg. Salinas, then a councilman, attended meetings where a business owner sought to reinstate a long-term contract that had expired and converted to month-to-month terms.

The business operated in Edinburg and the surrounding area. The owner had sought both to secure new work agreements and maintain existing ones with the city.

The owner spoke with Miguel Garza who outlined what would be needed to persuade the council to approve the deal. Garza claimed to know several council members, to include Salinas.

He said that for a payment, he could deliver Salinas' vote in favor of the contract and ensure a majority of council members supported it. Part of the money would go to certain members of the council who made up the majority.

On July 23, 2019, Salinas met with Garza and the business owner to discuss the pending contract. The business owner gave Garza $3,000 at that time, because Garza had represented they had an agreement to secure the Edinburg City Council vote on behalf of the business owner's company.

By attending this meeting, Salinas aided and abetted Garza's criminal scheme to have council members take official acts in exchange for monetary payment. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

13,000 Montgomery County Maryland Public School Employees Have Outdated Criminal History Checks - August 6, 2025

Montgomery County Public Schools (MCPS) has several deficiencies in its background screening process, leading to nearly 13,000 employees with outdated criminal history checks, according to an investigation by the county's Office of the Inspector General. That figure represents almost half of the more than 25,800 employees who work for the school district, according to the MCPS website.

In a report on its investigation released on Monday, the inspector general's office found that nearly 13,000 employees had outdated criminal history checks, and almost 5,000 individuals who may have unsupervised access to students haven't undergone a Child Protective Services (CPS) check.

Also, some contractors and volunteers with unsupervised access to students began work prior to the completion of criminal history checks, according to the report.

"The fact remains that thousands of individuals with unsupervised access to MCPS schools and students have not had a criminal history check in more than five years and thousands more have not completed a CPS check," the report said. "In the end, only one entity is tasked with and has accepted the responsibility for obtaining these background checks to safeguard employees and students, and that is MCPS."

In response, MCPS said Monday in a statement that it was releasing a background screening action plan to correct failures noted in the report.

The report and the district's response to the inspector general's office highlight an apparently contentious relationship between MCPS and the office. MCPS said the report included "significant inaccuracies and mischaracterizations," while the inspector general's office said MCPS senior leaders don't demonstrate "either accountability or transparency" regarding the issues noted in its report.

County Council President Kate Stewart (D-Dist. 4) and Vice President Will Jawando (D-At large) said in a statement Monday they were deeply alarmed by the report, saying it "reveals a culture of siloed work." (Source)

College Professor Pleads Guilty To Embezzling $670,000+ From Finance Company - August 14, 2025

Between 2019 and 2021, James Kroger, an attorney and, at the time of his indictment, a tax and accounting professor at Gustavus Adolphus College, embezzled over $670,000 from Lone Star Municipal Finance Company, LLC, a real estate joint venture in which he was a partner. To carry out the scheme, Kroger convinced his partner to invest approximately $840,000 into Lone Star to purchase distressed properties in Texas. Kroger managed the day-to-day operations of Lone Star. Kroeger used his position of trust to embezzle most of the invested funds, through transfers into his own personal bank account under the guise of "loans" from the company.

Kroger spent the money he embezzled on extravagant personal purchases. These purchases included large cash withdrawals, purchases of gold and silver bullion, checks to family members, paying off loans against insurance policies, and retail and travel purchases from Amazon, eBay, Apple, Delta, and other vendors. (Source)

Public Schools Payroll Services Director Sentenced To Prison For Stealing $470,000 - August 8, 2025

Between 2014 and April 2022, Kim Weinrich was employed by Mustang Public Schools in Oklahoma as Payroll Supervisor. Weinrich was later promoted to Director of Payroll Services in 2021. In her roles with the District, Weinrich administered, processed, and reconciled the bi-monthly payroll for the District's employees.

Beginning in July 2016, Weinrich manipulated the District's payroll accounting software to increase her net pay each pay period, and deposited the stolen funds into her personal bank account.

Weinrich's scheme resulted in several District employees underreporting their federal and state withholdings, which reduced the amount of their tax refunds. In all, between July 2016 and April 2022, Weinrich defrauded the District out of approximately $470,000. (Source)

University Of Utah Worker Arrested For Attempting To Kill Co-Worker - August 1, 2025
A 21-year-old University of Utah employee was arrested on attempted murder charges after he allegedly stabbed his coworker in the neck with a knife he brought from home.

The 2 part-time janitors were working in a building in the Ft. Douglas area when Jose Alfredo Ramirez-Porchas allegedly stabbed the 19-year-old victim. The victim had his back turned from Ramirez-Porchas at the time of the attack.

Following the stabbing, the victim ran away from Ramirez-Porchas and was able to be treated on the scene for what officials described as superficial wounds to his neck.

University of Utah police were able to locate Ramirez-Porchas near the Alta Ski Resort in Big Cottonwood Canyon and took him into custody. Porchas admitted to officers that he had decided the previous night to kill the victim, despite the victim not having done anything to motivate the attack. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Vice President Sentenced To Prison For $2.3 Million+ Embezzlement Scheme Over 10 Years / Used Funds To Pay Credit Card Bills - August 12, 2025
Kellie Johnson was employed with First Community Bank in Alabama for approximately 25 years.

