INSIDER THREAT INCIDENTS REPORT
FOR
June 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

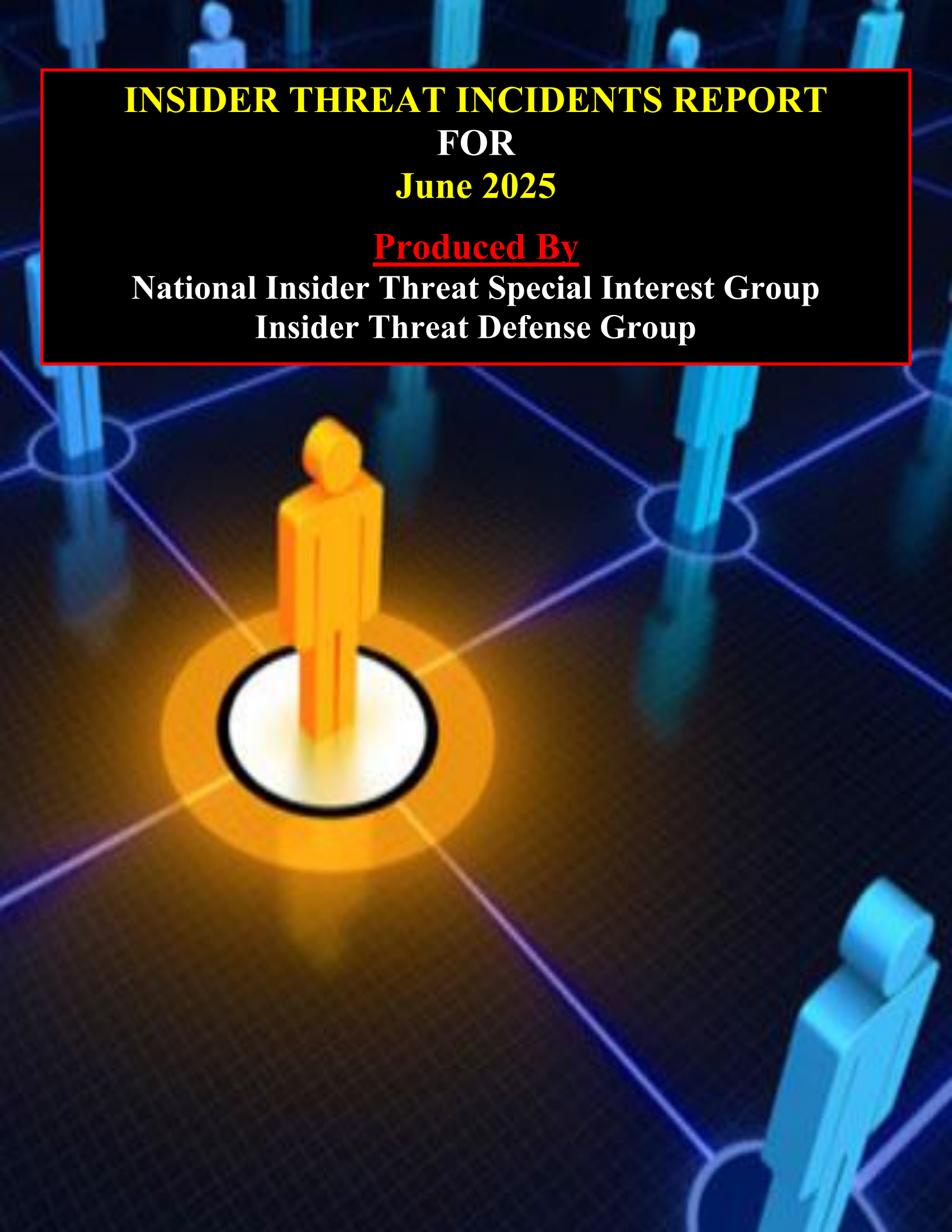

TABLE OF CONTENTS

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 **6,400+** 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 29** 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 JUNE 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Defense Contractor Arrested For Leaking India Naval Secrets To Suspected Pakistani Spies - June 1, 2025

A 27 year old junior defensce contractor has been arrested for allegedly leaking restricted information on India Navy warships and submarines to suspected Pakistani intelligence agents, Maharashtra's Anti-Terrorism Squad (ATS) said in a statement issued late Saturday.

Identified as Ravindrlidhar Verma, the accused was working in the electrical department of Mumbai based Muraed Krasni Defence Technology Pvt. Ltd., which handles sensitive repair operations for key defense establishments including the Naval Dockyard, Mazagon Dock Shipbuilders Ltd., and the India Coast Guard. His role granted him access to several restricted naval installations across Maharashtra.

Verma was arrested on Wednesday by the Thane unit of the ATS after investigators found he had shared operational details about 14 naval vessels, including warships and submarines. (Source)

Employee Sold His Login Credentials To Individual On Chat Platform That Resulted In Data Breach Affecting 72,000 Victims - June 15, 2025

A large-scale trial is opening after the discovery of a major data leak at a French work agency Adecco that left 72,000 victims in one of the most serious data-related frauds ever uncovered in France. 16 people are in are facing 22 charges including organized fraud and identity theft.

The central figure is a 20-year-old described by investigators as having "exceptionally high intellectual capacities" and a compulsive drive to find and exploit digital loopholes.

The case centers on the breach of the Adecco temporary work agency's internal systems. In 2022, a 19-year-old intern at an agency in Besançon, Doubs, sold his login credentials to a contact on an encrypted chat platform. He purportedly did not receive the €15,000 he had been promised for the login details and was arrested shortly afterwards.

The access allowed hackers to extract data on around eight million job seekers, including banking details. Using the stolen Adecco data, the group began issuing automated withdrawals of €49.85 from thousands of bank accounts - just below the €50 threshold that typically triggers fraud detection alerts. The small, repeated, sums went unnoticed for weeks. In total, nearly 33,000 people were debited without their consent, generating a confirmed loss of €1.6million. A further 40,000 attempts were blocked or later refunded. Banks involved have joined the trial as civil parties, having reimbursed around €1.4million.

The Adecco data breach also allowed the creation of fake ID cards and social security documents used to open 'mule' bank accounts for laundering the stolen funds. (Source)

U.S. GOVERNMENT

USAID Official And 3 Corporate Executives Plead Guilty To 10 Year Bribery Scheme Involving $550 Million+ In Contracts Using Shell Companies & Fraudulent Invoices - June 12, 2025

4 men, including a government contracting officer for the United States Agency for International Development (USAID), and 3 owners and presidents of companies, have pleaded guilty for their roles in 10 year long bribery scheme involving at least 14 prime contracts worth more than $550 million in U.S. taxpayer dollars.

Roderick Watson, who worked as a USAID contracting officer, pled guilty to bribery of a public official. Other individuals involved: Walter Barnes, Darryl Britt, Paul Young.

Beginning in 2013, Watson, while a USAID contracting officer, agreed with Britt to receive bribes in exchange for using Watson's influence to award contracts to Apprio. As a certified small business under the SBA 8(a) contracting program, which helps socially and economically disadvantaged businesses, Apprio could access lucrative federal contracting opportunities through set-asides and sole-source contracts exclusively available to eligible contractors without a competitive bid process.

Vistant was a subcontractor to Apprio on one of the contracts awarded through Watson's influence. After Apprio graduated from the SBA 8(a) program and it was no longer eligible to be a prime contractor for new contracts with USAID under this program, the scheme shifted so that Vistant became the prime contractor and Apprio became the subcontractor on USAID contracts awarded through Watson's influence between 2018 and 2022.

During the scheme, Britt and Barnes paid bribes to Watson that were often concealed by passing them through Young, who was the president of another subcontractor to Apprio and Vistant. Britt and Barnes also regularly funneled bribes to Watson, including cash, laptops, thousands of dollars in tickets to a suite at an NBA game, a country club wedding, downpayments on two residential mortgages, cellular phones, and jobs for relatives. The bribes were also often concealed through electronic bank transfers falsely listing Watson on payroll, incorporated shell companies, and false invoices. Watson is alleged to have received bribes valued at more than approximately $1 million as part of the scheme. (Source)

4 Individuals, Including 2 U.S. Postal Service Employees Charged For Stealing $80 Million+ In U.S. Treasury Checks - June 11, 2025

The individuals involved: Tauheed Tucker, Cory Scott, Alexander Telewoda, Saahir Irby., between June 2023 and September 2024.

Irby and Tucker, worked at as USPS as mail processing clerks. They stole thousands of envelopes containing U.S. Treasury checks from mail sorting machines at the USPS Philadelphia Processing and Distribution Center.

Irby and Tucker removed the checks from the USPS facility and sold them to defendants Scott and Telewoda, who then advertised the stolen checks for resale on the cloud-based instant messaging application Telegram. Upon receiving payment from interested buyers, Scott and Telewoda mailed the stolen Treasury checks to buyers around the country who attempted to cash the checks, without the knowledge or permission of the individuals to whom the checks had originally been issued.