Between July 2013 and June 2023, Johnson embezzled money from First Community Bank's Federal Reserve account to pay personal expenses, primarily credit card bills. To conceal her scheme, Johnson falsified transactions to reconcile the balance of the Federal Reserve account in the bank's general ledger and deleted her ACH transactions.

Johnson also altered account statements sent by the Federal Reserve that she was required to provide to the bank president, auditors, and others. The scheme ended when the bank president received a call from the Federal Reserve notifying him that the bank's ACH account was overdrawn.

When the bank president asked Johnson to provide the latest account statement, she provided a fraudulent statement showing a positive balance in the account.

Over the decade that she stole money from the bank, Johnson conducted approximately 273 fraudulent ACH transactions totaling over $2.3 million. Additionally, Johnson deprived the bank of $138,185.40 in interest income to the Federal Reserve account. (Source)

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

Former Clerk At Hospital Pleads Guilty To $1.6 Million COVID Pandemic Relief Funds Scheme Involving Data Stolen From 4000+ Hospital Patients - August 7, 2025

Wilkins Estrella and Charlene Marte pled guilty to conspiracy to commit wire fraud and bank fraud in connection with using social security numbers and other personally identifiable information belonging to hundreds of victims to open debit cards and attempt to fraudulently obtain $1.6 million in pandemic relief funds from the Internal Revenue Service (IRS) and the New York State Department of Labor.

The scheme resulted in almost $1 million in actual losses. Estrella, a former clerk at a Bronx hospital, is also charged with the wrongful disclosure of individually identifiable health information for accessing and stealing the data of at least 4,005 hospital patients for use in the fraud scheme.

From at least 2020 to 2022, Estrella and his romantic partner, Marte, misused the names, social security numbers, and other personally identifiable information belonging to hundreds of individuals to fraudulently obtain almost $1 million in COVID-19 stimulus checks and tax refunds from the IRS and unemployment insurance benefits from the New York State Department of Labor.

Estrella and Marte also arranged for these and other funds to be loaded onto hundreds of debit cards that they opened in other people's names using stolen data, and had the cards mailed to their homes and to the homes of their family members.

Estrella and Marte obtained this data from multiple sources, including a hospital in the Bronx where Estrella worked as a business clerk for almost a decade.

In 2020, Estrella was terminated from that role after an internal systems audit revealed that he had improperly accessed the protected health information of at least 4,005 hospital patients. (Source)

Hospital Pharmacist Spied On Coworkers For 10+ Years By Installing Keylogging Software On 400 Laptops And Workstations - April 8, 2025

The University of Maryland Medical Center is facing a class action lawsuit that alleges one of its pharmacists installed keylogging software on 400 laptops and workstations over a decade to spy on the personal lives and intimate moments of at least 80 coworkers.

Attorneys say UMMC pharmacist Matthew Bathula used the stolen credentials to access personal information and secretly record coworkers in their homes and throughout the workplace, according to a lawsuit filed in a Baltimore court. The university said the pharmacist was fired and is under a criminal investigation by federal law enforcement.

Attorneys representing the plaintiffs allege that Bathula installed keylogging software on hundreds of computers and workstations in clinics, treatment rooms, labs and a variety of other locations throughout the academic medical institution's campus.

Bathula then obtained coworkers' usernames and passwords for their personal accounts, including bank accounts, email, home surveillance systems, Dropbox accounts, Google Drives, dating applications, Google Nest and iCloud accounts.

Bathula captured and retained lists of Medical Center employees' login credentials. He used that information to then access the personal accounts of his coworkers, the lawsuit alleges. Once inside those accounts, he downloaded and retained Medical Center employees' private photographs, videos and personally identifying information.

He also surveilled Medical Center employees in real time in the privacy of their own homes and captured and recorded private and intimate moments with their spouses and families," the lawsuit alleges.

Bathula also allegedly used these login credentials to gain remote access to webcams to record videos of young doctors and medical residents in private moments at work, such as when UMMC coworkers who were new mothers pumped breast milk in closed treatment rooms."

It is pretty obvious that security controls involving LEAST PRIVILEGE and other security controls were not implemented. (Source)

Hospital Worker Installed Secret Cameras In Bathrooms - June 6, 2025

A former worker (Sanjai Syamaprasad) at a New York hospital's sleep disorders center has been indicted on criminal charges alleging he installed a hidden camera in the facility's bathrooms to record videos of staff and patients. The hospital has reported the incident to federal regulators as a HIPAA breach affecting thousands.

While only five victims - including one child - have been identified in the recordings so far, North Shore University Hospital's Sleep Disorders Center reported the incident in May to federal regulators as a HIPAA breach affecting 13,332 individuals and involving "unauthorized access/disclosure.

Syamaprasad installed the hidden cameras inside fake smoke detectors in multiple bathrooms of the sleep center and public bathrooms of the healthcare facility in Great Neck, Long Island, New York, between July 2023 and April 2024 and that he destroyed evidence of the recordings.

Prosecutors say Syamaprasad used a Velcro patch to attach a fake smoker detector with a hidden camera onto the walls of multiple staff and patient bathrooms at the sleep center and in public bathrooms of the rehab center.