Over the course of the scheme Irby and Tucker sold Scott and Telewoda thousands of stolen Treasury checks whose face value exceeded $80 million. Scott's and Telewoda's customers successfully negotiated approximately $11 million worth of these stolen Treasury checks at financial institutions. Irby is also charged with a separate instance of mail theft involving another batch of Treasury checks that he allegedly stole and sold to an unnamed individual in August 2024. (Source)

U.S. Postal Service Employee Sentenced To Prison For Role Stealing $18,000+ Of Postal Money Orders / Involved Boyfriend & Family Member - June 23, 2025

Christine Hedges began working for USPS around 2020 and worked for the last year of her tenure as a Lead Sales & Service Associate in Brockton.

From approximately October 2021 to August 2023, Hedges engaged in a scheme to steal USPS funds for her personal use. As part of this scheme, Hedges generated, for her own use, no-fee money orders without a customer physically present at her customer window and which a customer did not request. Hedges also stole cash from her USPS workstation and often attempted to conceal her theft by replacing the cash with the fraudulent money orders. During the relevant period, Hedges generated approximately 64 fraudulent no-fee money orders. Of those no-fee money orders, 11 were made out to her boyfriend or a family member. From on or about Aug. 1, 2023 to on or about Aug. 14, 2023, video surveillance from above Hedges' workstation showed Hedges on at least one occasion removing cash from her assigned drawer and putting it in her pocket. In all, Hedges stole approximately $18,939 in postal funds. (Source)

U.S. Postal Carrier Admits To Stealing $4,900+ U.S. Treasury Check From Mail / Used Funds For Personal Use - June 17, 2025

In 2021, Ernesto Rodriguez, while employed by the U.S. Postal Service as a mail carrier in Glastonbury, Connecticut, was asked by an acquaintance to intercept federal tax refund checks that would be mailed to addresses on his mail carrier route. After taking the checks, he would deliver them to an unknown individual in New York and be paid approximately $100 for each check. Rodriguez gave his acquaintance information about his route so that refund checks could be sent to those addresses, and was subsequently provided with approximately 10 names and addresses for checks he was supposed to take from the mail.

In October 2021, Rodriguez stole a U.S. Treasury tax refund check in the amount of $4,943.17 from the mail before it was delivered to an address on his route. On October 23, 2021, he deposited the check into his wife's bank account. On October 25, 2021, he transferred $4,500 from his wife's account to his own bank account, and subsequently spent the money for personal use.

Rodriguez resigned from the U.S. Postal Service on October 23, 2021. He told law enforcement that he only stole one check as part of this scheme. (Source)

Small Business Administration Employee Sentenced To Prison For $1 Million COVID 19 Fraud Scheme - June 17, 2025

Malaina Chapman was employed as a Disaster Relief Specialist with the Small Business Administration (SBA) from September 28, 2020 through March 18, 2021.

While employed by the SBA, Chapman became involved in multiple schemes to defraud the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan program, as well as local credit unions and local and state programs designed to assist those affected by the COVID-19 pandemic.

On February 10, 2021, Chapman submitted an online loan application in the name of Upscale Credit Lounge, LLC to a lender. In support of her application, Chapman submitted a false and fraudulent Schedule C (Form 1040) that reported gross revenues of $103,674 and a tentative profit of $81,860 for 2020. The lender relied upon the representations in Chapman's application to approve a loan in the amount of $17,052.50.

On February 19, 2021, Chapman submitted an online PPP loan application with the lender on behalf of DA TRAP, LLC.

In her application, Chapman claimed that she had four employees and an average monthly payroll of $14,191. In support of her application, Chapman submitted a false and fraudulent Employers Quarterly Tax Return (Form 941), which purportedly documented the wages paid by DA TRAP. Relying on the representations in the application, the lender approved a loan in the amount of $35,477.50.

In total, Chapman received $230,246 for the loan applications she submitted on her own behalf. Chapman also conspired with others to submit false and fraudulent PPP loan applications on their behalf. Six defendants were charged under case number 24-cr-20079. For that conspiracy, Chapman was held accountable for losses of $837,716. (Source)

U.S. Government Employee Who Teleworked Pleads Guilty To $225,000+ Of Fraudulent Time Reporting While Working Other Jobs - June 26, 2025

Between October 2021 and May 2025, Crissy Baker worked as a management and program analyst for the U.S. Department of Housing and Urban Development (HUD).

From October 2021 through July 2024, Baker held multiple full-time government contractor positions to perform human resources services for other federal agencies but did not seek approval from HUD to engage in this outside employment. Through this years-long scheme, Baker billed the government more than 24 hours in a single day between her employment with the federal government and contractors. The estimated loss to the government was $225,866. (Source)

Baker teleworked in all three positions, so she was able to conceal her employment with HUD and the two contarctors from each other. (Source)

Social Security Employee Pleads Guilty To Stealing $110,000+ For 28 Beneficiaries - June 27, 2025

Between January 2023 to May 2024, Christina Daniels used her position at the Social Security Administration office in Norcross, Georgia, to change the direct deposit information for approximately 28 beneficiaries. As a customer service representative, Daniels was able to make changes to beneficiaries' direct deposit information. Daniels abused this authority to steal more than $110,000.

She accomplished her theft by first opening Green Dot and Cash App accounts using personally identifiable information belonging to unwitting Social Security beneficiaries. After she created the new accounts, she changed the direct deposit information of the unsuspecting beneficiaries to one of the newly opened Green Dot or Cash App accounts that she controlled.

An internal investigation was launched after several retirement beneficiaries reported that they had not received their monthly benefit payments. Subsequent internal and law enforcement investigations revealed that Daniels had changed the direct deposit information for approximately 28 beneficiaries and that she redirected the benefits to accounts that she opened using the stolen PII of other beneficiaries – some of whom were her family members. (Source)

Federal Communications Commission Employee Arrested For Assault And Sexual Battery Attacks At Metro Rail Stations - June 3, 2025

Police have arrested a man in connection with two separate Metrorail station attacks that took place on Friday, May 30. Jeff Gary, 35, is being held without bond on multiple felony charges.

Gary was working at the Federal Communications Commission (FCC) as an assistant division chief. Upon hearing of the incident the FCC terminated Gary.

Investigators confirmed that Gary is the suspect in the two separate attacks on women. One took place at the Potomac Yard Metro Station, and the other near the Braddock Metro Station.

At the Potomac Yard Metro Station attack, the victim was on the upper level of the platform with her young daughter. She told police a man approached her, wrapped her up with his arms, pushed her up against the glass and started touching her. She said her daughter took her juice box and started pouring it on the man attacking her. The victim told police the man didn't leave until another adult walked up.

About an hour later, around 9:40 p.m., a woman in her mid-30s was walking in the 1100 block of Madison St. after leaving the Braddock Metro Station. She was approached from behind by a man who grabbed her and wrestled her to the ground. She resisted, shoved the suspect away, and ran to safety before calling 911.

Gary currently faces charges for assault and battery, sexual battery, and two counts of abduction with force. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former CIA Analyst Sentenced To Prison For Posting Top Secret SCI Classified Information On Social Media Platforms - June 11, 2025

Asif Rahman was an employee of the CIA since 2016, and had a Top Secret security clearance with access to Sensitive Compartmented Information (SCI).

Rahman provided the classified information to people who were not entitled to receive it, information which he posted on a social media platforms in October 2024.

On Oct. 17, 2024, Rahman accessed and printed two Top Secret documents containing National Defense Information regarding a U.S. foreign ally and its planned actions against a foreign adversary. Rahman removed the documents, photographed them, and transmitted them to individuals he knew were not entitled to receive them. By Oct. 18, 2024, the documents appeared publicly on multiple social media platforms, complete with the classification markings.

After Oct. 17, 2024, Rahman deleted and edited journal entries and written work product on his personal electronic devices to conceal his personal opinions on U.S. policy and drafted entries to construct a false narrative regarding his activity. Rahman also destroyed multiple electronic devices, including a personal mobile device and an internet router he used to transmit classified information and photographs of classified documents, and discarded the destroyed devices in public trash receptacles in an effort to thwart potential investigations into him and his unlawful conduct.

Beginning in the spring of 2024 and continuing through November 2024, Rahman repeatedly accessed and printed classified National Defense Information, including documents classified up to the Top Secret level, to take them to his residence.

There, Rahman reproduced the documents and, while doing so, altered them in an effort to conceal their source and his activity. Rahman then communicated Top Secret information that he learned in the course of his employment to multiple individuals he knew were not entitled to receive it. (Source)

Department Of Defense Employee Charged With Unlawful Retention Of Classified Documents By Putting In Backback And Walking Out Of Facility - June 24, 2025

Ewa Maria Ciszak, a civilian employee of the U.S. Department of Defense (DoD) was arrested for the unauthorized removal and retention of classified documents. Ciszak has been employed at the Missile Defense Agency (MDA) since January 2023.