At the end of his shifts, Syamaprasad allegedly removed the phony smoke detector and downloaded the camera footage onto an SD card. (Source)

Supervisor At Hospital Arrested After Hidden Cameras Found In Restrooms - August 27, 2025

Robert Shrader is a A former employee of Memorial Hermann Medical Center in Texas. Shrader is charged with invasive visual recording, which is a state felony. He was recently fired after multiple hidden cameras were found in both staff and public restrooms.

While performing routine maintenance, the construction team discovered a recording device that had been installed in the staff, single-stall, unisex bathroom. The wireless video camera was hidden in an HVAC system.

A security manager checked a micro SD card and discovered video of a man he recognized as Shrader installing the camera.

The card also contained 175 images of people using the restroom, unaware they were being recorded. On August 25, a second hidden camera was discovered, this time in a public bathroom. It contained 131 images. (Source)

Dental Office Employee Arrested For Stealing $29,000 - August 13, 2025

Felicia Waycaster worked for Great Expression Dental. She had been employed by the dentist office for about a year.

The dental office reported the alleged thefts to the police department in early June of this year. It was determined that the former employee, Waycaster, had been taking money from around the beginning of January of 2025 until early June. Waycaster used various methods to steal just over $29,000 from the business. It appears that there were multiple payments through cash (by customers.) Those payments were never made to the company. Waycaster took those payments. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

14 Huawei Employees Sentenced To Prison For Trade Secret Theft To Form New Startup Company - August 5, 2025

China's courts take tech secret pilfering seriously, if one of its homegrown companies appears to be the victim. A Shanghai court has sentenced 14 former Huawei employees, who were accused of taking a number of "chip-related business secrets" with them, when they scooted off to form a new startup called Zunpai Communication Technology. Sources indicate that the ex-Huawei engineers will face financial penalties and up to six years in jail.

The above case is reportedly a talking point in China. The topic of Intellectual property theft, its impacts on competitive industry, and on the people who work at these companies, have been thrust into the public psyche. However, the plaintiff in this case, Huawei, has yet to comment.

Zunpai was founded in 2021 by Zhang Kun, a former researcher at HiSilicon. Zhang had left Huawei in 2019, and in the interim, apparently headhunted talent from his old employer, with some success.

It is alleged that Zhang managed to attract some of his old colleagues over to Zunpai with high salaries and attractive stock options. But there's no such thing as a free lunch, and these potential employees were also reportedly expected to copy secrets before they quit Huawei.

Huawei initiated legal proceedings in August 2023. Shortly after this, in December 2023, Shanghai police arrested 14 individuals for activities infringing upon chip technology secrets. At the same time, 95 million Chinese yuan ($13.1 million) worth of Zunpai's assets were frozen.

Investigations by law enforcement indicated that 40 technologies in use by Zunpai were almost identical to those owned by Huawei / HiSilicon. (Source)

Intel Employee Sentenced To Probation And Fined $34,472 For Stealing Thousands Of Files / Trade Secrets To Secure Position At Microsoft - August 16, 2025

An ex-Intel employee has been sentenced to two years' probation and fined $34,472 for pilfering "thousands of files," which were reportedly instrumental to him landing a new position at Microsoft.

Varun Gupta was an Intel employee for 10 years, working as a product marketing engineer. He departed Intel in January 2020, moving directly to Microsoft. Gupta spent a lot of time copying files containing trade secrets shortly before leaving his employment at Intels Santa Clara headquartes.

These trade secrets were reportedly instrumental to Gupta securing his new position at Microsoft. Moreover, they were subsequently used for the benefit of Microsoft in processor purchasing negotiations with Intel. A particular PowerPoint document was referenced in the court records, indicating that the presentation slide(s) charted Intel's pricing strategy, as drafted for another major customer.

Gupta was ordered to pay the fine in full before heading back to France. The ex-tech exec and his family have started afresh in La Belle France, with eyes on a completely new career in the wine industry.

According to the report, Gupta is now studying for a qualification in vineyard management, while aiming to work as a technical director in the business. (Source)

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

University Of Texas MD Anderson Cancer Center Employee Charged With Stealing 90GB Of U.S. Funded Research And Taking It To China - August 26, 2025

A post-doctoral researcher at the University of Texas MD Anderson Cancer Center is accused of stealing research funded by the U.S. government and attempting to take it back to his native China.

Charging documents state Dr. Yunhai Li joined MD Anderson through a U.S. Department of State research exchange scholar visa in 2022. His employment made him an employee of the State of Texas.

Li was working at MD Anderson on a vaccine to prevent breast cancer from metastasizing. When the project was approximately 70% finished, Li toke up to 90 GB of research. When confronted by hospital officials, Li said he worked to convince them that he had permanently deleted the material while concealing it through a China-based cloud company.

Li had also retained his employment at a Chinese state-affiliated hospital while working at MD Anderson. (Source)

In-Depth Analysis Provides Insights Into The North Korea Fraudulent IT Workers Scheme That Has Infiltrated Many U.S. Companies – August 5, 2025

Law enforcement 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 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)

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

Construction Company Financial Controller Charged With Stealing $8 Million+ - August 15, 2025

Monterey County, was the controller of Company A, a civil contracting construction company headquartered in Salinas, California.