As part of her duties, she held a security clearance and had access to classified materials related to the national defense of the United States. Beginning in approximately February 2025, and continuing through June 18, 2025, Ciszak allegedly removed classified documents from MDA facilities without authorization and transported them to her personal residence and vehicle, which were not authorized for classified material storage.

On June 18, 2025, pursuant to a search warrant authorized by the U.S. District Court, federal agents executed a search of Ciszak's home, person, and vehicle. Agents recovered multiple documents bearing classification markings up to the SECRET level. Some of the documents had been placed in her personal backpack that day and transported directly from MDA to her home. (Source)

Department Of Defense Employee Sentenced To Prison For Unauthorized Removal & Retention Of Classified Information - June 17, 2025

Gokhan Gun was a civilian electrical engineer for the Department of Defense. He has pleaded guilty to unauthorized removal and retention of classified material.

Gun, 51, of Falls Church, Virginia, was born in Istanbul, Turkey, and is a dual citizen of Turkey and the United States. Through his employment, Gun possessed a Top Secret security clearance with access to Sensitive Compartmented Information (SCI) and received training on the proper handling and storage of classified information.

Beginning in May 2024, Gun, without permission, removed at least five classified documents from his Department of Defense workspace with the intent to retain them at his primary residence, which was not an approved facility for the storage of classified information.

On Aug. 9, 2024, Gun was scheduled to depart the United States on a morning flight to Mexico. However, FBI agents observed a ride share service arrive at the defendant's residence and approached Gun.

Agents observed inside Gun's residence a backpack inside which they located a Top Secret document and a notebook with handwritten notes that mirrored a Top Secret report. In the dining room, agents located additional classified documents, one of which Gun printed on Aug. 7, 2024, just two days before his scheduled departure. (Source)

U.S. Army Sergeant Pleads Guilty To Attempting To Share Classified information With China After Leaving Army Because He Still Retained His Access -June 18, 2025

Joseph Schmidt was an active-duty soldier from January 2015 to January 2020. His primary assignment was at Joint Base Lewis-McChord (JBLM) in western Washington in the 109th Military Intelligence Battalion. In his role, Schmidt had access to SECRET and TOP SECRET information. After his separation from the military, Schmidt reached out to the Chinese Consulate in Turkey and later, the Chinese security services via email offering national defense information.

In March 2020, Schmidt traveled to Hong Kong and continued his efforts to provide Chinese intelligence with classified information he obtained from his military service. He created multiple lengthy documents describing various "high level secrets" he was offering to the Chinese government. He retained a device that allows for access to secure military computer networks and offered the device to Chinese authorities to assist them in efforts to gain access to such networks.

Schmidt remained in China, primarily Hong Kong, until October 2023, when he flew to San Francisco. He was arrested at the airport. (Source)

Veterans Affairs Contractor Agrees To Pay $4.3 Million To Resolve Claims Of Over Billing For Products After Company Employee Raised Concerns - June 11, 2025

Omnicell, a company based in Delaware, has agreed to pay $4,366,660 to resolve claims that it fraudulently overbilled the United States Department of Veterans Affairs (VA) for medical device hardware and software.

Between January 2017 and February 2023, Omnicell held a federal contact with the VA to sell and lease products at a set price or negotiated discounted price.

When Omnicell became aware of certain pricing issues related to specific individual orders, including when federal government customers raised concerns and questions, Omnicell at times issued credits or otherwise

corrected prices charged to federal government customers. However, Omnicell did not always timely correct the known issues in its sales and pricing system in a systemic way, nor did Omnicell undertake an analysis to determine whether other federal government customers that may have been previously overcharged due to the pricing issues in order to provide those customers with refunds of overcharges.

In August 2023, a former Omnicell employee came forward with allegations of fraudulent product overcharging. This individual, known as a "Relator," filed a qui tam complaint under seal in the U.S. District Court (EDWA).

When a relator files a qui tam complaint, the False Claims Act requires the United States to investigate the allegations and elect whether to intervene and take over the action or to decline to intervene and allow the relator to go forward with the litigation on behalf of the United States. The relator is generally able to then share in any recovery.

As part of the settlement agreement, the relator will receive $785,998.80 of the settlement amount. $2,183,330 of the settlement amount has been designated as restitution, meaning that it will be returned to the VA. (Source)

U.S. Army Soldiers Sentenced To Prison For Alien Smuggling - June 18, 2025

A former U.S. Army soldier stationed at Fort Hood was sentenced to prison for aiding and abetting the transportation of illegal aliens for financial gain.

Enrique Jauregui, 26, organized a smuggling event in 2024, recruiting fellow soldiers Angel Palma, 21, and Emilio Lopez, 22. Jauregui provided Palma and Lopez with the location information to pick up illegal aliens to smuggle, supported them with encouraging messages and instructions, and intended to pay the two co-conspirators after they dropped off the illegal aliens.

On Nov. 27, 2024, Palma and Mendoza Lopez drove from Fort Hood to Presidio and picked up three illegal aliens before leading U.S. Border Patrol agents on a high-speed chase. At one point, the defendants hit a marked USBP vehicle with an agent inside, causing injuries. Palma and Lopez, along with the three illegal aliens, fled the vehicle on foot. All were apprehended except for Palma, who was located at a hotel in Odessa and eventually arrested. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Police Officers Plead Guilty To Charges For Vehicle Insurance Fraud Scheme - June 3, 2025

Between August 2018 and February 2020, Michael Owen and Jaron Taylor, who were Prince George's County (PGPD) and Anne Arundel County Policy Department officers, conspired with fellow police officers to engage in mail and wire fraud. Owen and Taylor, along with officers Candace Tyler, Conrad D'Haiti, and Davion Percy, and others, devised a scheme for insurance companies to pay out the remaining financing costs of unwanted vehicles.

Members of the conspiracy reported fictitious losses to insurers to obtain money or avoid paying off vehicles that were now worth less than the amount owed on them. The co-conspirators used their statuses as police officers to assist each other's claims by writing false police reports.

Then co-conspirators submitted fictitious police reports to insurers to validate the claim. The false police reports were intended to impede, obstruct, or influence subsequent investigations of the false insurance claims.

In August 2018, Owen and Taylor staged the theft of Taylor's Chevrolet Tahoe.

After Taylor filed a fraudulent police report, Owen and Taylor stripped the vehicle and drove it deep into the woods of a Maryland State Highway property near Largo, Maryland. Taylor then made a false claim to the United Services Automobile Association (USAA) for the loss, for which USAA paid out a total of $38,670.

Then in January 2020, Owen assisted D'Haiti in avoiding payment on the loan balance of a Jaguar XKR. In cooperation with D'Haiti and Percy, Owen devised a scheme to fake the vehicle's theft. On January 4, D'Haiti parked his Jaguar behind Marlow Heights Shopping Center where Percy worked as police chief.

D'Haiti then paid Percy $350 to arrange for another co-conspirator to tow the vehicle and extensively vandalize it for the purpose of creating a total insurance loss. Tyler subsequently filed the fictitious police report which D'Haiti used to substantiate his claim against Liberty Mutual Insurance. In February 2020, Liberty Mutual paid the Jaguar's lienholder, Navy Federal Credit Union, $17,585, on the false claim. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

County Treasurer Sentenced To Prison For Stealing $38 Million+ In County Funds By Wiring Funds To Fake Companies / Used Funds To Purchase Real Estate, Etc. - June 24, 2025

Elizabeth Gutfahr, who served as Santa Cruz County Treasurer from 2012 through 2024, embezzled and laundered approximately $38.7 million by wiring public funds from Santa Cruz County's account to accounts in the names of fake companies she had created that performed no legitimate business. Gutfahr then used the money to purchase real estate, to renovate her family ranch, to pay expenses for her cattle business, and to buy at least 20 vehicles.

Gutfahr's 10-year scheme involved approximately 187 wire transfers, which she was able to complete by undermining the two-step approval process required for transfers. Gutfahr used the token of a subordinate Santa Cruz County employee so that she could both initiate and approve the wire transfers. To cover up the scheme, Gutfahr falsified accounting records, cash reconciliation records, and reports of the County's investment accounts, thereby hiding the millions of dollars that she had stolen from Santa Cruz County. (Source)

Foreman For New York Town Sentenced To Prison For $2.4 Million Environmental Crime & Bribery Scheme - June 11, 2025

Robert Dyckman, the former Assistant General Foreman for the Town of Cortlandt, was sentenced to prison for his participation in the bribery and dumping scheme. Glenn Griffin is the owner and president of Griffin's Landscaping Corporation.