Beginning around October 2021 until November 2023, Dodson allegedly conducted approximately 136 unauthorized wire transfers from Company A's business account to her personal bank accounts that she falsely characterized as payments for materials for the company.

The information alleges that Dodson used a variety of means to conceal the unauthorized transfers to avoid detection and facilitate future transfers, including by intercepting and destroying paper bank statements sent by Company A's bank documenting the unauthorized wire transfers.

Dodson also allegedly downloaded Company A's bank statements, modified the electronic bank statements by removing her name from wire transfer descriptions, and saved the altered bank statements in Company A's records. The information further alleges that Dodson concealed the unauthorized wire transfers by falsely listing them in Company A's expense accounts in the accounting journal. Dodson is alleged to have conducted unauthorized wires totaling approximately $8,579,647.48. (Source)

Employee Charged For Embezzling $1 Million+ From Employer Using Various Fraud Schemes - August 13, 2025

Christopher Septon and was trusted with authority to use company funds to pay vendors, contractors, and other third parties. Septon worked for Ellis Properties, a family-run commercial real estate business located in Minneapolis, Minnesota. Septon worked for the company from 2010 until 2024, when his embezzlement was discovered.

Septon improperly charged more than $800,000 on the company credit card, directing the payments to his own payment-processing accounts.

He hid the fact that these payments were to his own accounts by writing false statements in the transaction memo lines, misrepresenting that the transactions were business-related and with third parties, when, in fact, they were transfers to Septon.

Septon also fraudulently obtained "reimbursement" checks from the company for business expenses he claimed he had paid personally, when, in fact, he had not. He used fake invoices, fake emails, and other lies to induce company personnel to issue the unwarranted reimbursement checks.

As part of the scheme, Septon also impersonated government agencies. Without their knowledge, Septon used the names of the City of Minneapolis, the Metropolitan Council, the Minnesota Department of Agriculture, and the Minnesota Pollution Control Agency to fraudulently obtain money from Ellis Properties, falsely claiming Ellis Properties owed certain payments to those agencies and instead directing the funds to himself.

Hundreds of thousands of dollars in profits from the fraud were transferred from account to account, then retained by Septon. In total, Septon embezzled more than $1 million from Ellis Properties. (Source)

Environmental Consulting Company Employee Sentenced To Probation And Ordered To Re-Pay $123,000 Of State Funds He Stole - August 7, 2025

Alan Jones was employed by an environmental consulting company located in Chesterton, Indiana. Jones and the company were hired by gas station owners to manage and perform remediation work related to underground storage tank leaks.

The State of Indiana created a state trust fund, administered by the Indiana Department of Environmental Management, to help reimburse those remediation costs.

Jones submitted false and fraudulent applications for reimbursement of costs that were not actually incurred and caused state funds to be paid to the consulting company for which it, and Jones, were not entitled. (Source)

Walmart Employee Arrested For Stealing $10,000+ From Cash Register - August 20, 2025

A 51-year-old employee at a Walmart has been arrested after being accused of stealing over $10,000 from a register.

Ontario County Sheriff deputies say David Ashworth took money from a register during his shift and hid a money bag with the money inside. Deputies say he then took the money at the end of his shift and left the store. (Source)

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

Company Executive Director Pleads Guilty To Embezzling $1.5 Million from Employer / Used Funds For Travel, Gambling, Etc. - August 27, 2025

Justin Marquardt admitted that he stole approximately $1.5 million from his employer's bank accounts and used those funds for his personal benefit.

Marquardt held the title of executive director at his company and by virtue of his position, had access to all company finances and financial accounts from 1994 to 2023. As part of his scheme, Marquardt, without authorization, transferred funds from his employer's bank accounts to his personal accounts and wrote himself unauthorized checks from business bank accounts.

Marquardt spent most of the money on personal expenses, including travel and gambling online and at casinos. To hide his embezzlement, Marquardt omitted these unauthorized transactions from the business's QuickBooks ledger that he provided to an accountant and tax preparer. Marquardt also recorded false and fraudulent payments as business expenses in the QuickBooks records to conceal his embezzlement. (Source)

Company Business Manager Sentenced To Prison For Embezzling $612,000 By Requesting Reimbursements For Fictious Business Expenses - August 27, 2025

Jeremy Ubben admitted that he embezzled $612,000 from his law firm employer between March 2023 and Aug. 2024.

Ubben was employed as the firm's business manager and had full administrator rights to the firm's online payroll processing program. Beginning in March 2023, Ubben submitted and approved for himself reimbursement requests for fictious business expense expenditures totaling tens of thousands of dollars. Ubben also admitted that he laundered proceeds from his theft through his TD Ameritrade brokerage account. (Source)

Chief Financial Officer For Staffing Firm Sentenced To Prison For Embezzling $510,000+ / Used Funds For Travel, Jewelry, Gold & Renovations To His Personal Residence - August 20, 2025
Charles Nelson misappropriated the money in 2018 and 2019 while working in the firm's Chicago office as the Chief Financial Officer.

Nelson made a series of unauthorized credit card purchases for his personal benefit, initially on meals and travel and later on jewelry, gold, and renovations of his personal residence. Nelson used the fraud proceeds to purchase many extravagant items, including Cartier and Rolex watches, a gold and diamond bracelet, and high-end appliances for his home. Nelson executed the fraud scheme by circumventing multiple corporate controls over expenditures. (Source)

Employee Sentenced To Prison For Embezzling $500,000+ From 2 Companies He Worked For / Used Funds For Friends & Acquaintances - August 14, 2025
Scott Foster was sentenced to prison for embezzling a total of $501,000 from two companies he worked for.

Foster was ordered to repay $306,199 to the St. Louis County company where he worked as a mid-level executive in human resources. Foster pleaded guilty in February to one count of wire fraud and admitted manipulating the human resources systems to create an employee account for his paramour.

Foster triggered wages and benefits totaling more than $273,000 to be paid to his paramour over nearly five years, until Foster was terminated in December 2022. He also used a corporate American Express card to pay for more than $33,000 in personal travel for himself, his paramour and other friends and acquaintances.

After Foster's guilty plea, the U.S. Attorney's Office was contacted by a non-profit children's hospital where Foster had been working since June 2023. After learning about the embezzlement from the St. Louis County company, they investigated and discovered Foster had fraudulently used hospital credit cards for unauthorized personal expenses and travel, the memo says.

Foster, who had received a $20,000 relocation bonus to move to the area of the hospital after being hired, instead stayed in Charlotte and used the hospital credit cards to pay for airfare and lodging to commute to his job. He also used these credit cards for personal travel, and to pay for first-class air travel to St. Louis and a hotel stay. Foster's embezzlement from the hospital did not stop even after he learned he was being investigated for the embezzlement from his first employer. Foster was ordered to pay $194,855 to the hospital. (Source)

Law Firm Office Manager Pleads Guilty To Embezzling $400,000+ Over 4 Year Period / Used Funds For Personal Enjoyment & Lifestyle- August 18, 2025
Todd Chapman was employed as the firm's office manager for approximately 30 years until April 2022. During this time, Chapman was authorized to write checks from the firm's bank accounts for legitimate business expenses.

From approximately 2016 through approximately 2022, Chapman personally enriched himself by writing unauthorized checks from the law firm's accounts and client trust accounts to himself. As part of his guilty plea, Chapman admitted that he carried out his scheme by using the trust he gained from his 30-year tenure with the firm to obtain complete and exclusive control of its day-to-day finances. To conceal or disguise the embezzlement, Chapman funneled money he stole from clients through the firm's operating accounts, forged signatures on checks, created false documents, made false statements under oath in civil lawsuits by former firm clients, and made false statements to federal law enforcement agents investigating the loss of client funds at the firm.

Chapman embezzled at least $409,000 from the estates of three deceased firm clients, $100,000 that one minor client was supposed to receive upon turning 18, and $15,838.84 of an initial $20,000 settlement deposit for another minor client who suffered an injury as an infant. Chapman also embezzled $13,686.21 from a $20,375 PPP loan that the firm legitimately received to provide emergency financial aid during the COVID-19 pandemic. Chapman admitted that he spent the embezzled funds for his personal enjoyment and lifestyle. (Source)

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

County Employee Charged With Stealing $150,000+ To Support His Own Company - August 14, 2025

A former employee of the Palatka Housing Authority (PHA) in Florida, an independent government organization that helps build and create affordable housing options for those in need, is being charged with funneling more than $150,000 of federal funds provided to the organization into his own company.

Thomas Hoffman, who worked at the PHA as a network administrator and payroll administrator, according to a LinkedIn profile, is accused of committing the fraud beginning at least in July 2023 and continuing through February 2025.

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

Company Software Developer Sentenced To Prison For Sabotaging Network After Being Placed On Leave / Impacting 1000+ Employees Globally - August 21, 2025

In March 2025, a jury convicted Davis Lu, 55, of causing intentional damage to protected computers. Lu was employed as a software developer for the victim company headquartered in Beachwood, Ohio, from November 2007 to October 2019.

Following a 2018 corporate realignment that reduced his responsibilities and system access, Lu began sabotaging his employer's systems. By Aug. 4, 2019, he introduced malicious code that caused system crashes and prevented user logins.

Specifically, he created "infinite loops" (in this case, code designed to exhaust Java threads by repeatedly creating new threads without proper termination, resulting in server crashes or hangs), deleted coworker profile files, and implemented a "kill switch" that would lock out all users if his credentials in the company's active directory were disabled. The "kill switch" code — which Lu named "IsDLEnabledinAD", abbreviating "Is Davis Lu enabled in Active Directory" — was automatically activated when he was placed on leave and asked to surrender his laptop on Sept. 9, 2019, and impacted thousands of company users globally.