From 2018 until February 2020, Griffin and Dyckman engaged in an unauthorized dumping scheme. Dyckman gave Griffin and his employees unauthorized access to Arlo Lane, a Cortlandt facility, to dump hundreds of large truckloads of unauthorized materials such as thick concrete, cement with rebar, tiles, bricks, large rocks, and soil.

After the illegal dumping, Griffin billed and received payments from the Town of Cortlandt for removing and hauling away the very materials that Griffin had illegally dumped at Arlo Lane with Dyckman's assistance.

In exchange for access to Arlo Lane, Griffin paid Dyckman cash bribes. As part of their sentences, Griffin and Dyckman were each ordered to pay $2.4 million in restitution to their victims. (Source)

Former State Worker Pleads Guilty To Embezzling $878,000+ Of State Funds Over 4 Years - June 9, 2025

Matthew Ping began working for the Washington State Office of Administrative Hearings (OAH) in 2009. By 2017 he had been promoted to the role of Management Analyst and served as the department's credit card custodian.

Between 2019 and 2023, Ping used a sophisticated scheme to abuse his credit card access so he could embezzle funds from the state agency.

Ping hid the fraud from his employer. Ping opened accounts with payment processors and gave the accounts display names that indicated the accounts were associated with legitimate OAH business vendors.

Between 2019 and 2021, Ping secretly charged more than $330,000 to OAH credit cards as purported payments to these vendors. In fact, the money went to accounts Ping controlled. In 2021, Ping set up an account via a different payment processor and continued the fraud, stealing approximately $530,000 in additional funds from OAH. Ping also used OAH credit cards to buy $17,359 in personal items from Verizon and Walmart.

Ping also circumvented state procedures designed to detect credit card fraud. For example, OAH required that Ping's co-workers review and approve Ping's credit card transactions, but Ping would provide false or incomplete lists of transactions during that review process. After the review, Ping would add in his fraudulent charges and upload and approve payment himself without the required oversight on his fraudulent transactions.

He also took steps to manipulate the accounting data to make it more difficult to determine that he had violated protocol by uploading, reviewing, and approving his own transactions

In all Ping secretly executed 210 transactions with the phony vendors he created for a total loss to the state of $860,756. The improper charges on his state issued credit card total $17,359, bringing the total loss to the State of Washington to $878,115. (Source)

California Politician / County Supervisor Sentenced To Prison For Accepting $550,000 In Bribes Involving $10 Million+ In COVID Relief Funds - June 9, 2025

Andrew Hoang Do, a former politician who served on the Orange County Board of Supervisors, was sentenced to prison for accepting bribes for directing and voting in favor of more than $10 million in COVID-19 pandemic relief funds to a charity affiliated with one of his daughters.

From February 2015 until his resignation in October 2024, Do was one of five supervisors on the Orange County Board of Supervisors, which is responsible for the county's $9 billion annual budget.

Beginning in 2020, in exchange for more than $550,000 in bribes, Do voted in favor of and directed millions of dollars in COVID-related funds to the Viet America Society (VAS), a charity affiliated with his daughter.

Do directed and worked together with other county employees to approve contracts with – and payments to – VAS. Do further admitted he acted corruptly and abused his position of trust as a county supervisor. (Source)

City Employee Sentenced To Prison For Embezzling $430,000+ / Used Funds For Entertainmentm Gambling, Etc. - June 17, 2025

Leo Pellegrini is the former Director of Health and Human Services and Director of the Department of Environmental Services for the City of Hoboken in New Jersey.

Pellegrini embezzled money from the City of Hoboken by diverting approximately $223,500 in payments intended for the City of Hoboken to bank accounts he controlled. Pellegrini also embezzled money from the City of Hoboken by submitting approximately $234,432.60 in his personal expenses, which the City of Hoboken unknowingly paid.

Pellegrini used the embezzled funds on personal expenses including meals, entertainment, and gambling, allowing him to live far beyond his means. (Source)

Washington Metropolitan Area Transit Authority Train Operators Arrested For $360,00+ Health Care Fraud And Disability Scheme - June 16, 2025

The individuals arrested were: Michelle Shropshire, Harlisha Jones. They were arrested for health care fraud, wire fraud, mail fraud, aggravated identity theft and conspiracy charges.

From June 2021 through January 2024, Shropshire and Jones, both Train Operators employed by the Washington Metropolitan Area Transit Authority (WMATA), conspired to use Jones's insurance policies with

American Family Life Assurance Company of Columbus (AFLAC) to submit fraudulent health care and short-term disability insurance claims for injuries, medical treatments, and disability periods that did not exist.

Shropshire and Jones used the information of real doctors to create fraudulent medical excuse notes and physician's statements, including forged doctors' signatures, that were submitted to AFLAC in support of the insurance claims.

Then, shortly after AFLAC paid each claim to Jones, she paid a kickback to Shropshire using a percentage of the total claim payment. As a result of those fraudulent insurance claims, AFLAC paid Jones approximately $58,750, of which Jones paid approximately 20% back to Shropshire.

The indictment further alleges that in addition to Jones, Shropshire assisted numerous other WMATA employees with submitting fraudulent health care and short-term disability insurance claims to AFLAC.

As a result of that scheme, AFLAC paid at least $362,035.14 in phony insurance benefits to Shropshire, Jones, and other WMATA employees.

Those employees included Sharon Washington, Selethia Blake, Brady Turner, Lushawn Foreman, Margot Jackson and others.

Washington, Blake, Turner, Foreman, and Jackson have each admitted to their involvement in Shropshire's scheme, including paying kickbacks to Shropshire using a portion of the claim payments they received, and have pleaded guilty to conspiracy to commit health care fraud. (Source)

State Employee Pleads Guilty To Fraudulently Obtainingg $200,000 By Re-Directing Funds To Her Personal Bank Account - June 25, 2025

From approximately April 2020 to March 2021, Paris Haynes was employed with the Louisiana Workforce Commission (LWC) as a customer service representative. In this position, she was responsible for assisting individuals with their unemployment insurance claims.

During the course of the scheme, Haynes accessed and made changes to approximately forty (40) claimant accounts in order to redirect Pandemic Unemployment Assistance (PUA) program benefits to her own bank accounts or to accounts under her control. In total, Haynes obtained at least $200,000 in PUA benefits to which she was not entitled. (Source)

2 Department Of Motor Vehicles Employee Arrested For Selling Drivers Licenses To Illegal Immigrants / Employees Received $120,000 - June 12, 2025

8 people have been arrested after a joint investigation by the Bay County Sheriff's Office and Homeland Security Investigations in Florida, where illegal immigrants were allegedly paying to get fraudulent driver's licenses.

Investigators say suspicious driver's license transactions were occurring at the Bay County Tax Collector's Office, and 2 DMV employees were being financially compensated to provide driver's licenses to those who did not qualify for them.

"Analysis of financial records confirms that the employees were receiving large sums of currency from numerous sources," Sheriff Ford said.

Investigators say individuals were traveling from across the state, some as far as Miami, to get licenses without taking proper tests.

The 2 employees arrested where Bancelie Velazco and Demetrius Smith. Velazco has been charged with nine counts of DMV Employee Issue Unlawful DL and nine counts of Official Misconduct. Smith has been charged with eight counts of DMV Employee Issue Unlawful DL and eight counts of Official Misconduct.

Authorities seized $120,000 from the homes of the 2 employees arrested. (Source)

Maryland Property Owner Paid $10,000+ In Bribes To Baltimore City Department Of Finance Employee To Remove Debts Owed To State - June 11, 2025

James Erny was charged with paying bribes to Joseph Gillespie, a former Baltimore City Department of Finance, Revenue Collections, employee.

From about August 2021 through September 2023, Erny paid Gillespie at least $10,000 in bribes in exchange for Gillespie extinguishing various financial obligations he owed to Baltimore City. The debt was in connection with various properties Erny owned, including unpaid water bills.

Gillespie accepted these bribes — typically 10-15 percent of the amount owed to the City — in exchange for removing or extinguishing these financial obligations, including for citations, tax, and water obligations, which caused losses for the City. He also accepted bribes in exchange for delaying or postponing due dates — without approval or permission from other City officials — for payments owed to the City. By adjusting payment due dates, this prevented the City from placing liens on these properties.

Once Gillespie received bribe payments, he then extinguished the financial obligation owed by marking it as paid in the City's online records.

After removing the obligation, Gillespie sometimes sent a photograph of a cashier slip reflecting that the City received payment toward the financial obligation when, in fact, no such payment was made. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former University Employee Arrested For Threatening To Carry Out Mass Shooting And Bombing Against Children's Hospital - June 4, 2025

A former Syracuse University (SU) employee was arrested and charged with making a terroristic threat after threatening to carry out a mass shooting and bombing at Upstate Golisano Children's Hospital.

The former employee, 27 year old Adam Dedrick, admitted to the threats and false active shooting report at SU in April. Officers found no signs of physical bombs or any threat upon arrival. A SU spokesperson confirmed Dedrick is no longer employed by the university. (Source)

School Employee Arrested For Stealing $12,000+ - June 5, 2025

An investigation was launched in April regarding a former employee, identified as Kayla Jones, 33, who reportedly misappropriated approximately $12,624.92 during her employment at Central Middle School.

Deputies say an internal audit and follow-up investigation revealed that the funds were taken in separate amounts over time. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Union President Pleads Guilty To Embezzling $10,000+ / Use Funds For Bars, Restaurants, Etc. - June 26, 2025

Kyle Chasse, 38, embezzled over $10,000 in union funds between 2020 and 2022, while serving as the union's president.

Chasse withdrew cash and made debit purchases using the union's bank account, all without authorization by the union. The debit transactions included purchases from bars, restaurants, vending machines, and other businesses. Chasse made false statements to cover up his fraudulent use of the funds. These false statements included a union financial disclosure form filed with the federal government, in which Chasse misrepresented the amount of money he had received from the union. (Source)

BANKING / FINANCIAL INSTITUTIONS

Credit Union Assistant Branch Manager Sentenced To Prison For Role In $2 Million+ Loan Fraud Scheme - June 5, 2025

Eulice Alvey pleaded guilty to conspiracy to commit bank fraud. The judge ordered Alvey to pay restitution in the amount of $2,075,458.57.

On September 6, 2018, a Neches Federal Credit Union (NFCU) member contacted the credit union and reported there were loans reflected on their account that they did not request.

Shortly thereafter, another member notified the credit union that they also had loans on their account that were not theirs. This type of notification then became common over the next few weeks, involving as many as 30 members, all associated with Billy Ray Thomas, an assistant branch manager for NFCU. An investigation revealed Thomas was working with Alvey to commit bank fraud. Alvey would fabricate fraudulent purchase invoices for tractors from his business, Oil City Tractor, LLC, and send the invoices to Thomas. Thomas would then use credit union members' information to request a loan.

Once the loan was approved, Thomas would share the proceeds with Alvey and they would use the money for personal and business ventures. In April 2025, Thomas was sentenced to 34 months in federal prison. (Source)

Bank Teller Sentenced To Prison For Stealing $180,000+ From Customers Accounts - June 16, 2025

While working as a teller at a bank branch in Boston, Derek Aut stole from the bank accounts of two customers by forging the victims' names on withdrawal slips, among other things.

When one of the victims noticed money missing from her account, Aut attempted to cover his theft by taking money from the other victim's account and depositing it into the first victim's account. In total, Aut took more than $180,000 from the victims' accounts. (Source)

TD Bank Employee Pleads Guilty To Accepting Bribes To Fraudulently Open 140+ Bank Accounts - June 25, 2025

In late 2022, Jhonnatan Rodriguez began opening bank accounts for unknown individuals in exchange for bribes of approximately $200 to $250 per account. During the scheme, Rodriguez accepted bribes in exchange for fraudulently opening approximately 140 bank accounts, some of which were used for fraud.

In carrying out this bribery scheme, Rodriguez would often forge the purported customers' signatures on account opening documents. To protect his identity, Rodriguez used the alias "Jorge" on a text messaging app to communicate with the individuals seeking bank accounts. (Source)

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

Health Care Company Agrees To Settle HIPAA Violation Caused By Employee And Pay $800,000 Penalty - May 29, 2025

The Florida healthcare provider, BayCare Health System, agreed to settle the HIPAA violation case and paid a $800,000 financial penalty. BayCare Health will adopt a corrective action plan and be monitored by Health & Human Services' Office for Civil Rights (OCR).

An investigation was launched in response to an October 2018 complaint from a patient about unauthorized access to her printed and electronic medical record following a visit to BayCare Health's St. Joseph Hospital in Tampa, Florida. After receiving treatment at the facility, the woman claimed to have been contacted by an unknown individual who had photographs of her printed medical records. She also received a video recording of the person scrolling through her electronic medical record on a computer screen.

OCR's investigation substantiated the woman's complaint and confirmed there had been unauthorized access to her protected health information by a malicious insider.

Since credentials must be entered in order to view patient records within the electronic medical record system, the unauthorized access could be traced to a specific individual, a non-clinical former staff member of a physician's practice. That individual was provided with access to electronic medical records for continuity of patients' care. (Source)

Hospital Employee Fired For Accessing 2,000+ Patients Records For 5 Years / Used Information To Promote His Healthcare Business - June 6, 2025

More than 2,000 patients at Jackson Health System in Miami, Florida, had their personal data, including names, address and medical information, accessed in a lengthy breach that spanned nearly five years. Social Security numbers weren't compromised, according to the hospital.

The data breach was conducted by a Jackson employee who accessed the information to promote a personal healthcare business.

News of the breach comes just days after an executive with the hospital system's fundraising arm was arrested on allegations that she pocketed more than $1 million through an almost decade-long kickback scheme.

This isn't the first time patient records have been breached at Jackson. The U.S. Department of Health and Human Services in 2019 fined the hospital system $2.15 million "over three patient health information breaches, including missing boxes of paper records, an employee leaking information about an NFL player to an ESPN reporter, and another employee stealing and selling other records. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Company Awarded $452 Million In Damages Because Former Employees Stole Trade Secrets - June 13, 2025

In a major trade secrets case, Insulet Corp. v. EOFlow Co., Insulet (Omnipod) was awarded $452 million in damages against EOFlow, a competitor, for misappropriating Insulet's trade secrets related to the Omnipod insulin pump. The jury found that EOFlow had hired former Insulet employees, stole trade secrets, and used them to create a competing insulin patch pump, the EOPatch.

After being awarded one of the largest damages verdicts in the history of trade secrets law, Insulet proceeded immediately for the entry of a permanent injunction to enjoin defendants from manufacturing, marketing, advertising, selling, distributing, or seeking regulatory approval for any product that was designed, developed, or manufactured, in whole or in part, using or relying on the four purloined trade secrets anywhere in the world. (Source)

Coinbase Damaging $400 Million Data Breach Involved Employees Paid By Cyber Criminals To Steal Data - June 16, 2025

Coinbase disclosed that cyber criminals paid contractors embedded in its support operations to siphon sensitive data, including government ID images, account balances and fragments of financial records. This wasn't a one-time breach; it was a calculated extraction, slow enough to stay beneath the radar and damaging enough to cost an estimated $400 million to contain.

Coinbase, in a statement shared with Bloomberg, said it began observing unusual activity from some of these customer representatives as far back as January. The threat actors are also said to have bribed enough customer service agents to achieve "effectively on-demand access to Coinbase customer information over the past five months. (Source)

Tesla Sues Former Engineer For Stealing Trade Secrets Using Personal Smartphones To Launch Rival Startup - June 12, 2025

Tesla sued a former engineer for allegedly stealing trade secrets from its humanoid robotics program, Optimus, and using them to launch a rival startup.

The lawsuit accuses Zhongjie "Jay" Li of stealing trade secrets regarding Tesla's development of advanced robotic hand sensors to launch his startup Proception, a Y Combinator-backed company building robotic hands.

The complaint states that Li, who worked at Tesla from August 2022 to September 2024, downloaded confidential information about Optimus on two separate personal smartphones.

The complaint also added that during the last few months of his time at Tesla, Li researched "humanoid robotic hands" on his workplace computer in addition to making internet searches regarding venture capital and other startup funding sources.

"Less than a week after he left Tesla, Proception was incorporated," the complaint stated. "And within just five months, Proception publicly claimed to have 'successfully built' advanced humanoid robotic hands—hands that bear a striking resemblance to the designs Li worked on at Tesla."

Proception's website states the company is working to "revolutionize human-robot interaction by building the world's most advanced humanoid hands." (Source)

Hormel Foods Is Suing 2 Employees Accusing Them Of Stealing Trade Secrets - June 20, 2025
Hormel is seeking unspecified monetary damages and is asking for the return and deletion of confidential data. The breakfast sausage maker is seeking unspecified monetary damages and is demanding the recipes be returned, according to court documents.

"Johnsonville appears to have undertaken a coordinated effort to interfere with Hormel's employment relationships and obtain Hormel's confidential, proprietary and trade secret information," Minnesota-based Hormel said in its complaint, describing the sausage market as "increasingly competitive."

Johnsonville hired Hormel Foods' former Director of Operations Brett Sims in 2023, according to the lawsuit, filed June 18 in Minnesota. Hormel alleges Sims tried to solicit other Hormel employees to work for Johnsonville within a year of switching jobs.

Sims' successor heading sausage products, Jeremy Rummel, later took a job with Johnsonville, then allegedly sent "highly sensitive confidential, proprietary, and trade secret information" to his own personal email account before he gave notice to Hormel Foods, the lawsuit says.

Rummel, who had been with Hormel since 1991, worked with Sims and other Johnsonville staff to steal those secrets "for the express purpose of exploiting the information for Johnsonville's benefit, and to Hormel's detriment, in the marketplace," court documents say. Rummel and Sims had previously signed nondisclosure agreements when they began working at Hormel. (Source)

Employee Heading To Prison For Stealing Hundreds Of Confidential Technical Documents And Selling, Espionage Benefited Russia - June 26, 2025
The Dutch Public Prosecution Service (Openbaar Ministerie, OM) on demanded a four-year prison sentence for German A., a 43-year-old former employee of ASML, accused of industrial espionage benefiting Russia.

According to the OM, German A. sold manuals and technical documents from leading Dutch chip manufacturers, including ASML, NXP in Nijmegen, and startup Mapper in Delft, to Russian contacts. These documents were allegedly used to help Russia develop its own semiconductor industry, violating EU sanctions imposed on Russia.

The prosecution said German A. copied hundreds of confidential documents onto USB sticks and hard drives over several years. He then physically delivered the USB sticks in Moscow, reportedly receiving 40,000 euros in cash for the information.

The OM emphasized the seriousness of the offense, noting that microchips are crucial components in military vehicles, precision weapons, and drones. By enabling Russia's semiconductor production, German A. is believed to have made "a substantial contribution" to the violence in Ukraine. (Source)

CHINESE / NORTH KOREA FOREIGN GOVERNMENT ESPIONAGE / THEFT OF TRADE SECRETS INVOLVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES
North Korea Cyber Criminals Targeted Employee With Deceptive Zoom Calls To Trick Him Into Installing Malware - June 19, 2025
The North Korea-aligned threat actor known as BlueNoroff has been observed targeting an employee in the Web3 sector with deceptive Zoom calls featuring deepfaked company executives to trick them into installing malware on their Apple macOS devices.

The attack targeted an unnamed cryptocurrency foundation employee, who received a message from an external contact on Telegram.

"The message requested time to speak to the employee, and the attacker sent a Calendly link to set up meeting time," security researchers Alden Schmidt, Stuart Ashenbrenner, and Jonathan Semon said. "The Calendly link was for a Google Meet event, but when clicked, the URL redirects the end user to a fake Zoom domain controlled by the threat actor."

After several weeks, the employee is said to have joined a group Zoom meeting that included several deepfakes of known members of the senior leadership of their company, along with other external contacts. (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

Employee Sentenced To Prison For Embezzling $900,000+ From Employer Over 4 Years - June 17, 2025

From 2016 to 2021, Michelle Wilshire was employed by a family-owned business located in Conover, North Carolina, identified as Company A.

During the relevant time, Wilshire was in charge of the company's Comdata account, a third-party payment processing and debit card issuing service, which the company used for fleet management and payment services for its drivers. Wilshire executed the scheme by issuing multiple Comdata prepaid debit cards in her name and in the names of other individuals, including former company employees, fictitious employees, and current employees who were not aware the cards existed.

Wilshire then caused Comdata to load funds onto the prepaid debit cards, which she then withdrew via ATM cash withdrawals. Between November 2017, and July 2021, Wilshire withdrew more than $528,000 from prepaid Comdata debit cards.

In addition to the debit card scheme, Wilshire embezzled company funds by using Comdata's Comchek and Comchek Mobile services to issue checks in the defendant's name and to make multiple wire transfers into Wilshire's personal bank account, totaling over $315,000. Wilshire also caused more than $58,000 of the company's funds to be transferred through Comdata into the bank account of a former company employee. (Source)

Company President Pleads Guilty To Embezzling $413,000+ - June 17, 2025

John Tharp served as president of Bendco, a Texas company that specialized in bending pipes, tubes and other metal materials for oil and structural applications. The company filed for bankruptcy in February 2018.

Tharp admitted to embezzling funds by diverting and cashing customer payments at local businesses. He also directed Bendco to issue fraudulent checks payable to cash, fictitious vendors or companies with no legitimate business ties. To conceal the theft, Tharp altered the company's financial records, including by deleting invoices.

Tharp carried out the scheme while Bendco was in bankruptcy proceedings. As part of that process, the company was required to deposit all incoming funds into a Debtor in Possession (DIP) account.

Tharp admitted he caused Bendco to file false monthly operating reports to the bankruptcy court, falsely stating that all funds had been deposited into the DIP account. Tharp acknowledged his embezzlement resulted in a loss of $413,480. (Source)

Investment Company Employee Pleads Guilty To Insider Trading Scheme That Provided Him A Profit Of $200,000+ - June 6, 2025

While working from his home, Ryan Squillante was employed as the Head of Equity Trading at Irving Investors, an investment company headquartered in Denver, Colorado. As a result of his position at Irving Investors, Squillante received material non-public information (MNPI) about various publicly traded companies. On 15 different occasions between August 2022 and May 2023, Squillante used MNPI for his own benefit by executing transactions in securities of these companies, making a total profit of $220,912.

As an example, in February 2023, Squillante received MNPI about Praxis Precision Medicines, Inc. (Praxis), a clinical-stage biopharmaceutical company whose common stock traded on the NASDAQ.

Between February 27 and March 2, 2023, Squillante "sold short" 38,086 shares of Praxis at an average price per share of approximately $3.04.

On March 3, 2023, before the market opened, Praxis announced poor results from its drug trial, stating that the drug's effects did not achieve its primary endpoint with statistical significance.

Following the announcement, Squillante "covered" his short sale by purchasing 38,086 Praxis shares at an average price per share of approximately $1.82, making a profit of approximately $46,421. (Source)

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

Office Manager / Bookkeeper For Realtor Sentenced To Prison For Embezzling $453,000+ Over 5 Years / Used Funds To Pay Her Credit Card - June 18, 2025

Lauren Eldridge was an office manager and bookkeeper for nine years with Keller Williams Realty River Cities (KW) on Georgia.

KW representatives noticed some discrepancies in a KW account in Oct. 2022 and that Eldridge had moved money out of that account to other accounts. When Eldridge was initially questioned about the transfer, she did not provide a clear explanation. Eldridge resigned from her position soon afterward.

Law enforcement was notified in Jan. 2023; a review of the KW accounts revealed that a total of $453,876.68 in monthly electronic payments were made to Eldridge's personal American Express account from KW accounts

between Jan. 2017 and Sept. 2022. Eldridge admitted to KW representatives and their legal counsel in Dec. 2022 that she embezzled the money from KW to pay her personal American Express credit card balance every month. She reported that she intended to pay this money back when she first began taking funds after she had charged $30,000 to her American Express for home repairs.

Eldridge was ordered to pay $453,876.64 in restitution to KW. (Source)

Financial Manager For Children's Advocacy Center Sentenced To Prison For Stealing $411,000+ Over 4 Years - June 13, 2025

From November 2018 to June 2022, while employed as the fiscal manager for the Children's Advocacy Center of Northeastern Pennsylvania (CAC/NEPA), Angela Saar engaged in a scheme to defraud the CAC/NEPA. Formed in 1998, the CAC/NEPA, is a private, non-profit, tax-exempt 501(c)(3), whose mission is to provide excellence in the assessment and treatment of child abuse and neglect.

During her tenure as the fiscal manager for the CAC, Saar diverted fraudulent payments of various kinds from CAC/NEPA bank accounts into her own personal bank accounts for her personal benefit.

Some of the diverted payments involved fraudulent mileage reimbursements, while others involved Saar inflating her bi-weekly paychecks by thousands of dollars.

The total amount of restitution ordered payable to the CAC/NEPA was $411,940.11. Saar also similarly defrauded a second charitable organization in Lackawanna County for which she paid restitution. (Source)

Office Manager Sentenced To Prison For Embezzling $400,000+ Over 4 Years / Used Funds For Personal Expenses - June 13, 2025

Between December 2019 and February 2023, Nichole Lawrence was employed as an office manager for a business in Western Kentucky.

She used her position to embezzle approximately $400,000 from the business. Lawrence used the stolen money to pay personal expenses. Lawrence was also ordered to pay $400,000 in restitution. (Source)

Employee Arrested For Embezzling $330,000+ / Used Fund To Support His Family & Way Of Life - June 4, 2025

Eric Skipper, a Lipscomb Powersports employee was arrested and charged with theft of more than $300,000 in April 2025. Lipscomb Power Sports had filed a report of the crime in July 2024 after he was fired.

Skipper's embezzlement efforts included fraudulent returns, sales records manipulating, and exploiting software loopholes. Records claimed that Skipper was one of the only person with the access to the records system, and the ability to manage cash intake and deposit returns.

Skipper admitted to the embezzlement and told investigators he took the funds to support his family and way of life. Skipper stole at total of $331,983.20 from Lipscomb Powersports. (Source)

Finance Director For Non-Profit Organization Sentenced To Prison For Embezzling $320,000 / Used Funds To Pay For Travel For Himself, Family & Friends - June 17, 2025

Jarrett Lewis was employed by the non-profit organization (NPO) between June 2021 and October 2022.

While serving as Director of Finance, Lewis perpetrated a scheme to defraud his employer. Lewis was one of three employees at the NPO with access to the non-profit's bank account. It was part of Lewis's duties to pay bills on behalf of the organization. Lewis was also provided with a VISA card for an account belonging to the NPO and was authorized to use the VISA card to incur expenses on behalf of the NPO for goods and services related to its operations.

On 32 occasions, Lewis took advantage of his position by accessing the NPO's account and causing funds to be transferred to his personal account and for his own personal benefit.

Lewis also used the non-profit's VISA to book and pay for personal travel for himself, his family, and friends. Lewis was ordered to pay restitution of $318,000. (Source)

Chemical Manufacturing Company Managing Partner Sentenced To Prison For Using $250,000 Of Company Funds To Build House - May 30, 2025

Jerry Noles was the managing partner of Coil Chem LLC, a chemical manufacturing company based in Washington, Oklahoma.

Noles opened a $690,000 revolving line of credit through First National Bank (FNB) for the bank-authorized purpose of funding Coil Chem's operating expenses. Noles later caused the advance of $250,000 from the company's credit line into another account under Noles' control, then directed a coconspirator to immediately withdraw and deposit the funds into the account of a local home builder to help pay for the construction of a new home for Noles. Noles then sought and obtained a $1,200,000 home construction loan from FNB, despite the fact he had already paid a portion of the home's construction costs with the money fraudulently obtained from Coil Chem's credit line. (Source)

Chief Financial Officer Pleads Guilty To Stealing $211,000+ / Used Funds To Pay For Spouse's Long Term Care, Etc. - June 6, 2025

Pamela Kahut is the former Chief Financial Officer of Pacific States Marine Fisheries Commission (PSMFC). pleaded guilty Thursday for stealing money from PSMFC's health benefit trust account.

Kahut had access to and controlled PSMFC's health benefit trust account that was created to pay benefits, fees, and other charges for PSFMC employees covered under its self-funded health care benefit program.

On September 21, 2020, Kahut wrote a check in the amount of $2,812.85 from the health benefit trust account to pay for her spouse's participation in PSFMC's long-term care insurance program.

In total, between October 2014 and September 2020, Kahut stole approximately $211,083 from PSMFC's health benefit trust account. Kahut used the funds to pay for her spouse's long-term care annual premiums, pay off her pension loans, and to pay her credit card bills. (Source)

Employee Arrested For Stealing $10,000+ In Cash From Store Safe - June 25, 2025

Amonie Owens, 31, was arrested June 19 following an investigation by the Aberdeen Police Department into a reported internal theft at the Burlington store in Aberdeen.

The Aberdeen Police Department, officers were called to the store after management reported a suspected larceny by an employee. During the investigation, officers reviewed surveillance footage and identified Owens as the suspect. Police say the video confirmed Owens accessed the store's safe and removed more than $10,000 in cash. (Store)

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

Public Works Employee Arrested For Stealing County Owned Diesel To Fuel His Trucking Company Trucks - June 3, 2025

Joseph Ridley, 47, was arrested and charged with Second-Degree Official Misconduct, Second-Degree Pattern of Official Misconduct, Third-Degree Theft by Unlawfully Taking, and Third-Degree Conspiracy to Commit Theft, according to the Atlantic County Prosecutor's Office (ACPO).

Ridley is employed as a supervisor in the Roads and Bridges Department within the Atlantic County Department of Public Works and also owns trucking company Z5 Logistics LLC.

Officials say that on May 27, 2025, Atlantic County Fleet Management authorities spotted a large box truck fueling at the county-owned fueling station in Northfield, New Jersey. When staff approached, the box truck was driven away.

The incident resulted in the launch of an investigation. "It was uncovered that Ridley provided this code to employees of his business: Z5 Logistics LLC," ACPO said.

"On June 2, 2025, detectives from the Atlantic County Prosecutor's Office apprehended employees of Z5 Logistics LLC as they were fueling the business trucks at the Atlantic County fuel site without authorization. Investigation led to the arrest of the employees as well as Ridley." (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former IT Manager Charged With $1 Million Theft & Money Laundering Scheme Using Fraudulent Invoices And Shell Company - June 24, 2025

Charles Richardson was employed as an information technology professional with the Pittsburgh-based philanthropic foundation The Heinz Endowments.

Between 2016 and 2024, Richardson embezzled almost $1 million in funds from his employer through a shell corporation Richardson controlled and fraudulent invoices that billed the foundation for work not performed or performed by other vendors. (Source)

Company Senior Staff Accountant Sentenced To Prison For Embezzling $440,000+ Using Fraudulent Invoices / Used Funds For Personal & Family Members Expenses - June 6, 2025

Between April 2022, and June 2024, Erin Martin defrauded a business, located in Amherst, NY, which employed her as a Senior Staff Accountant. Martin reported to the Chief Financial Officer and was responsible for, among other things, ensuring that the company's vendor invoices were paid timely.

Martin created fraudulent vendor invoices addressed to her employer. Martin would then make unauthorized electronic funds transfers from the company's bank account directly into her personal bank account, purportedly as payments on the fraudulent invoices she had created. In total, Martin caused 95 electronic funds transfers totaling $440,395.00. Martin used these funds to pay her own personal and family members expenses. (Source)

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

Former Employee Responsible For $2 Million Attack On Network - June 25, 2025

A former employee of analytics platform Fuzzland disclosed that a former employee was responsible for a $2 million exploit that targeted Bedrock's UniBTC protocol in September 2024.

In a new transparency report, Fuzzland revealed that the employee used social engineering tactics, supply chain attacks and advanced persistent threat techniques to steal sensitive data that enabled the attack. The platform said the attacker exploited the vulnerability in UniBTC after it was internally discussed in an emergency response call.

The company added that its ex-employee inserted a malicious code that created backdoors in engineering workstations and remained undetected for weeks. The access allowed the attacker to receive sensitive information and act on the vulnerability first flagged in a Dedaub report.

Bedrock is a multi-asset liquid restaking protocol offering UniBTC, UniETH and UnilOTX products. These synthetic representations of major blockchain tokens allow users to earn yields through staking.

On Sept. 27, Bedrock confirmed that it had been exploited, which affected its UniBTC product. The attacker drained $2 million in liquidity from its decentralized exchange pools. Despite the hack, Bedrock's total value locked (TVL) grew from $240 million in September 2024 to $535 million in June 2025, according to DefiLlama. (Source)

Fired Construction Employee Arrested For Vandalizing High Priced Bulldozer And Backhoe - May 30th 2025)

New details today have emerged about the suspect arrested for vandalizing a high-priced bulldozer and backhoe being used to build the Southwest Trail in Saline County in Arkansas.

Police arrested a former employee (Clint Guthrie) just days after he was fired, and investigators say there was a tense dispute over his final paycheck what prompted them to investigate him.

Guthrie was terminated from his employment with James A. Rogers excavating last Friday, just hours before the damaged equipment was discovered.

"Mr. Guthrie got fired from the business at approximately 3:30. Responds back to the business, there's some phone conversations. We have video of him driving back to the job site," says Lead Detective Tim White.

After Guthrie left the scene, he was involved in a vehicle accident and received a citation from the Arkansas State Police. Upon reviewing ASP dash cam footage, investigators noted that Guthrie's pant legs appeared wet and muddy.

"We talked for the company, got a direction to look. We found the vehicle and were able to track that vehicle through video. And we were able to put together a very tight timeline which put Mr. Guthrie in the area at the time of the crime," says White.

Authorities were led to review the equipment logs, which revealed that the machines had been powered down around the same time as Guthrie's accident. Surveillance footage from the area later confirmed that Guthrie's vehicle was seen near the job site around the time the final piece of equipment was shut down. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Employee Working For Multinational DVD Company Pleads Guilty To Stealing, Selling Pre-Release Commercial DVDs For Blockbuster Films - March 6, 2025

Steven Hale, 37, worked for a multinational company that, among other things, manufactured and distributed DVDs and Blu-rays of movies.

From approximately February 2021 to March 2022, Hale allegedly stole numerous "pre-release" DVDs and Blu-rays, that is, discs being prepared for commercial distribution in the United States and not available for sale to the public.

These included DVDs and Blu-rays for such popular films as “F9: The Fast Saga,” “Venom: Let There Be Carnage,” “Godzilla v. Kong,” “Shang-Chi and the Legend of the Ten Rings,” “Dune,” and “Black Widow.”

Hale allegedly sold the DVDs and Blu-rays through e-commerce sites. At least one pre-release Blu-ray that Hale allegedly stole and sold, “Spider-Man: No Way Home,” was “ripped” — that is, extracted from the Blu-ray by bypassing the encryption that prevents unauthorized copying — and copied. That digital copy was then illegally made available over the internet more than a month before the Blu-ray’s official scheduled release date. Copies of “Spider-Man: No Way Home” were downloaded tens of millions of times, with an estimated loss to the copyright owner of tens of millions of dollars. (Source)

Car Dealership Employee Arrested For Stealing $200,000 In Luxury SUVs Off The Lot - June 26, 2025

A now-former employee of Smythe Volvo Cars in Summit, New Jersey, may have been inspired to do something straight out of the movie "Gone in 60 Seconds."

A major plot point in the film was three Mercedes that were considered unstealable; their special laser-cut keys had to be ordered from the factory in Germany, and the cars wouldn't open or start without them. Kip Raines had this covered with a connection at a dealer who would get keys made for the cars he intended to steal. Maybe you see where we're going with this.

The Summit Police Department arrested Henrri Bonilla of Newark for allegedly stealing three cars from the dealership during his employment. The first, a 2025 Volvo EX90, was reported on April 15. A second EX90 was reported stolen from the same dealer on May 7. Switching things up a bit, a 2021 Mercedes-Benz GLE mysteriously disappeared off the lot on May 26 (no laser-cut key necessary, it seems).

These cars are collectively worth around $200,000. Police say that Bonilla used his access to key fobs, which make cars easier to steal, to carry out the heists. (Source)

FedEx Freight Employee Charged For Stealing 27 iPhones - June 24, 2025

On June 20, at about 4:00 a.m., members of the Broome County Sheriff’s Office Road Patrol responded to a larceny complaint at FedEx Freight East, located on Industrial Park Drive in Kirkwood in New York

The security specialist told officers that an employee had been stealing from an inventory of Apple iPhones at the facility since April by sneaking them inside his coat pocket.

Following an investigation, including review of security footage, Leon J. Roberts, 22, of Endicott, was charged with the felony of grand larceny. (Source)

Employee Arrested For Stealing 2,000 Pounds Of Copper Wire And Selling For $10,000 - June 13, 2025

On June 4, Aberdeen investigators were advised of a larceny from an employee that had previously occurred, resulting in the theft of over 2,000 pounds of copper wire. The name of the business was not released.

Detectives began to investigate the allegations and were able to confirm the copper wire had been fraudulently sold at a recycling center in Lumberton. Detectives continued to investigate by utilizing GPS records, video surveillance, and business receipts, and were able to confirm Hammonds was responsible. Detectives began to investigate Hammonds further and determined that he had previously sold an additional 1400 lbs of copper wire that was stolen from his employer. It was confirmed that Hammonds stole copper wire on four occasions over the past 5 months, and obtained $10,000 for the stolen property. (Source)

Jewelry Store Manager Sentenced To Prison For Stealing $170,000+ In Diamonds, Jewelry, Silver, Gold, Cash - June 26, 2025

Lucy Roberts, a former jewelry store manager at a high-end shop in the United Kingdom (U.K.) was arrested after she was caught "dripping in diamonds" in multiple vacation selfies.

Roberts would frequently bring jewelry home during the year she was employed at the shop. When her coworkers became suspicious, she explained that she was simply "conducting work at home and sorting stock for the workshop," according to authorities.

Roberts quit the job, however, and decided to go on vacation. During that time, Roberts sent her former coworkers selfies from aboard a cruise ship while donning multiple items that had gone missing from the shop.

During an investigation into Roberts, authorities located "thousands of pounds worth of jewelry strewn around in boxes beneath the bed and in cupboards" inside her home.

Roberts stole more than $170,000 in diamonds, silver, gold, cash and jewelry" in total from the business.

Authorities located and arrested Roberts at Heathrow Airport in London after she was caught "wearing a substantial amount of stolen jewelry." Police also discovered additional stolen merchandise inside her suitcase. (Source)

Woman Dressed As Home Depot Employee Arrested For Stealing 2 Portable Air Conditioners - June 26, 2025

2 people have been arrested after a shoplifting incident at a Home Depot in East Haven. At around 12:40 p.m., Home Depot loss prevention called police after seeing a woman walking out of the store with a cart load of unpaid merchandise.

The woman, later identified as 35-year-old Mercedes Zebrowski of Bridgeport, was wearing a home depot apron in an effort to pose as an employee.

Home Depot staff recovered two portable air conditioners valued at nearly $800.

Officers located Zebrowski and a male driver, later identified as 40-year-old Julio Velazquez of Bridgeport, in a nearby car. Zebrowski, who still had the Home Depot apron, was taken into custody.

Officers found Zebrowski had multiple active arrest warrants from various jurisdictions, totaling $130,000.00 in bonds. Zebrowski was arrested and charged with larceny in the fifth degree.

Velazquez was arrested and charged with interfering with an officer and conspiracy to commit larceny in the fifth degree. She is currently being held on a total of $130,500.00 in bonds. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Casino Employee & Husband Arrested For Embezzling $89,000+ From Casino - June 4, 2025

San Jose police have arrested a casino worker and her husband on suspicion of embezzling from the business.

Casino employee Ellen Mangundayao, 38, allegedly embezzled gaming chips from the business between May 1 and May 22, police said. She would then hand the chips to her husband, 41-year-old Mark Mangundayao, who would go and cash them out.

Police believe the duo conspired in the embezzlement of hundreds of thousands of dollars over several years.

Authorities obtained arrest warrants for the couple as well as search warrants for two associated homes in San Jose, police said.

Ellen had roughly $4,750 worth of casino chips on her when she was taken into custody, and detectives seized over $75,000 in cash and about $10,000 worth of additional casino chips while serving the search warrants at the residences. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

No Incidents To Report

OTHER FORMS OF INSIDER THREATS

Report Warns That Autonomous Artificial Intelligence Agents Are Becoming Unmonitored Insiders Within Enterprise Networks - June 25, 2025

AI agents are increasingly acting like digital employees within enterprise environments, but organizations are largely failing to treat them as such, according to a new report from BeyondID, a managed identity solutions provider.

The company's 2025 survey of U.S.-based IT leaders uncovered a troubling disconnect: While a majority of organizations claim readiness for artificial intelligence in network security, fewer than half monitor the access or behavior of the very AI systems they deploy.

AI agents are increasingly acting like digital employees within enterprise environments, but organizations are largely failing to treat them as such, according to a new report from BeyondID, a managed identity solutions provider.

The company's 2025 survey of U.S.-based IT leaders uncovered a troubling disconnect: While a majority of organizations claim readiness for artificial intelligence in network security, fewer than half monitor the access or behavior of the very AI systems they deploy. (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

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Family Dollar Employee Arrested For Shooting Customer For Stealing Merchandise - June 11, 2025

A Family Dollar employee (Jerome Stepp) was arrested after he allegedly shot a man in the butt for reportedly stealing company merchandise, according to police.

According to court documents, around 15 minutes after the theft occurred officers heard gunshots near the store. The report said that a man was shot in his buttocks. While at the scene of the shooting, officers spoke with a witness who described the shooter and their vehicle. When the officers went back to Family Dollar they saw the vehicle and the two Family Dollar employees that the witness described.

Stepp, who is engaged to the other Family Dollar employee, told her that they needed to get the merchandise back. When they drove down the street they found the man on the bicycle and Stepp fired a warning shot. The reported thief dropped the merchandise when he was hit by the second shot that was fired. (Source)

Altercation Between 2 Walmart Employees Results In 1 Being Shot / Critically Injured - June 20, 2025

A Walmart employee is critically injured after being shot by another employee at the Bartlett Supercenter store.

The police say the shooting stemmed from an altercation between two employees. Police say the victim was taken to the hospital in critical condition. According to police, the suspect was taken into custody without incident.

Police said two employees were arguing before the shooting. Investigators haven't said what the fight was about.

Walmart responded Friday, saying the suspect was no longer employed by the company: "Violence is unacceptable, and the associate has been terminated. We are cooperating with police." (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.

TYPES OF INSIDER THREATS

- ☐ 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 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.

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 (**6,400+ 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

Why Insider Threats Remain An Unresolved Cybersecurity Challenge

Produced By: IntroSecurity And NITSIG / June 2025

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

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

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

(Download Report)

U.S. Government Insider Threat Incidents Report For 2020 To 2024
The NITSIG was contacted by Senator Joni Ernst's office in December 2024, and a request was made to write a report about Insider Threats in the U.S. Government for the Department Of Government Efficiency (DOGE). (Download Report)

Department Of Defense (DoD) Insider Threat Incidents Report For 2024
The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. (Download Report)

Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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

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

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS
https://www.nationalinsiderthreatsig.org/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

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

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

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

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

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

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED
Conducted Via Classroom / Onsite / Web Based
TRAINING

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

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

STUDENT / CLIENT SATISFACTION

ITDG training courses have been taught to over **1000+** individuals. Our clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM. Our client satisfaction levels are in the **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 675 Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, 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
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

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

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