Additionally, on the day he was directed to turn in his company laptop, Lu deleted encrypted data. His internet search history revealed he had researched methods to escalate privileges, hide processes, and rapidly delete files, indicating an intent to obstruct the efforts of his co-workers to resolve the system disruptions. Lu's employer suffered hundreds of thousands of dollars in losses as a result of his actions. (Source)

Hacking Humans Report Provides Insights That Social Engineering And Targeted Impersonation Of Employees Are Making Traditional Security Strategies Obsolete - August 20, 2025

Government agencies have spent billions building digital fortresses. A new generation of threat actors, however, is circumventing those investments by exploiting the most persistent vulnerability: agency employees.

According to a new report from Scoop News Group and Proofpoint, attackers are bypassing agencies' technical defenses by targeting employees directly through sophisticated social engineering. What's causing growing concern: Agency help desks have emerged as a "high-value target."

The report, "Hacking Humans: How to Defend Against Your Biggest Cyber Risk," argues that traditional security measures are increasingly ineffective against attackers who use deception and impersonation to penetrate agency IT systems. That's prompting agency officials to adopt a "human-centric" defense strategy, acknowledging that people are now the primary battleground for protecting sensitive government data and services.

The threat is no longer limited to generic phishing emails. Attackers now conduct detailed reconnaissance on employees, using information from data breaches and social media to craft highly convincing impersonations. The report details an instance where a threat actor, posing as an oncologist, nearly tricked a help desk specialist at a health institution into resetting a caller's credentials. The attempt failed because the specialist was savvy enough to sense something was amiss about the call. That level of intuition, the report warns, is not scalable across an entire workforce.

Technical defenses like firewalls are still essential, but attackers are actively circumventing them. The report finds that social engineering is the dominant tactic, with 60% of data breaches involving a human exploitation. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Washington University School Of Medicine Assistant Professor Admits To Embezzling $412,000 By Stealing & Selling The Schools IT Equipment - August 27, 2025

Gary Grajales-Reyes submitted false requisition requests to Washington University (WU) School of Medicine for internal and external hard drives and graphics cards falsely claiming that the computer equipment was for his WU Medicine research laboratory.

Relying upon the false requisition requests, WU Medicine purchased the requested computer equipment from its vendor, which then shipped the computer equipment directly to Grajales-Reyes' research laboratory. WashU Medicine then paid for the computer equipment.

After Grajales-Reyes received the falsely obtained computer equipment he sold the equipment by two different methods, without the knowledge or authority of WU Medicine. He sold some of the computer equipment through his personal eBay site, and he also sold some of the computer equipment to an Amazon based third-party seller.

He used the money obtained by selling the computer equipment for his own personal expenses unrelated to the work and operations of WU Medicine, and without the knowledge or authority of WashU Medicine. Over the period of his scheme, Grajales-Reyes submitted 73 false requisition requests to WU Medicine for internal and external hard drives and graphics cards, which included approximately 761 different computer parts. , WashU Medicine and Washington University paid approximately $412,163 for the computer parts, which Grajales-Reyes then sold for money which he used for his own personal expenses, unrelated to the work and operations of WU Medicine.

Federal law enforcement seized a substantial quantity of collectible trading cards from Grajales-Reyes' laboratory. He had purchased the cards with some of the funds he obtained from selling the computer parts. (Source)

Miami Heat Basket Ball Team Security Employee Charged For Stealing $2 Million Worth Of Memorabilia And Selling - August 5. 2025

Marcos Perez is a former employee of the Miami Heat Basketball Team. He is charged with transporting and transferring stolen goods in interstate commerce.

Perez is accused of stealing millions of dollars' worth of Miami Heat game-worn jerseys and other valuable memorabilia, which he later sold to online brokers.

Perez, a 25-year retired veteran of the City of Miami Police Department, was employed as a security officer with the Miami Heat from 2016 to 2021 and later worked as an NBA security employee from 2022 to 2025.

During his tenure, Perez worked on the game-day security detail at the Kaseya Center, where he was among a limited number of trusted individuals with access to a secured equipment room.

This equipment room stored hundreds of game-worn jerseys and other memorabilia that the organization intended to display in a future Miami Heat museum.

During his employment, Perez accessed the equipment room multiple times to steal over 400 game-worn jerseys and other items, which he then sold to various online marketplaces.

Over a three-year period, Perez sold over 100 stolen items for approximately $2 million and shipped them across state lines, often for prices well below their market value. As an example, Perez sold a game-worn LeBron James Miami Heat NBA Finals jersey for approximately $100,000. That same jersey later sold at a Sotheby's auction for $3.7 million.

On April 3, law enforcement executed a search warrant at Perez's residence and seized nearly 300 additional stolen game-worn jerseys and memorabilia. The Miami Heat confirmed that these items had been stolen from their facility. (Source)

Employee Misuses Purchasing Authority To Purchase $500,000+ In Medical And Surgical Tools - August 29, 2025

In June of 2025, North Haven police in Connecticut were contacted by a local medical-surgical manufacturing facility regarding the embezzlement of medical and surgical tools valued at over $500,000.

Police identified 37-year-old Jason Sabo, of Branford, as a suspect. They say that Sabo misused his purchasing authority during his employment. After reviewing the evidence, police issued a warrant for his arrest.
Sabo was arrested and charged with larceny in the first degree, computer crimes, and tampering with physical evidence. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Hospital Nurse Sentenced To Prison For Stealing Fentanyl From 5 Hospitals And Using For Personal Use - August 8, 2025

Eric Brewer was a Florida licensed registered nurse who worked at various hospitals in the Tampa Bay, Florida area. Brewer tampered with fentanyl intended for patients by removing a portion of the controlled substance from its container, at times diluting it with another substance, and using the drug for his own personal use.

On seven occasions between June 2 and September 12, 2023, Brewer repeatedly took needles, syringes, and saline flushes from the supply room, entered the treatment room of another nurse's patient who was receiving intravenous fentanyl, and stole the patient's fentanyl by redirecting it into a Styrofoam cup.

At other times, Brewer stole fentanyl directly from a secure medication locker or started and stopped the patient's intravenous (IV) pump of fentanyl to steal it. After stealing the drugs, Brewer injected them into himself in a restroom.

Brewer's criminal conduct came to the attention of hospital administrators on September 12, 2023. Although he was not assigned to care for any patients receiving fentanyl, Brewer volunteered to change the fentanyl IV drip bag for another nurse.

Brewer acquired a 100mL fentanyl IV bag and tubing from the secured medication locker and disbursed it to the patient. Shortly thereafter, Brewer entered a restroom. When he left the restroom, nurses observed Brewer stumbling, slurring his speech, and falling asleep. An inspection of the restroom revealed a bloody needle and paper towel, which Brewer had used to inject himself with fentanyl. A hospital employee reported Brewer to a manager who requested he take a drug test. Brewer refused and was fired. Subsequent lab testing of the fentanyl IV bag he had administered that morning revealed that fentanyl had been removed from the drip bag and diluted approximately 50% with saline. (Source

Outpatient Surgical Center Nurse Who Stole Fentanyl Vials Sentenced To Prison - August 12, 2025

Kristen Carotenuto was employed as a nurse at an outpatient surgical center in Stamford, Connecticut. As part of her employment, she was granted access to a secure location used by the surgical center to store controlled substances, including hydromorphone and fentanyl.

In December 2024, Carotenuto removed several vials, each containing hydromorphone or fentanyl, from the secure storage area. She then took the vials home, removed the controlled substances using a syringe, and used the drugs. She then refilled the vials with either saline or water and returned the tampered vials to the storage area in a location where they could be distributed for patient use. There is no evidence that any patients received the tampered medications. (Source)

OTHER FORMS OF INSIDER THREATS

Airport Employee Arrested For Stalking Other Employees Using GPS Tracking Devices On Their Vehicles - August 8, 2025

Dustin Madden, an employee at an Alaska airport has been arrested for allegedly stalking fellow staff members by placing GPS tracking devices underneath their vehicles, according to the state department of transportation.

Officials said Madden's arrest follows "multiple reports" from airport staff members who "discovered GPS trackers on their personal vehicles while parked in the airport's employee parking lot."

Madden was charged with four misdemeanor counts of stalking and one felony count of tampering with evidence, but officials said "further charges may be forthcoming." Two of the stalking incidents known by officials occurred in July, with a third in 2024 and a fourth in 2022, according to court records.

The suspect had been an employee at the airport since Sept. 30, 2020, and is now on administrative leave, officials said. (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
No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'
Walmart Employees Arrested For Punching A Customer With Disabilities - August 29, 2025
Two Naugatuck Walmart employees were arrested in connection with the assault of customer who has disabilities, police said. Naugatuck police identified the suspects as 45-year-old Shelly Alam and 39-year-old Robert Mclaughlin.

"Police learned that two customers, one of them handicapped and using an electric scooter, were shopping for clothing and needed assistance," police said in their report. "One of the customers asked an employee, [Alam], for assistance. Alam responded in a manner in which a verbal altercation between the two took place and then escalated." Police said Alam also ridiculed the customer's handicap.

When the customer requested to speak with the store manager, another employee, whom police identified as Mclaughlin, approached the customer and punched the customer in the head. It resulted in minor injury.

Alam was arrested and charged with conspiracy to commit third-degree assault, risk of injury to a child, and interfering with an officer/resisting arrest.

Mclaughlin was arrested and charged with third-degree assault, risk of injury to a child, and interfering with an officer/resisting arrest. (Source)

EMPLOYEES' INVOLVED IN TERRORISM
No Incidents To Report

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

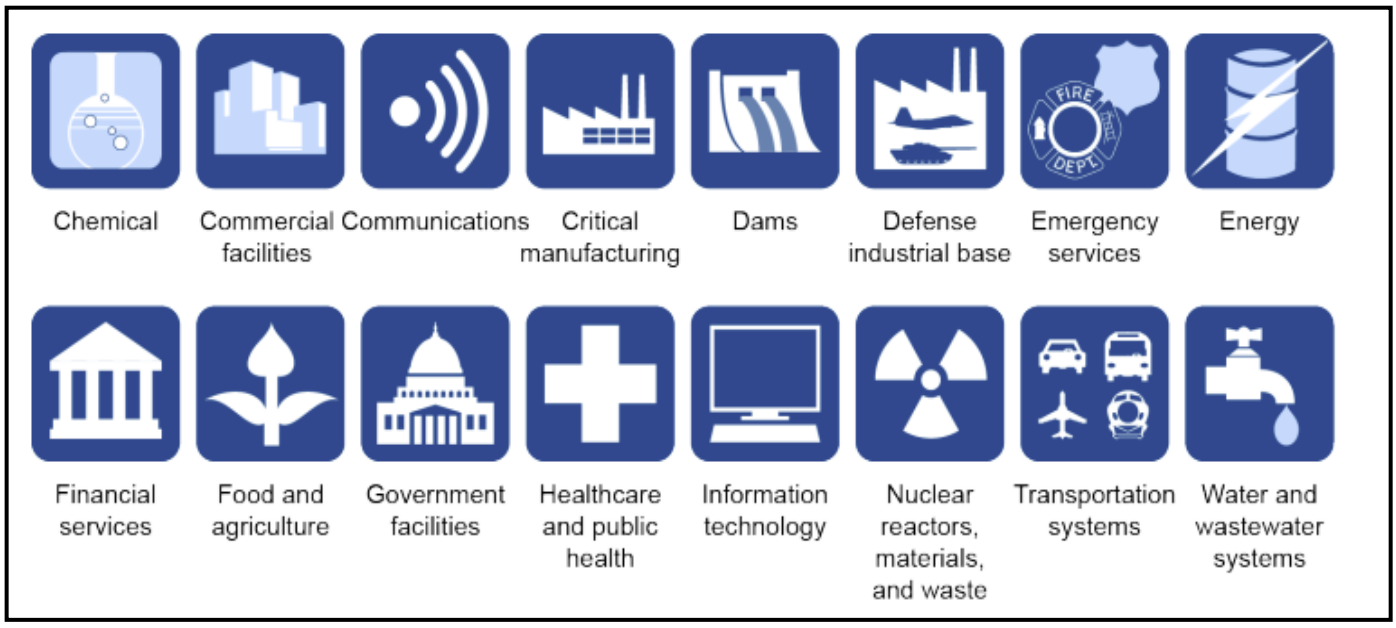
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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 ORGANIIZATIONS 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

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

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

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

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

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

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

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

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

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

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

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

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

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

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

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

Fraud In Government Organization's / Infographic

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee.

As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

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

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

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

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

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

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

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

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

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

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

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

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman.

Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

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

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

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

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

TRADE SECRET THEFT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners.

As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

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

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

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

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

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering."

The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union.

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

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

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

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

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

Former Controller Of Oil & Gas Company Sentenced To Prison For Role in $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999.

In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

EMPLOYEE EXTORTION

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

The websites listed below are updated daily and monthly with the latest incidents.
There is NO REGISTRATION required to download the reports.

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-incidents-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
Produced By:
National Insider Threat Special Interest Group (NITSIG)
Insider Threat Defense Group (ITDG

Insider Threat Fraudulent Invoices & Shell Schemes Report / August 2025
Pages 6 to 24 of this report will highlight employees that are involved in **1)** Creating fraudulent invoices (For Products, Services And Vendors That Don't Exist) **2)** Manipulating legitimate invoices **3)** Working with external co-conspirators / vendors to create fraudulent or manipulated invoices.

These fraudulent invoices will then be submitted to the employer for payments to a shell company created by the employee, who will receive payment to a shell company bank account or through other methods. These fraudulent invoices schemes may happen just once or become reoccurring.

Employees may also collaborate with other employees, vendors or third parties to approve fraudulent invoices in exchange for kickbacks. An accounts payable employee might work with a vendor to create fraudulent invoices, and then the employee ensures the invoices are approved. Then the employee and vendor share the proceeds after the payment is issued.

These schemes can be disguised as legitimate business transactions, making them difficult to detect without proper internal controls. A shell company often consists of little more than a post office box and a bank account.

These schemes are often perpetrated by an opportunist employee, whose primarily focuses is for their own self-interest. They take advantage of opportunities (Lack Of Controls, Vulnerabilities) within an organization, often with little regard for the ethics, consequences or impacts to their employers. They are driven by a desire to maximize their personal financial gain.

From small companies to Fortune 500 companies, this report will provide a snapshot of fraudulent invoicing and shell companies schemes that are quite common.

This report and other monthly reports produced by the NITSIG provide clear and indisputable evidence that Insider Threats is not just as a data security, employee monitoring, technical, cyber security, counterintelligence or investigations problem. Download Report

Why Insider Threats Remain An Unresolved Cybersecurity Challenge
Produced By: IntroSecurity: NITSIG - ITDG / 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/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

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

NITSIG Overview

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

NITSIG Membership

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

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

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

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

NITSIG IRM Resources

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

NITSIG LinkedIn Group

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

NITSIG Advisory Board

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

https://www.nationalinsiderthreatsig.org/aboutnitsig.html

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
561-809-6800
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

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 With Legal Guidance From Attorney
- ✓ 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.

Even our most experienced students that have attend our training courses, or taken other IRM Program training courses and paid substantially more, state that they are amazed at the depth of the training content and the resources provided, and are very happy they took the training and learned some new concepts and techniques for IRM.

Our client satisfaction levels are in the **EXCEPTIONA**L 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 700+ Clients:

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

Additional Background Information On ITDG

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

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

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

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Risk Management Program Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG