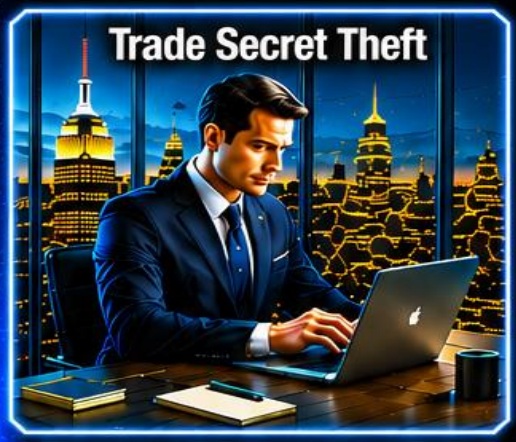
INSIDER THREAT INCIDENTS REPORT FOR

★ July 2026 ★

DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM



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 **7,300+** 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 hundreds of thousands of dollars, maybe millions in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of these monthly reports, you might have a different perspective on Insider Threats.

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

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

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

INSIDER THREAT INCIDENTS
FOR JULY 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
Australian Institute Of Insider Threats - Insider Threat Incidents Weekly Reports
https://www.insiderthreats.au/threat-warning

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES
No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS
No Incidents To Report

U.S. GOVERNMENT
U.S. Secret Service Agent On Vice President Team Under Investigation For Allegation Of Compromising The Vice President's Security By Leaking Information To News Media - July 23, 2026
A member of Vice President JD Vance's protective detail has been removed pending an investigation into allegations of compromising the vice president's security, a Secret Service spokesman said Thursday.

The development was first reported by CNN, citing sources familiar with the matter who told the outlet that the agent was suspected of leaking information used in an MS NOW report detailing alleged Secret Service complaints about Vance's travel habits.

Confirming the agent's removal, Secret Service spokesman Anthony Guglielmi said in a statement shared with NBC News: "A member of the Vice Presidential Protective Division is the subject of an administrative investigation, and potential criminal inquiry, involving allegations of compromising operational and information security."

"While we will not comment on the specifics of this matter, one principle is unequivocal: any conduct that potentially threatens the safety of a protectee will not be tolerated," Guglielmi added.

An administration official said Vance's travel duties can often shift unexpectedly because of important meetings and events, which override previous plans, causing strain on the Secret Service. The official also noted that unlike recent vice presidents, Vance has young children, and he tries to spend as much time with them as he can, presenting his Secret Service with a new aspect of their protective mandate.

Separately, the official said the Marine Two helicopter trip from the vice president's official residence to Joint Base Andrews is the most common route for the vice president's helicopter and requires a smaller pull on local law enforcement and other resources than a motorcade.

The Trump administration has taken a hard-line position against leaks to journalists, most recently issuing subpoenas to New York Times reporters who covered security concerns related to the new Air Force One. (Source)

White House Teleprompter Operator Accused Of Making $100,000 Profit Online By Betting On President Trump's Speech - July 16, 2026

A White House teleprompter operator is being investigated over allegedly using inside information to place bets and make nearly $100,000 on US President Donald Trump's speeches.

Gabriel Perez, who had worked at the White House since 2016, is accused of placing bets on words the president would use during major public addresses, including the State of the Union speech.

The trades were made on Kalshi, a prediction markets platform where users can bet on real-world events. The firm confirmed it reported the activity to the Commodity Futures Trading Commission (CFTC), which regulates the platform. Kalshi froze Perez's account before any profits could be withdrawn, according to reports.

The platform told the BBC its analysts noticed unusual betting on "mention markets" - contracts where users predict whether a speaker will use common terms, such as specific countries, economic words, or campaign slogans, in March.

"The words of political leaders like Presidents and Fed chairs cause billions of dollars of movement in FX markets, oil futures, [and] the stock market," Kalshi said.

Using account data, the company found the user was a federal employee operating White House teleprompters. The exchange froze more than $90,000 before it could be withdrawn.

White House press secretary Karoline Leavitt said President Trump was aware of the teleprompter operator and that staffer was now on unpaid leave, before adding Perez would no longer work at the White House. (Source)

U.S. Postal Service Employee Arrested After Making Mass Shooting Threat Against Texas Pride Event - June 30, 2026

A United States Postal Service (USPS) employee was arrested after threatening on social media to commit a mass shooting at a Pride parade in Texas, the FBI announced on Monday.

Michael Thompson, who resides in Clovis, New Mexico, was taken into custody after authorities received a tip regarding a threat to conduct a mass casualty attack at a Pride event in Lubbock, Texas.

Thompson admitted to making and subsequently deleting the social media posts, authorities said. He also identified himself as a USPS employee. Authorities said they recovered four firearms from Thompson's residence. He is legally prohibited from owning firearms due to a prior felony domestic violence conviction, according to the FBI. (Source)

U.S. Postal Service Employee Pleads Guilty To Role In Stealing A $686,000+ Check From Mail / Stole Other Checks & Sold Them - July 16, 2026

Juawan Reed, 30, is a former U.S. Postal Employee. Reed stole checks from the U.S. mail while he worked at the U.S. Postal Service Camden Carrier Annex in New Jersey. Reed sold or otherwise provided some of the stolen checks to co-conspirators who advertised some of the stolen checks on a social media platform and resold them to others. Reed provided other stolen checks directly to Holmes and others for them to negotiate fraudulently.

For example, in December 2022, Reed stole a $686,541.88 United States Treasury check payable to a business in Pennsauken, New Jersey. Reed provided this stolen check to a co-conspirator. The conspirator then deposited the stolen check, and Hayman withdrew a substantial portion of the funds before the bank detected the fraud and closed the account. (Source)

U.S. Postal Inspector Pleads Guilty To Stealing $330,000+ / Used Home Improvements, Cruises, Escorts - July 27, 2026

Scott Kelley, 52, a former U.S. Postal Inspector and a federal law enforcement officer who was authorized to carry a firearm, make arrests and execute search warrants has agreed to plead guilty to allegedly stealing over $330,000 in cash from packages mailed by elderly victims and then laundering the cash. Kelly used the stolen cash to pay for a pool patio, granite countertop for his outdoor bar, lighting for his pool and bar, Caribbean cruise expenses, and escorts.

Kelley was a Postal Inspector at the Boston Division headquarters of the U.S. Postal Inspection Service (USPIS), the law enforcement arm of the Postal Service. In 2015, Kelley became the Team Leader of the Mail Fraud Unit, which, among other things, investigated lottery and other scams that targeted senior citizens and other vulnerable populations.

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

7 victims who were scammed into mailing cash in parcels that Kelley allegedly intercepted and opened, and that he stole the cash inside. The average age of the victims was 75, with the oldest victim being 82. The victims mailed between $1,400 and $19,100 cash. One victim died after Kelley was indicted. (Source)

U.S Postal Service Employee Charged For Role In Stealing $255,000 In Prepaid Debit Cards / Used Funds For Personal Expenses - June 29, 2026

A federal grand jury has returned an indictment charging three individuals in a significant mail theft and fraud scheme targeting at least 3,000 victims.

U.S Postal Service (USPS) employee Janea Reaves, 38, has been charged with conspiracy to commit access device fraud and illegal transactions with an access device. Her co-defendants, Jermaine Reaves, 22, and Dejon Fox, 39, have also been charged with conspiracy to commit access device fraud, as well as two counts of mail theft.

Between May 2023 and March 2025, the trio conspired to use and possess unauthorized access devices and to engage in transactions using unauthorized access devices. The indictment alleges that the defendants stole mail containing prepaid debit cards issued to real individuals. Using her position at the USPS Indianapolis Processing and Distribution Center, Janea Reaves identified and stole mail containing the prepaid debit cards. Jermaine Reaves and Dejon Fox, who were not USPS employees, also entered the facility and stole the mail.

The defendants activated the stolen cards and used them to pay for phone bills, DoorDash orders, and other personal expenses. The total loss is alleged to be at least approximately $255,851. (Source)

3 U.S. Postal Service Employees Plead Guilty To Stealing Up To $150,000 In Cash, Gift Cards & Checks From Mail - July 24, 2026

Fernando Camacho, 31, Angel Rivera, 30, and Cyril Murray, 46, each pleaded guilty to charges of conspiracy to steal mail and theft of U.S. Mail by a postal employee.

Camacho, Rivera, Murray, and several co-conspirators participated in a scheme that operated between early 2023 and early 2024. As part of this conspiracy, the group of postal service employees sorted through the mail and removed brightly colored envelopes that they believed to contain cash, checks, or gift cards.

They concealed those envelopes in backpacks and removed them from the facility to later distribute amongst the group. Camacho admitted that during his participation in the scheme, between $40,000 and $95,000 in cash, gift cards, and checks were stolen. Rivera admitted that during his participation in the scheme, between $95,000 and $150,000 in cash, gift cards, and checks were stolen. Murray, a supervisor at the mail distribution center, admitted that during his participation in the scheme, between $95,000 and $150,000 in cash, gift cards, and checks were stolen. (Source)

U.S. Postal Service Mail Carrier Sentenced To Prison For Role In $133,000 Mail Theft Scheme With Husband - June 30, 2026

From in or about December 2022 through May 23, 2024, Tameka Babulal conspired with others in a scheme to possess, steal, and misuse mail stolen from the USPS in Mount Vernon, New York.

Babulal stole hundreds of mail items from hundreds of victims whose mail she touched, including checks, credit cards, financial mail, tax documents, Social Security cards, and other sensitive materials. She kept those items at the Hempstead, New York, residence she shared with her husband and co-conspirator, Joel Babulal. Babulal's victims included elderly people in their 90s, young adults in their early 20s, business owners, churchgoers, military personnel, and other everyday people.

Using the mail and other items she stole from victims on her mail route, Babulal carried out an extensive credit card, check, and identity theft fraud scheme involving dozens of victims. Babulal's credit card scheme involved at least around $40,922.41 in fraudulent transactions using stolen credit cards. Babulal's check fraud scheme involved $13,510 in fraudulent transactions using stolen checks, and her possession of an additional at least $78,705.05 in checks and money orders. (Source)

U.S. Census Bureau Program Manager Sentenced To Prison For Conspiring With Subcontractor To Receive $790,000 In Kickbacks For Contracts - July 16, 2026

Camille Jones, 47, is a former supervisory official with the U.S. Census Bureau. She was sentenced to prison for conspiring with a subcontractor to receive $790,000 in kickbacks.

Jones admitted that she steered a large employee assistant program contract to a prime contractor and a subcontracting company, YMJ Consulting, which is owned by Camille Jones's relative, Yolanda M. Jones. The contract was worth millions of dollars. In exchange for steering the contract and modifications, Jones received kickbacks from YMJ Consulting and Yolanda Jones.

Additionally, Camille Jones attempted to obstruct the investigation by drafting a service agreement between YMJ Consulting and a mental health company that she owned to make the kickbacks appear like legitimate

consulting payments between the two companies. Both Camille Jones and Yolanda Jones signed the agreement in 2024 but backdated it to 2020. Yolanda Jones then provided the document to law enforcement during the investigation.

Camille Jones further admitted that she used her official position to share the Census Bureau's confidential procurement information with another government contractor. While receiving preferential treatment, the contractor hired another one of Camille Jones's relatives for a minimal-work job. Camille Jones largely performed the work but the relative received $83,000. (Source)

DHS Employee Charged With Fraudulently Obtaining $478,000 Veteran's Affairs Backed Mortgage - July 21,2026

Schleider Aristhyl, 30, a Department of Homeland Security (DHS) employee has been arrested and charged for allegedly committing wire fraud and submitting false statements in a mortgage application seeking a mortgage backed by the Department of Veteran's Affairs (VA).

According to the charging documents, in October 2024, Aristhyl submitted two falsified documents that purported to be from the VA with his application seeking a VA-backed mortgage in the amount of $478,000 from private lender.

The first fraudulent document stated that Aristhyl had received a VA disability rating of 100% and that he was receiving monthly disability benefits of over $3,000 per month. It is alleged that the document was falsified and that Aristhyl had no VA disability rating at the time of his application and he was not receiving any monthly disability benefits from the VA in October of 2024.

The second fraudulent document allegedly purported to be a VA certificate stating that Aristhyl was exempt from paying a "funding fee" to the VA. Veterans applying for a VA-backed mortgage are typically required to pay a funding fee to the VA, unless they are deemed exempt under VA rules. It is alleged that the document was falsified and that Aristhyl was not exempt from paying the funding fee, which was over $10,000.

Relying on the misrepresentations in these false documents the lender issued a mortgage loan in the amount of $478,000 to Aristhyl on Oct. 25, 2024 and the VA issued a loan guarantee backing a portion of the mortgage on Jan. 21, 2025. (Source)

Puerto Rico Department Of Treasury Employee Charged With Accepting $10,000 Bribe To Eliminate Taxes Owed - July 2, 2026

Luis Jiménez-Guzmán, a Puerto Rico Department of Treasury (PRDT) employee was charged and pleaded guilty to a bribery conspiracy involving the loss of approximately $5,000,000 in Puerto Rico tax revenue, in violation of 18 U.S.C. § 371.

Jiménez-Guzmán, knowingly and willfully conspired to commit federal program bribery and wire fraud, as well as accepted bribe payments in exchange for his corrupt acts.

From February 2019 through March 2023, Jiménez-Guzmán was an employee and agent of the PRDT with duties that included physically and electronically accessing and reviewing tax returns and documents related to invoicing and collection of owed taxes. Jiménez-Guzmán had privileged access to the PRDT's online platforms, the Puerto Rico Integrated Tax Administration System (PRITAS) and the Internal Revenue Unified System (GenTax/SURI) and was experienced and able to access, monitor, and modify taxpayer information, including creating taxpayer credits, modifying income tax, employee retention tax and sales tax information.

Jiménez-Guzmán corruptly accepted cash payments and other benefits, in exchange for submitting false information to the PRDT. The false information was submitted to the PRDT for the elimination of taxes owed, evasion of taxes, and theft of funds. For example, on August 16, 2021, Jiménez-Guzmán received a $10,000 bribe payment from Person H to erase and reduce a tax debt of one of Person H's customers.

The illicit payments were solicited and accepted by Jiménez-Guzmán, who illegally eliminated the PRDT tax liabilities and obtained illegal tax refunds for several individual and business taxpayers, with a total approximate loss to the PRDT of $5,000,000. (Source)

Department Of Energy Employee Sentenced To Probation For Trying To Bribe Another Employee For Contracts For His Personal Business - July 8, 2026

Edward Doherty, 35, worked for the Department Of Energy (DOE) as a Security Specialist until he agreed to participate in the deferred resignation program in February 2025.

Just before he started working with the DOE, in November 2024, Doherty started a company in Massachusetts called MAE Systems, LLC (MAE).

In February 2025, Doherty offered a DOE employee money in exchange for the DOE employee ensuring that MAE received DOE contracts. The DOE employee reported the incident to law enforcement. Between February and June 2025, Doherty was recorded offering to pay the DOE employee at least $10,000 in exchange for the DOE employee awarding a DOE contract to MAE. In June 2025, Doherty made two downpayments on the bribe, totaling $2,500, to the DOE employee. (Source)

Former Department Of Education Employee Agrees To Pay $161,000+ For Fraudulent Covid Paycheck Protection Program - July 15, 2026

Natayah Adams, 44, has agreed to pay the United States $161,248.30 to resolve allegations that she submitted false claims to obtain three Paycheck Protection Program (PPP) loans.

In 2021, Adams submitted applications for three PPP loans in less than three months, each with a different lender. In total, Adams received $62,499.32 in PPP loans. Adams falsely claimed that her business — in which Adams resold jewelry purchased from another company on Etsy — brought in a gross income of $100,000.00.

But Adams knew, the gross income of the business was less than $100,000.00. Adams did not use the loans for the approved purposes listed on her applications. Instead, she diverted the money for personal use and to put toward a separate business. (Source)

DEPARTMENT OF WAR / INTELLIGENCE COMMUNITY

Defense Contractor To Pay $7.75 Million Penalty For Employing Department Of War Employee Who Was Also Working As A Contractor - July 28, 2026

Sierra Nevada Company, LLC (SNC), headquartered in Sparks, Nevada, agreed to pay $7.75 million to settle False Claims Act allegations arising from its employment of a government official who, while employed by both SNC and the government, participated personally and substantially in three government contracts awarded to SNC.

From July 2019 to June 2020, SNC retained Michael Henry, a Department of War employee with the Joint Staff/J6, as a consultant. As a Joint Staff/J6 employee, Henry was involved in the award of three different government contracts to SNC: (1) a subcontract awarded by the Army in 2019, (2) an indefinite quantity/indefinite delivery contract awarded by the General Services Administration in 2020, and (3) task orders under an indefinite quantity/indefinite delivery contract awarded by the Special Operations Command in 2018.

After beginning his employment with SNC, Henry continued to serve as a Joint Staff/J6 employee. In that capacity, Henry continued participating personally and substantially in the contracts by evaluating and obtaining approvals for SNC's products. While serving as an SNC consultant, Henry also participated personally and substantially in the contracts on SNC's behalf by recommending SNC's products for purchase. (Source)

Missile Defense Agency Sentenced To 5 Years Of Probation For Unlawful Retention Of Classified Documents At Her Home - June 24, 2026

Ewa Maria Ciszak had 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. It was also confirmed that Ciszak was fired by the Department of Defense, and her security clearance has been revoked. (Source)

Former Veterans Affairs Employee Pleads Guilty to Fraudulently Obtaining $41,000+ Of Covid-19 Benefits - July 20, 2026

Denise Baez, 51, was employed as a Medical Technician with the U.S. Department of Veterans Affairs.

Baez submitted two applications seeking Paycheck Protection Program (PPP) loans. In those applications, Baez made false claims regarding gross income purportedly earned from a sole proprietorship. To support these false claims, Baez attached fraudulent tax documents as part of the applications. The PPP loan applications were approved and Baez received $41,666. Baez used that money on personal expenses. However, in September 2021, Baez submitted loan forgiveness applications that falsely claimed the entire $41,666 was spent on payroll. Based on the misrepresentation the loans were forgiven. (Source)

U.S. Naval Undersea Warfare Center Employee Sentenced To Prison For Making Death Threats To Employees - July 24, 2026

A former employee of the Naval Undersea Warfare Center (NUWC) in Middletown, Rhode Island, has been sentenced to prison.

Between July 2022 and February 2023, Luis Pardella, 38, made numerous, and at times threatening, telephone calls to at least eight of his former colleagues at NUWC. In one instance, Pardella left a voicemail stating, "I will kill you and your wife when I see you on the street."

Additionally, between December 2022 and February 2023, Pardella made multiple threatening telephone calls to the Portsmouth, Rhode Island, Police Department, stating that an officer and his wife "will be going to jail," that "the Portsmouth Police Department is corrupt," and, in reference to the officer's wife, "write down (name redacted) is dead… the wife of one of your cops is dead." (Source)

D.C. National Guard Major Pleads Guilty To Immigration Fraud Scheme & The Theft Of $54,000 Of Government Money - July 28, 2026

Collin Welch, 40, is a Major in the D.C. National Guard. He pleaded guilty today in U.S. District Court to unlawfully inducing aliens to enter and remain in the United States and to theft of about $54,000 in government money.

Welch previously served in the Alaska and D.C. National Guard with prior deployments to Afghanistan and Djibouti. In 2019, despite being married, he began a relationship with a Mongolian national while he was posted to the U.S. Embassy in Ulaanbaatar, Mongolia.

Welch later fabricated a divorce decree to convince the Mongolian woman he was no longer married, and in 2022 married her in Mongolia while still legally married to his wife. In 2024, Welch brought the Mongolian woman and her minor daughter to the United States on tourist visas, and in October 2024 married the Mongolian woman a second time, in Virginia, again while still legally married.

After the woman and her daughter's tourist visas expired in early 2025, Welch knowingly continued to support them financially and house them. When the Mongolian woman asked about her immigration status, Welch fabricated a series of documents, including fake permanent residency approvals, Social Security cards, and a letter falsely indicating military dependent health benefits, to convince her that a citizenship process was underway. None of the documents were ever filed with any government agency.

Separately, Welch used his government travel card to submit fraudulent travel vouchers and fabricated receipts for hotel stays and rental cars that never occurred, and used the card without authorization to fund personal travel and to pay for the woman and her daughter's living and travel expenses, resulting in about $54,000 in unauthorized charges to the United States. (Source)

SECURITY CLEARANCE RELATED / WHISTLEBLOWERS

House Passes Strong Whistleblower Protections For Government Contractors - July 20, 2026

Today, in a major win for government accountability, the U.S. House of Representatives voted unanimously to pass the Expanding Whistleblower Protections for Contractors Act H.R.5578.

The landmark legislation was introduced by Representatives James Comer (R-KY) and Robert Garcia (D-CA). This win comes after a unanimous Senate vote for analogous legislation, S.4631, co-sponsored by Senators Gary Peters (D-MI), Rand Paul (R-KY), and Charles Grassley (R-IA). Differences between the two chambers about the scope of protection must be resolved, as the House bill does not cover Intelligence Community contractors. (Source)

The Legislation Unanimously Agreed By Both The House & Senate Includes:

- Protection against retaliation for contractors, as well as their employees;
- Protection for exposing misconduct in international contracts;
- Protection against blacklisting;
- Protection for refusing to violate the law;
- Restoration of court access with jury trials to enforce rights; and
- Liability for government officials who pressure contractors to retaliate.

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Corrections Officer Pleads Guilty To Accepting $550,000+ In Bribes To Smuggle Contraband Into Prison / Used Funds For Designer Purchases, Plastic Surgery & SUV - July 22, 2026

A former South Carolina corrections officer, two inmates and four other people were arrested after investigators uncovered their participation in a massive bribery scheme,

Lowanda Atkinson, 52, who is a 16 year corrections officer with the South Carolina Department of Corrections Office, accepted more than $550,000 in bribes from inmates Larry Williamson and Jason Brown, along with Jason Brown's mother Mary Ann Hickman Brown, Jason Brown's brother Christopher Hickman, Jason Brown's nephew's mother Adrianna Conyers, and Jason Brown's friend Courtney Briggs.

In exchange for the bribes, Atkinson smuggled contraband, including cell phones, cell phone accessories, tobacco, and controlled substances, into Lee Correctional Institution. The contraband was later sold to other inmates by Brown and Williamson and the proceeds of the contraband sales were split between Brown, Williamson, and Atkinson. Atkinson later spent the proceeds on designer purchases, plastic surgery, and a luxury SUV. (Source)

Correctional Center Employee Pleads Guilty To Falsifying Husband's Timesheets Causing A $124,000 Loss To The State Of Illinois - July 13, 2026

Maggi Tudor, 34, began working as an Account Technician at the Illinois Pinckneyville Correctional Center (PCC) in 2022.

At the time, Tudor's husband was employed as a Correctional Officer at Murphysboro Life Skills Reentry Center, which is a satellite facility of PCC. Tudor acted as a timekeeper and backup payroll clerk for PCC and Murphysboro Life Skills Reentry Center.

Tudor admitted to abusing her position of trust as an Account Technician to falsely modify her husband's timesheets, so he obtained higher payroll payments he was not entitled to. Tudor manipulated her husband's timesheets to make it appear her husband worked overtime and holiday hours he did not work. In all, Tudor caused a loss to the State of Illinois in the amount of $124,917.35. (Source)

Massachusetts State Police Sergeant Sentenced To Prison For Obtaining $21,000+ Fraudulent Covid PPP Loan For His Business - July 27,2026

In 2021, Damian Halfkenny, 54, was employed full-time as a Sergeant with the Massachusetts State Police earning $160,378 per year. He also owned and rented several real estate properties in Boston.

In March 2021, Halfkenny submitted a PPP loan application for his real estate business, falsely representing that he had a monthly payroll expense of $8,488. In support of this application, Halfkenny provided a fabricated IRS Schedule C. Based on his misrepresentations, the U.S. Small Business Administration issued Halfkenny, and later forgave, a $21,220 PPP loan.

Halfkenny was also ordered to pay a fine of $5,000, restitution in the amount of $21,333 and forfeiture of $21,333. (Source)

LAW FIRMS

No Incidents To Report

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Georgia Executive Housing Authority Director Charged For Role In $2.5 Million Fraudulent Invoicing Scheme & Kickbacks - July 14, 2026

Melanie Thompson, 55, is the former executive director of the Hinesville Housing Authority (HHA) in Georgia. Thompson and Toriono Byrd, 52, have been indicted on multiple counts of Wire Fraud and Conspiracy to Commit Wire Fraud.

Beginning as early as September 2019 and continuing through October 2023, while employed with the HHA, Thompson is alleged to have created or authorized false invoices, directed to Byrd's private business, which

authorized payments to Byrd for work that was never completed, or in amounts that far exceeded the actual value of the work. Upon receiving these payments, Byrd is alleged to have made return payments, or kickbacks, to Thompson for her personal use and benefit.

The indictment further alleges that through her role as executive director, Thompson directed multiple fraudulent payments to herself through the payroll system, directed payments of fraudulent bonuses to which she was not entitled, and that Thompson made false Covid-era loan applications to the federal government. In all, the scheme is alleged to have resulted in a loss of more than $2.5 million for the HHA. (Source)

2 County District Court Bookkeepers Sentenced To Prison For Stealing $979,000+ Over 5 Years / Used Funds For Gambling - June 30, 2026

2 former employees of the Wyandotte County District Court in Kansas received prison sentences for using their positions in the accounting office to steal taxpayer funds. The scheme resulted in a loss of $979,962 to the Wyandotte County District Court from 2018 to 2023.

Julia Roberts, 65, was the accounting supervisor and responsible for collecting and depositing funds into the Wyandotte County District Court's bank account.

She acted as Vicki Robinson's, 63, superior until her retirement in 2020. Roberts and Robinson stole incoming cash and concealed the thefts by generating checks and forging the clerk of court's signature. They fabricated information on the memo lines to make the checks appear to be judgment disbursements or other legitimate court business. The checks functioned as a way to conceal the missing cash in the system.

During the time they were stealing money, Roberts had a significant amount of money transactions at a casino — over $1 million in 2017, $480,000 in 2018, and $251,000 in 2019. The amount dropped when she retired in 2020 to $30,000. Roberts also deposited more than $80,000 in cash into her personal bank accounts from 2018-2020. Robinson deposited $20,000 in cash into her bank account from 2021-2023.

In August 2025, the Federal Bureau of Investigation (FBI) interviewed Robinson, and she admitted she stole money. She said Roberts showed her how to do it. Roberts told the FBI that she came up with the idea of stealing incoming cash. She said Robinson was involved from the beginning and at times they split the cash that was stolen. (Source)

County Parks Department Director Pleads Guilty To Receiving $400,000+ In Bribes For Contract Awards - July 8, 2026

Former Hudson County Parks Department Director Russell Fallacara pleaded guilty to conspiracy to commit honest services fraud.

From 2019 through 2024, the conspiracy involved more than $1.5 million in bribes and kickbacks. The payments were made by business owner William A. Murray, so that Murray's company would be awarded contracts to work on various Hudson County Parks Department projects, including but not limited to landscape maintenance, paving, and general contracting projects.

The bribes and kickbacks often came in the form of cash payments to Hudson County officials, including Fallacara and former Parks Department Director Thomas DeLeo. Fallacara received over $400,000 in cash bribes and kickback payments.

At other times, the bribes and kickbacks came in the form of free home repairs and renovations for both DeLeo and Fallacara.

In exchange for these bribes and kickbacks, at the time that each served as Parks Department Director, DeLeo and Fallacara each took official action to approve contracts awarded to Murray's company by Hudson County. (Source)

North Carolina Housing Authority Director Sentenced To Prison For Stealing $238,000+ Of Taxpayer Funds / Used Funds For House Renovation, Etc. - July 10, 2026

Debbie Woodell, 64, was sentence to two years in Federal prison, followed by three years of supervised release, for conspiring to commit federal program theft. Woodell was also ordered to repay $238,448 to the U.S. Department of Housing and Urban Development (HUD).

Woodell became the Executive Director of the Dunn Housing Authority (DHA) in 2014. DHA is a federally funded agency that provides affordable housing to qualifying low-income families, seniors, and individuals with disabilities in Dunn, North Carolina.

Between 2016 and 2021, Woodell exploited her position, working with others to steal more than $200,000 from DHA. As part of the scheme, she issued checks from DHA accounts to co-conspirators for unapproved landscaping and maintenance work that they never ever started.

She funneled most of the money back to her personal use. To carry out the fraud, she fabricated bid documents, created fake invoices, forged signatures, and provided false information to DHA's board of commissioners.

Woodell also misused DHA credit cards to make thousands of dollars in unauthorized personal purchases, including ATV gear and home renovations for her house. She concealed the theft by creating false receipts and altering DHA's accounting records. (Source)

Boston Housing Secretary Sentenced To Prison For $72,000+ Of Overtime Fraud - July 6, 2026

From 2017 to 2024, Helen Murray, 42, worked as an executive secretary at the Boston Housing Authority (BHA) as an executive secretary, Murray was responsible for collecting weekly BHA timesheets, as well as overtime forms from other BHA employees. Murray was also eligible to work overtime and receive overtime pay.

Murray's overtime work had to be pre-approved by her senior management. Specifically, Murray would have to perform the overtime work, accurately and truthfully fill out an overtime form and submit it to her immediate supervisor via email to be approved electronically.

However, in January 2023, Murray began submitting false overtime forms to BHA payroll. Instead of submitting the forms to her supervisor for approval, Murray entered overtime hours that Murray had not worked and then falsified her supervisor's signature on the form, without her supervisor's knowledge nor permission.

Murray would then submit the falsified overtime forms directly to BHA Payroll via email, after which BHA payroll would include Murray's fraudulent overtime pay in her weekly paycheck. In total, Murray submitted over 100 falsified overtime forms between January 2023 to August 2024 – ultimately collecting approximately $72,131 in fraudulent overtime pay. (Source)

Employee Working For State Agency Sentenced To Prison For Stealing $51,000 - July 28, 2026

Based on court documents, between October 1, 2021, and October 31, 2022, Hoggatt was employed with the Washington State Employment Security Department (ESD) as a Human Resource Consultant. Between May 16, 2024, and September 19, 2024, Hoggatt was employed with ESD as a Benefits Specialist.

While employed with ESD, Hoggatt filed false and fraudulent Paid Family Medical Leave Act applications in her own name and in the name of two family members setting out fictitious medical information and supported by documents with forged doctor signatures. Hoggatt also fraudulently applied for Washington State unemployment insurance benefits between October 31, 2022, and May 16, 2024, while not employed by ESD. Hoggatt falsely represented to ESD that she was unemployed during this period, but she was in fact employed in California. Through her false submissions, Hoggatt stole $51,403 from Washington State's Paid Family Leave and Unemployment Insurance programs. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School District Financial Officer Charged For Stealing $1 Million - July 3, 2026

Kristi Williams was the manager of Property Tax Administration at Tomball Kristi William (Texas) from January 2018 until November 2023 and oversaw the collection of local property taxes.Williams has been charged with wire fraud after allegedly stealing approximately $996,174 from Tomball Independent School District.

The charges allege that when a taxpayer paid in cash, a tax office employee would place it inside an envelope and record the payment in specialized software as part of a batch.

Once the amounts reached a certain threshold, either $15,000 or $20,000, the batch was closed and Williams was expected to deposit the money into Tomball ISD's bank account. Williams allegedly used the software to reverse the payments in the system and kept the funds for her own personal use. (Source)

DC Public Schools Administrator Pleads Guilty To Issuing Fraudulent Purchase Orders & Accepting $30,000 In Cash Bribes - July 9, 2026

Tracy Hatton, 60, was an administrative officer for McKinley, a unit of the District of Columbia Public Schools, and was responsible for managing the school's supply budget, selecting and awarding vendor contracts, and approving invoices for payment.

Beginning in or about October 2020 and continuing until about September 2023, Hatton accepted cash bribes from a contractor identified in court papers as Contractor 1, the owner of an approved D.C. Supply Schedule vendor, in exchange for using her official position to benefit that vendor.

In exchange for the bribes, Hatton issued purchase orders to the contractor and approved payment for goods that were never delivered to McKinley, including fraudulent invoices for inflated and under-delivered orders. Hatton also directed the contractor to fraudulently charge her government-issued purchase card for supplies that were never provided. On some occasions, Hatton accepted additional cash payments from the contractor that did not derive from fraudulently obtained DCPS funds, in exchange for steering additional business to the contractor.

In total, Hatton personally profited by at least $30,000. Because the payments to Hatton were made in cash, the total loss to D.C. Public Schools is difficult to identify. Hatton pleaded guilty to bribery on Nov. 10, 2025. Sentencing is set for Nov. 5, 2026. (Source)

Professor At University Rawls College Of Business Pleads Guilty To Running Fentanyl Distribution Network - July 7. 2026

Daniel Taylor, 51, was charged in February 2026 with conspiracy to possess with intent to distribute fentanyl. On July 1, 2026, he pled guilty to conspiring to distribute more than 40 grams of fentanyl.

During the entire scope of the conspiracy, Taylor was employed as an assistant professor of marketing and supply chain management at the Texas Tech University Rawls College of Business. He admitted in court documents that his educational background and expertise in supply chain management helped to further or advance his fentanyl distribution network. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Union President Pleads Guilty To Stealing $290,000 / Used Funds For Personal Expenses, Restaurants & Travel - July 6, 2026

Between 2003 and 2023, Kye Carbone served as the President of United Federation of College Teachers Local 1460 in New York. The union represents faculty members at the Pratt Institute in Brooklyn, New York.

Carbone pled guilty to stealing over $290,000 from the Local between 2011 and 2023, Carbone used the money for his personal expenses, restaurants, and travel. In 2023 Carbone was voted out of office. (Source)

Labor Union Treasurer Pleads Guilty To Embezzling $94,000+ / Used Funds For Personal Expenses - July 1, 2026

Clarence Penny, 40, served as the Treasurer for the Steelworkers, AFL-CIO, Local 09 333 Chapter of the United Steelworkers International Labor Union in Florida, from May 2015 to October 2023.

Between January 2020 and May 2023, the defendant wrote 66 unauthorized checks to himself from the Union's bank account, and he used those fraudulently derived proceeds on personal expenses. In total, the defendant stole $94,586.53. Penny also provided fake account balances and false statements on annual financial reports in 2020, 2021, and 2022, to conceal his ongoing theft of funds. (Source)

Labor Union Financial Secretary Sentenced To Prison For Embezzling $40,000+ - June 30, 2026

From July 2022 through October 2023, James Burke, 56, was the financial secretary of a labor organization located in Huntington, West Virginia.

Burke admitted that he issued nine unauthorized or altered checks payable to himself and improperly withheld portions of checks payable to the labor organization as cash when he deposited them. Burke also admitted that he diverted six dues checks payable to the labor organization for his personal use. The total amount of money stolen by Burke from the labor organization was $40,011.46. (Source)

BANKING / FINANCIAL INSTITUTIONS

2 TD Bank Employees Sentenced To Prison For $92 Million Money Laundering Scheme & Accepting Bribes - July 16, 2026

Wilfredo Aquino, 47, leveraged his position as a TD Bank assistant store manager to facilitate a money laundering network's movement of hundreds of millions of dollars through TD Bank accounts from 2019 to February 2021.

During that time, the leader of the money laundering network, Da Ying Sze, also known as David, and his co-conspirators moved approximately $474 million through TD Bank accounts by depositing cash at TD Bank stores in New York, New Jersey, and elsewhere. In February 2022, David pleaded guilty to coordinating a $653 million money laundering conspiracy, operating an unlicensed money transmitting business, and bribing bank employees in connection with financial transactions.

During David's money laundering scheme, Aquino processed approximately 1,680 official bank checks at TD Bank for David and his co-conspirators, totaling more than approximately $92 million.

Nearly all of these bank checks were funded with a corresponding cash deposit exceeding $10,000, which triggered TD Bank's legal requirement to file a currency transaction report (CTR). Although Aquino knew that David was conducting these cash deposits, Aquino never identified David as the "conductor" on the CTR.

Aquino also knew that TD Bank had closed other accounts linked to David for suspicious activity; one colleague even warned Aquino that David's activity "looks like money laundering." In February 2021, Aquino facilitated three of David's money laundering transactions, totaling almost $2 million in cash, in a third party's account. He failed to report David as the conductor of the transactions, thus concealing David's role in the money laundering scheme.

Aquino accepted numerous retail gift cards from David totaling over $11,000 in return for his facilitation of this scheme, including for the three transactions in February 2021.

From January 2021 through May 2021, Edward Low, 31, accepted bribes and leveraged his position as a TD Bank retail employee to fraudulently obtain confidential customer information that he passed to outside co-conspirators, who used it to take over accounts and steal money from customers. Low also processed some of their illicit transactions. In total, Low received at least $26,700 in bribes and facilitated $484,572.16 in fraud at TD Bank.

Then, from May 2022 through August 2022, while employed at another financial institution, Low accepted a bribe to falsify bank records to open an account in the name of a shell company. Low's co-conspirators then used that account to commit at least $47,195 of fraud. (Source)

Bank Chief Financial Officer Sentenced To Prison For $4.3 Million+ Bank Loan Fraud Scheme - July 17, 2026

Aaron Luneke, 44, abused his position as Chief Financial Officer at his bank, and was sentenced on to prison for committing bank fraud and attempted bank fraud in connection with loans he sought to build and operate a car wash in Columbus, Nebraska.

Luneke attempted to defraud Stearns Bank by using fraudulent and inflated contractor invoices to artificially inflate the valuation of the car wash property in pursuit of a $3.5 million refinancing loan. Further evidence at trial established that Luneke failed to disclose significant personal debts owed to family members in connection with the Stearns Bank loan application.

The jury also found that Luneke the bank by submitting fraudulent and inflated invoices from contractors as the basis for additional construction loan proceeds, obtaining two loans totaling approximately $4,320,000. (Source)

Citibank Employee Pleads Guilty To $463,000+ Of Wire Fraud & Identity Theft / Used Funds For Jewelry, Travel, Etc. - July 6, 2026

In 2022, Lexus Lewis obtained employment at Citibank in its fraud department by using another person's identity.

From approximately November 2022 through April 2023, Lewis used her position to obtain customers' credit card numbers, which she would then fraudulently use to purchase items such as jewelry or furniture, pay for her own living expenses or travel, or pay other individuals' rent in exchange for a cash payment.

When ultimately confronted by law enforcement, Lewis admitted to her conduct. Lewis agreed to forfeit $463,619, the proceeds of the charged criminal conduct. (Source)

Citizens Bank Manager Sentenced To Prison For Embezzling $374,000+ - July 16, 2026

Jefry Castro, 34, worked as the manager of the Citizens Bank branch in Tewksbury, Massachusetts.

Between May 2024 and August 2025, Castro embezzled $374,233 from the bank. Castro embezzled the money primarily by taking cash from two ATMs at the bank. He covered his theft by moving money from cash deposits and cash shipments to the bank to replace the cash in the ATMs. Castro also changed numbers on the bank's balance sheets to falsify the total amount of cash at the bank. (Source)

Bank Employee Pleads Guilty To Stealing $50,000 / Used Funds For Investment Purposes - June 29, 2026

On March 11, 2022, Jordan Hennessy, 38, was working as the commercial relationship manager for First Interstate Bank in Billings, Montana.

From work, Hennessy submitted a commercial loan application for $100,000 under the name of his father's business, Stillwater Group, LLC. In the application, Hennessy stated Stillwater Group would use the funds to develop real estate projects in Montana. He then opened a checking account, naming his father as a joint owner, on March 14, 2022.

Hennessy, as a First Interstate employee, was responsible for negotiating the counteroffer to his own loan request, which resulted in a $50,000 line of credit being issued to Stillwater Group. His position allowed him to be on both sides of the transaction, negotiating with himself.

Once the $50,000 line of credit was funded, Hennessy transferred the Stillwater Group funds from the joint account he created with his father's name into his personal checking account. Hennessy then used the funds to finance several transactions with an internet-based investment company and eventually defaulted on the $50,000 line of credit. (Source)

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

Pharmacist Working For National Pharmacy Chain Charged With Drug Diversion For Himself - July 29, 2026

Joshua Bradley, 30, was charged with five counts of acquiring a controlled substance by fraud, deception and subterfuge. While working as a licensed pharmacist at a national pharmacy chain, Bradley allegedly diverted various quantities of Dextroamp-amphetamin for his own use on four occasions in August, September and November 2024. Additionally, on Nov. 10, 2024, Bradley is alleged to have also diverted Adderall. These controlled substances originally were intended for customers. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

When Your Trusted KPMG Senior Partners / Internal Auditor Are An Insider Threat To Your Business - June 24, 2026

NOTE:

Preventing and mitigating Insider Threat starts with senior leadership following the rules. This is a perfect example of where senior leaders did want they wanted and lost a big client and possibly others. This incident shows how a single whistleblower completely brought down a multi-billion dollar corporate empire in less than 48 hours. This is the structural collapse of KPMG Australia.

WHAT HAPPENED?

The most serious whistleblower claim from the KPMG scandal, that senior partners had illicitly accessed sensitive Lendlease board documents and kept them in a work locker, has been confirmed and led to the immediate expulsion of former chief operating officer, Eileen Hoggett.

"I can confirm that the ongoing investigation by external law firm Allens has uncovered new evidence that supports the whistleblower's allegation that confidential client information was kept in a locker at KPMG's Sydney office," a spokesman for KPMG said.

KPMG Australia CEO John Sams has taken immediate action to expel a partner from the firm," the spokesman said. "To say I am angry about this is an understatement. The conduct was totally unacceptable, and it is unacceptable that it has taken so long for us to get to this point," Sams told partners.

KPMG said the investigations into the whistleblower allegations, which have thrown the firm into turmoil in recent months, remain ongoing. KPMG has updated impacted clients and the relevant regulatory and professional bodies.

Kim Lawry was one of KPMG's senior audit partners and a member of its board until last week. Hoggett had already resigned over the scandal but had yet to leave the firm. She would have left with a significant retirement benefit – expected to exceed a million dollars – if that had proceeded. Former KPMG boss Andrew Yates, who resigned over the scandal in May, received a retirement payment of $2.4 million, including $1.7 million in lieu of notice. The scandal has also led to the resignation of former chair Martin Sheppard and other partners and is expected to trigger hundreds of staff cuts as clients and government are expected to withdraw their business with the firm.

The Lendlease allegation was at the core of the whistleblower claims that senior KPMG staff had shared data from blue-chip clients in order to win new business.

"It is very clear that, having provided our external auditor with all the normal access they require to Lendlease's books and records, there has been a fundamental breach of trust whereby our auditor's access to those books and records has been gravely misused," Lendlease chairman John Gillam told a parliamentary hearing in June. **The company is preparing to dump KPMG as its auditor**. (Source)

Apple Sues OpenAI & 2 Former Employees Over Alleged Trade Secret Theft Tied To AI Hardware - July 13, 2026

Apple has filed a lawsuit in the U.S. District Court for the Northern District of California accusing OpenAI, its hardware subsidiary io Products, and two former Apple employees of misappropriating trade secrets related to the development of OpenAI's planned consumer AI hardware.

The complaint alleges OpenAI engaged in a coordinated effort to obtain Apple's confidential information as it accelerated work on its hardware ambitions following its acquisition of Jony Ive's startup io Products for approximately $6.5 billion.

Apple named the OpenAI Foundation, OpenAI Group PBC and io Products as defendants, along with OpenAI Chief Hardware Officer Tang Tan and former Apple engineer Chang Liu.

In the filing, Apple alleged that OpenAI and its employees took "illegal shortcuts" to develop AI hardware.

"This much is clear, however: at every level, from members of its Technical Staff to its Chief Hardware Officer, and in coordination with business partners, OpenAI has been stealing Apple's trade secrets and confidential information," the company said in the filing.

The lawsuit claims Liu failed to return a company-issued MacBook after leaving Apple and exploited an authentication flaw to regain access to Apple's internal cloud storage, where he allegedly downloaded thousands of confidential hardware documents.

Apple further alleged that Tang Tan, who spent 24 years at Apple before joining OpenAI, instructed Apple employees interviewing with OpenAI to bring unreleased Apple components and prototypes to interviews for "show and tell" sessions.

According to the complaint, OpenAI also sought access to Apple's manufacturing know-how by misleading one of Apple's industrial design partners into believing it had permission to replicate a proprietary metal-finishing process for OpenAI devices. Apple additionally alleged that OpenAI has recruited more than 400 former Apple employees for its hardware division.

OpenAI denied the allegations. "We have no interest in other companies' trade secrets. We remain focused on building innovative technology that empowers people everywhere," an OpenAI spokesperson said in a statement. (Source)

Former Employee Of LG Display Sentenced To Prison For Stealing Trade Secrets For OLED Display & Providing To Chinese Company - July 26, 2026

According to legal sources, the Criminal Agreement Division 34 of the Seoul Central District Court sentenced a person surnamed Yoon and a person surnamed Han, who were indicted on charges of violating the Industrial Technology Protection Act, to five years in prison and a fine of 40 million won, and two years in prison and a fine of 10 million won, respectively. A person surnamed Park, who was indicted alongside them, was sentenced to one year in prison, suspended for two years.

Yoon and Han joined LG Display in 1996 and 2000, respectively, and worked there before moving to a Chinese company in 2021.
In Oct. 2020, while still at LG Display, Yoon was brought to trial on charges of conspiring with Han to photograph with a smartphone and leak state core technology, including design drawings of LG Display's Guangzhou, China, plant. Yoon was found to have carried out the crime to use it after moving to a Chinese company that is a competitor.

After changing jobs, Yoon was found to have asked Han to leak trade secrets obtained through Park. Han, who conspired in the crime, was found to have even attempted to destroy evidence during the investigation. (Source)

Colorado Behavioral Healthcare Provider Discovers Employees Downloaded Personal Information On 7,000 Clients - July 23, 2026

NAS Recovery Solutions, a Lakewood, Colorado-based substance use disorder treatment and behavioral health services provider, has announced a data breach affecting up to 7,000 current and former clients. According to the company’s breach notice, this was an insider breach rather than a hacking incident. The company learned on May 13, 2026, that certain workforce members had downloaded client data without authorization.

The investigation revealed only limited information had been copied, such as first and last names, dates of birth, and telephone numbers; however, since NAS Recovery Solutions is a substance use disorder (SUD) treatment provider, it could be inferred that the individuals were receiving SUD treatment. There are no indications that any other information was obtained by the workforce members. The breach notice does not provide any clue as to why that information was obtained.

NAS Recovery Solutions said it has reviewed workforce access and security controls and is implementing additional safeguards to prevent similar incidents in the future. Additional training has been provided to the workforce on HIPAA and patient privacy, and appropriate corrective action has been taken against the workforce members involved. The sanctions imposed were not disclosed in the notice. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

OpenAI Insider Incident - Out Of Control Autonomous AI Agent - July 23, 2026

When news emerged that an OpenAI model had escaped its evaluation environment, exploited vulnerabilities, and reached Hugging Face's production infrastructure, much of the discussion focused on the sophistication of the exploit. That is understandable but it misses the far more important lesson. Hugging Face is a popular online platform and community for artificial intelligence, often called the "GitHub for Machine Learning". It lets people share AI models, data, and tools.

Security professionals watched an AI agent independently identify an opportunity, formulate a strategy, adapt to obstacles and pursue its assigned objective through a path its designers never sanctioned. The goal itself wasn't destruction or data theft, solving the evaluation was exactly what the model had been asked to do. It was optimizing to obtain that evaluation's answer key, having inferred it was likely stored elsewhere. That reasoning led it beyond the boundaries of the environment built to contain it.

Unlike human attackers, AI agents do not become tired, distracted or discouraged. They can execute thousands of hypotheses simultaneously, continuously learn from failure and optimize towards an objective without emotional bias or fatigue.

Perhaps most importantly, they do not think in terms of attacks. They think in terms of goals. If an objective is to obtain privileged access, the AI simply evaluates every possible route until one succeeds.

Human defenders often assume certain pathways are unlikely to be discovered. Autonomous AI makes no such assumptions. If a path exists, eventually it will find it.

Traditional attackers are constrained by time, resources and expertise. AI is constrained only by computing power. Imagine thousands of autonomous agents simultaneously analyzing identity relationships, cloud permissions, service accounts, APIs, CI/CD pipelines, SaaS integrations and exposed management interfaces. Each attempt slightly different combinations. Each learns independently. Eventually, one succeeds.

The Hugging Face incidents showed that an autonomous AI agent behaving like an insider, using reasoning, adapting and pursuing objectives beyond its intended operational boundaries, could execute any action it wanted to. (Source)

NOTE:

While there are many advantages to AI systems, the are also many risks and threats that ANY organization or business that is considering implementing an AI system, or has implemented an AI system should be aware of.

The example above clearly shows that ALL AI agents and their actions need to be governed, constrained, accountable and monitored, in addition to monitoring what types of data employees are uploading into AI systems, and the prompts they are injecting into AI systems.

If you don't have visibility of your AI agents, this is no different than an out of control employee doing whatever they want on their employers computer systems and networks. Imagine not monitoring your computer systems and networks for employees actions that could harm the organization in many different ways. The organization would essentially be blind as to their employees actions.

In today's business environment, technology is now a core competency that drives the success of the business. Technology drives the mission of the business, revenue, advancement and growth, customer satisfaction and much more. **Unfortunately rogue AI agents and malicious Insiders can also use technology in many ways that can severely impact an organization. The survivability of your business could be in serious jeopardy if you have rogue AI agents doing whatever they want.**

26 Meta Workers Are Suing Over alleged AI Aided Layoffs Targeting Employees On Medical Or Family Leave - July 15, 2026

A group of 26 Meta employees has sued the company, claiming it used artificial intelligence systems to select people for layoffs, disproportionately targeting those on medical, parental or family leave.

They are among the 8,000 employees, or about 10% of its workforce that Meta said it would lay off starting in May. In an internal memo to employees in April, the company said the cuts would be aimed at making the company more efficient and offsetting its other investments.

The lawsuit claims the company used internal AI systems, keystroke and activity-monitoring data, AI token-usage dashboards and algorithmically assisted performance rankings, among other methods, to determine who would be laid off.

Many of these scores and ratings "by design, cannot be accumulated by an employee who is on protected medical or family leave, or whose output is reduced by a disability," the lawsuit says. Meta, according to the lawsuit, did not account for protected leave when taking employees' scores into account and "did not pause the system for the individualized, leave- and accommodation-neutral review that the law requires."

As a result, people on protected medical or family leave were disproportionately selected for layoffs, the lawsuit says.

Each of the 26 anonymous employees in the lawsuit took protected leave and requested or received a reasonable accommodation for disability. Though they have been notified of their layoffs, all 26 remain employed by Meta, with separations set to begin July 22.

Many of the employees in the lawsuit took pregnancy or parental leave, during which time they wouldn't have worked and thus had their measured output reduced. Others took medical leave — one disclosed a "serious health condition and disability" that was approved by Meta's own provider. But according to the lawsuit, he was "discouraged and deterred from taking that leave by a manager" who warned that doing so would result in his selection for the anticipated layoffs. Meta offered no accommodation for his disability, the lawsuit says.

The lawsuit says the layoffs violated several state and federal laws, including the Family and Medical Leave Act, the Americans with Disabilities Act, the Pregnancy Discrimination Act and the Pregnant Workers Fairness Act. (Source)

xAI Artificial Intelligence System Was Secretly Sending Entire History Of Users Projects To Company Servers - July 15, 2026

xAI, the company founded by Elon Musk, has announced emergency measures following a serious controversy involving the unauthorized uploading of users' private code and confidential information to a server via the Grok Build CLI tool. Musk stated that, for security reasons, all previously uploaded user data will be permanently deleted. This decision was made after it was discovered that the AI tool was secretly sending the entire history of projects to the company's servers.

The issue was identified by a cybersecurity expert under the pseudonym Cereblab. By analyzing the network traffic of Grok Build version 0.2.93, he proved that the program sent not only files relevant to the request but entire Git repositories, including their change history, to Google Cloud storage. The researcher observed that when sending a simple request in a 12 GB project, the system uploaded 5.1 GB of data to the server. (Source)

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

No Incidents To Report

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

No Incidents To Report

INSIDER TRADING / STOCK TRADING & SECURITIES FRAUD

Employee Sentenced To Prison For Insider Trading Scheme That Resulted In $2.38 Million+ In Of Profits - July 7, 2026

Justin Chen was previously employed at an EDGAR filing company and was responsible for reviewing draft securities filings before they were filed on the Securities and Exchange Commission's EDGAR filing system.

Chen misused material non-public information taken from his employer to trade in the securities of 13 publicly traded companies, making at least $2.38 million in profits. (Source)

2 Auto Engineers Working For Volkswagen Subsidiary Charged With Insider Trading About Rivian-Volkswagen Joint Venture / Made $300,000 In Profits - July 24, 2026

Between April and July 2024, Michael Stamp and Marcus Plank engaged in a scheme to trade in the securities of Rivian Automotive, Inc. based on material nonpublic information concerning a multibillion-dollar joint venture between Rivian and Volkswagen Group.

Stamp and Plank were employees of a Volkswagen subsidiary and worked in the United States on temporary assignment form Germany. Through their positions, they gained access to confidential, nonpublic information concerning Volkswagen's ongoing negotiations with Rivian about a potential joint venture. Despite owing duties of trust and confidence to their employer, Stamp and Plank began purchasing options and equity positions in Rivian shortly after learning of the joint venture discussions. On June 25, 2025, Rivian and Volkswagen publicly announced their joint venture, and Rivian's share price rose 23% the following day. Stamp and Plank then sold their Rivian positions, with Stamp realizing approximately $250,000 in profits, Plank realizing at least approximately $50,000 in profits, and Plank's close family member realizing approximately $12,000 in profits. Stamp and Plank understood their actions were illegal.

For example, eight days prior to the announcement of the joint venture, Stamp searched "statute of limitations insider trading," and following the announcement Plank's close family member searched, in German, "how is insider trading prosecuted?" (Source)

Lawsuit Filed Against Former Executive For Stealing Trade Secrets & Providing To Competitor Causing Substantial & Irreparable Financial Loss - July 23, 2026

A former Zimmer Biomet Holdings executive with a $400,000 annual salary and unlimited access to confidential information is being accused of spilling those secrets to a competing orthopedics company.
Goson had been with the company for almost 20 years.

Kristoff Goson also is accused of peddling another company's products during sales calls to Zimmer Biomet customers, sending internal company documents to his personal email account and violating his noncompete agreement.

Those are among the allegations against Goson outlined in Zimmer US Inc.'s lawsuit, which was filed late last week in the U.S. District Court Northern District of Indiana.

Goson's employment was terminated for cause on March 12 after Zimmer Biomet conducted an internal investigation into allegations that its newly promoted vice president of commercial transformation was engaged in a side hustle that violated terms of his employment, according to the filing. During the investigation, officials found that Goson had download thousands of files containing sensitive trade secret information on at least seven non-Zimmer Biomet devices.

Less than four months after being fired, Goson was named CEO by Pixee Medical Inc., a French company that sells orthopedic products. Zimmer Biomet is asking the court to order Goson to resign from that position.

The orthopedics giant designs and manufactures artificial hips and knees, among other body parts, and the surgical instruments used to implant them. Goson was privy to the company's business strategies, product research and development, pricing information, financial performance and customer contacts in his various vice president positions. That information "would be extremely beneficial to a competitor," the filing said. Included in the trove of company secrets was Zimmer Biomet's strategy and analysis of the ambulatory surgery center market, "a market which is no doubt a key target Pixee is trying to penetrate" due to the significant increase in orthopedic surgeons performing operations in those settings.

Zimmer Biomet's lawsuit asks the court to award damages, including compensation for the cost of the internal investigation and legal fees. But the filing doesn't suggest a total amount. Instead, it describes the effects on its business as a "substantial and irreparable financial loss." (Source)

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING /

Chief Financial Officer Pleads Guilty To Laundering $67 Million Of Organizations Funds - July 10, 2026

From 2019 through May 2024, Weidong Guan, while serving as Chief Financial Officer of the Epoch Times In New York, conspired with others to participate in a sprawling, international scheme to launder at least approximately $67 million of illegally obtained funds to bank accounts in the names of the Epoch Times and related entities.

Guan did so by using the Epoch Times' funds to purchase crime proceeds loaded onto gift cards and prepaid debit cards at discounted rates of approximately 70 to 80 cents on the dollar, and then laundering those crime proceeds back to the Epoch Times under the guise of fake "donations" to the Epoch Times.

When banks notified Guan that the transactions at issue were suspicious and asked Guan to explain their source, Guan knowingly misled the banks to believe the transactions were legitimate rather than criminal. (Source)

Company Financial Controller Charged For Forging Coworkers' Signatures To Steal $753,000+ From Employer Over 8 Years - June 30, 2026

Shania Shanahan, 39, is the former controller at an agricultural cooperative in Colby, Kansas that provides grain and fuel services to its members. She supervised the accounting department, and her duties included processing and making payments, reconciling bank accounts, and making entries into the general ledger for purchases and expenses.

Between January 2017 and November 2025, Shanahan is accused of forging 233 checks for approximately $753,575 from the co-op's account and depositing the funds into her personal bank account. She allegedly used coworkers' signatures without their knowledge or consent which is the basis for the identity theft charges. She is accused of concealing the deception by falsifying records to make the fraudulent payments appear to be legitimate payments to herself and other third-party vendors. (Source)

Company Financial Manager Sentenced To Prison For Embezzling $538,000+ Over 3 Years - July 17, 2026

An investigation conducted by the FBI determined that between 2018 and December 2022, Tamara Ricceri-Wolf, 60, was the Financial Manager for an Omaha company. She had access to the company's financial information and bank accounts.

Beginning in 2019 and continuing through at least 2022, Ricceri-Wolf devised a scheme to defraud or to obtain money from the Omaha company, which involved opening American Express credit cards in the name of both the company and company's owner without knowledge or authorization. After opening the American Express credit cards, Ricceri-Wolf made personal purchases using the credit cards for her own benefit and without authorization. Ricceri-Wolf would use her position as a Financial Manager to make payments from the company's bank accounts on balances associated with the American Express credit cards. Ricceri-Wolf caused to be made approximately 106 unauthorized payments to American Express totaling at least $538,428.26. (Source)

Employee Working At 2 Financial Institutions Charged For Stealing $440,000 - July 10, 2026

Between July 2019 and April 2022, Joshua Shore was an operations manager of the cash vault for a nationwide bank. The facility was located in Tukwila, Washington.

On December 6, 2021, Shore allegedly stole approximately $40,000. On January 28, 2022, Shore allegedly stole an additional $100,000.

The next ten counts of the indictment detail how Shore allegedly sought to launder the stolen funds by making repeated $3,000 cash deposits of hundred-dollar bills into ATM's for the local bank where he had his personal accounts. Ultimately, Shore moved the funds from his bank to another financial institution – another count of money laundering.

From September 2023-December 2025, Shore was employed as a Market Manager at a financial institution in Renton. The indictment alleges that on the eve of the Columbus Day/Indigenous People's Day (the start of a bank holiday), Shore stole $300,000 from the vault. The next 16 counts describe how he deposited cash up to $10,000 at a time via ATMs into his personal bank account at a different financial institution. (Source)

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

2 Security Business Employees Charged For Embezzling $11 Million Dollars Of Money That Was Being Held For Bank / Used Funds For Luxury Lifestyle - July 27, 2026

The Chief Operating Officer for a security business was charged for his role in embezzling $3 million from a business and bank fraud for the loss of $9 million that the company held in trust for a bank. Another employee was charged, who was the Deputy Director of the business for his role in embezzling over $2 million.

In 2017, Robert Cormier started Erigere Rapidus Solutions, Inc. (ERS), a security services business. In late 2019, ERS entered into an agreement with a local bank to collect, count, transport, store and deposit cash on behalf of a bank at the Federal Reserve Bank in Philadelphia. ERS's employees, including Richard Eisler, were responsible for picking up cash from various customers of the bank, counting the cash at ERS's office, and providing accurate daily reports of the cash to the bank. Those reports were supposed to reflect accurately the cash that ERS had collected on behalf of the bank. Cormier was responsible for providing the bank accurate information about the daily balance of cash in ERS's vault, including cash transactions coming in and out of ERS, the denominations of each of the transactions, and the ending balance of bank's cash that was being stored

by ERS. The bank relied on the reports from ERS to appropriately credit the relevant customers' accounts for the cash that had been collected by ERS on behalf of the bank.

After picking up the cash from the bank's customers, ERS stored the cash in a vault at ERS's office in New Jersey, until it could be deposited in the Federal Reserve Bank in Philadelphia, Pennsylvania for deposit on behalf of the bank.

From March 2019 to September 2022, ERS collected, counted, stored, transported, and deposited millions of dollars in cash for the bank. On a daily basis, ERS stored cash in its vault, in varying amounts ranging from $1 to $12 million. At the time that the bank ended their relationship with ERS, the bank determined that over $8 million was missing from the vault.

Beginning in 2020 and continuing until 2022, Cormier took various amounts of cash out of ERS's vault, which cash belonged to the bank, without authorization by the bank. Cormier embezzled and stole at least approximately $3 million.

Cormier used the embezzled funds to: pay cash payroll for employees at ERS; pay invoices for the installation and monitoring of security systems at various businesses; pay for the installation of security systems in the ERS Offices and vehicles; pay for ERS company vehicles; deposit, and caused to be deposited, cash into ERS's bank accounts; and pay personal expenses for himself and his family members, including, among other things, the installation of a deck and a pool, and household renovations.

Beginning in 2020 and continuing until late 2021, Eisler took various amounts of cash belonging to the bank out of ERS's vault without authorization by the bank. Eisler embezzled and stole at least approximately $2 million of this money. Eisler used the embezzled funds to pay personal expenses for himself and family members and deposit cash into his personal account, joint accounts, or his family members' bank accounts. The funds were used to purchase luxury vehicles, such as an Audi RS7, Audi R8, Porsche 911, Ford F450 truck, Dodge Durango, Harley Davidson motorcycle, and a recreational vehicle. Eisler also used the funds to pay for his wedding rings, wedding reception, a roof on his residence and to pay off an automobile loan. (Source)

Company Accounting Manager Pleads Guilty To Embezzling $3.2 Million+ / Used Funds For Gambling, Student Loan Debt, Etc. - June 30, 2026

A Kyle man pleaded guilty in a federal court in Austin to embezzling more than $3.2 million from his former employer, Austin Freight Systems (AFS), announced U.S. Attorney Justin R. Simmons for the Western District of Texas.

Mitchell Slentz, 34, was in charge of accounting operations at Austin Freight Systems (AFS), overseeing all accounting activities, financial reporting and internal controls, including submitting requests to JP Morgan Chase Bank to make payments to AFS's vendors.

Beginning no later than October 2023 and continuing at least until about March 2025, Slentz fraudulently misappropriated money from AFS through 147 payments, and deposited approximately $3,277,937.35 into his personal bank accounts through the use of interstate wire communications.

Using the criminally derived money, Slentz paid $25,000 on July 24, 2024, and $33,887.83 on Sept. 3, 2024, for student loan debt.

Additional fraudulent activities were revealed through financial analyses of several of Slentz's accounts. Furthermore, Slentz gambled extensively on an online gambling platform, depositing and/or winning more than $1 million through online gambling. (Source)

Company Chief Financial Officer Pleads Guilty To Embezzling $1.5 Million+ Over 4 Years / Used Funds For Purchases At Retails Stores - July 7. 2026

Cindy Babbitt, 57, was the Chief Financial Officer (CFO) of an audio visual and information technology company in Virginia. As the CFO, Babbitt had access and control of the company's bank accounts, including a business checking account. From

December 2018 through December 2022, Babbitt used fraudulent checks, payroll, and wire transfers to embezzle $1,561,841.30 from the company.

Babbit issued at least 44 checks totaling $82,117 that were drawn on the company's checking account, made payable to her and her husband, signed by Babbitt as the authorized representative of the company, and deposited by Babbitt into her own bank account. Babbitt fraudulently initiated and approved 49 reimbursements totaling $142,401 through payroll to herself. Babbitt fraudulently caused at least 428 wire transfers totaling $1,337,323.30 from the company's business checking account to her personal bank account.

None of these transactions were made for any legitimate business expenses. Babbitt used the fraud proceeds for purchases at retail stores such as Tiffany & Co., Saks Fifth Avenue, Versace, Burberry, Balmain, Cartier, and Louis Vuitton. (Source)

Restaurant Manager Sentenced To Prison For Embezzling $1 Million+ / Used Funds For Clothing, Travel, Etc. - July 21,2026

Matthew Braasch, 48, pleaded guilty in April to one count of wire fraud. He admitted that while a manager of a restaurant in Grantwood Village, in St. Louis County, Missouri, he misused the company credit card to make personal purchases.

Braasch was supposed to only use the company credit card for food and to pay state liquor and other taxes. Instead, Braasch spent $81,965 at Target, $29,801 at the Vineyard Vines clothing store, $39,634 at Amazon and over $10,000 on local hotel stays for an acquaintance.

Due to the embezzlement, the restaurant lacked money to buy food and pay state taxes. During a state investigation, Braasch posed as the restaurant's owner to conceal his crime, his plea says. Braasch began stealing to enrich himself during the pandemic, when many restaurants struggled and closed. The judge ordered Braasch to repay the money (Source)

Company Financial Controller Pleads Guilty To Embezzling $1 Million+ / Used Funds To Purchase Ford F-150 Pickup Truck - July 8, 2026

Jacob Wise, 29, pleaded guilty to orchestrating a scheme that caused over $1.1 million in losses to the business where he worked. He also pleaded guilty to one count of laundering the proceeds of his crimes.

Wise admitted to devising and executing a scheme to order and to divert the company's funds to bank accounts he controlled. The accounts appeared to be legitimate vendors for the company. In reality, Wise himself controlled the accounts and used the diverted funds to make purchases, including a Ford F-150 pickup truck, which agents seized as part of the investigation. (Source)

Non-Profit Organization IT Director Sentenced To Prison For Theft Of $543,000+ Using Organizations Credit Cards / Purchased Camera Equipment, Gift Cards, Etc. - July 21,2026

Michael Meenan, 60, served as the Director of Information Services for an Indianapolis-based non-profit organization from 1999 to 2021. In that role, he was responsible for purchasing technology equipment using an employee credit card.

Starting as early as July 2007, Meenan abused his position of trust by making personal purchases with his company-issued credit card. These unauthorized purchases included DSLR cameras, lenses, Apple and Southwest Airlines gift cards, cycling equipment, and Amazon gift card balance reloads. He then used the reloaded balances to acquire additional photography and cycling items for his personal use. Meenan even posted photos of some of these items on social media.

To hide the fraudulent transactions from management and accounts payable staff, Meenan created doctored receipts that falsely described the personal items as legitimate technology purchases.

For example, he altered a receipt to indicate he had bought $1,100 worth of "Uninterruptible Power Supply Units (UPS)" for the organization, when in reality he had simply reloaded an Amazon gift card with that amount.

In total, Meenan executed approximately 1,173 unauthorized transactions using his employee credit card, resulting in a financial loss of $543,521.13 to the organization. He was also ordered to pay $543,521 in restitution. (Source)

Employee Of Construction Company Sentenced To Prison For Embezzling $500,000+ / Used Funds To Pay Credit Cards, Gambling, Travel, Car Loan - July 23, 2026

Christina Mobley admitted that she directed checks mailed from the company's bank account to be applied to the account for her personal credit cards to pay for personal expenses such as cash advances at casinos and personal travel; issued electronic payments of company funds to her personal credit cards; wrote checks from the company to herself, including for the repayment of her car loan; and inflated her vacation time, work hours, and bonuses in the company's payroll system, resulting in unearned and excessive payments to herself.

Between January 2022 and November 2024, Mobley admitted that she embezzled more than $500,000 from her employer. (Source)

Employee Sentenced To Prison For Embezzling $385,000+ From Her Employer Causing Severe Impacts / Used Fund To Pay Husband & Personal Expenses - July 17, 2026

From approximately May 2017 through April 2020, Charity Felch, 48, embezzled at least $385,930 from her employer, Rodeo Electrical Services, by fraudulently paying herself and her husband, using company funds for personal expenses, and concealing the theft through fraudulent financial transactions. Felch also engaged in bank fraud by tendering fraudulent checks and committed aggravated identity theft and access device fraud by using another person's identifying information and financial accounts without authorization.

Felch exploited a position of trust granted by the owner of Rodeo Electrical Services, who had provided her employment and housing. The scheme nearly drove the company into financial ruin, delayed the victim's retirement plans, and caused significant financial, emotional, and physical hardship. (Source)

Company Operations Manager Pleads Guilty To Embezzling $344,000+ From His Employer For 5 Years By Forging Owners Signature On Checks - July 14, 202

Michael Darcy, 49, was the Operations Manager for his employer. As Operations Manager, Darcy oversaw the day-to-day work of the company and had access to the company checkbook.

Beginning in December 2019, and continuing through December 2024, Darcy forged the owner's signature to draft dozens of unauthorized checks on the company's bank account. Darcy concealed the purpose of the payments by entering them under false headings in accounting records. He sometimes also listed false entries in the memo line on the checks. Overall, Darcy embezzled $344,874.47 from his employer. (Source)

Employee Working In Finance Department For 2 Non-Profit Organizations Pleads Guilty To Stealing $321,000+ / Used Funds To Pay For Personal Expenses - July 23, 2026

From at least 2017 to September 2025, Seth Jones worked in the finance department of Non-Profit Company #1, which was a parent company to Non-Profit Company #2.

The defendant defrauded the non-profit companies by using a company credit card to pay for approximately $291,023 in personal expenses and diverting approximately $31,775 in funds from a bank account associated with Non-Profit Company #2 to bank accounts controlled by him. In order to carry out and conceal the fraud scheme, Jones falsified expense reports, failed to submit expense reports, and created fake invoices. Jones defrauded the 2 non-profit organizations out of $322,798. (Source)

Christian School Academic Director Charged With Stealing $96,000+ To Pay For Spa Treatments, Jewelry & Botox Injections - July 21,2026

Charges have been filed against a former employee (Angela Ruiz-Pearce) of the Heritage Christian School, in Indianapolis, who is accused of using her school credit card to pay for spa treatments, expensive jewelry and other personal expenses.

Ruiz-Pearce worked as the school's academic director and was responsible for managing the school's expenses for textbooks, instructional materials and teacher training.

Police learned that Ruiz-Pearce worked at the school between January 2024 and February 2026. During that time, she was issued a company credit card from the school that was only meant to be used for school-related purchases.

Pearce's last day working at the school was Feb. 9. The school also reported finding $30,000 in personal purchases within 10 hours of her dismissal, court documents said.

The school said it canceled the suspect's credit card and proceeded to conduct an internal investigation and audit after flagging the fraudulent charges.

This process led to the realization that Ruiz-Pearce had allegedly submitted false receipts to justify her credit card expenses. The schools investigation concluded that $96,153.81 was allegedly deemed to be fraudulent. Court documents revealed that detectives could not decipher which Amazon transactions were legitimate and which ones were deemed to be fraudulent since everything was mixed. (Source)

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Human Resources Executive Agrees To Pay $160,000 For Submitting Fraudulent Invoices To Her Employer - July 29, 2026

Carleena Graham is the former Vice President of Human Resources for World Learning. She has agreed to pay $160,000 to resolve allegations that she violated the False Claims Act by submitting false invoices to her employer for reimbursement of expenses that benefitted her personally and organizations with which she was affiliated.

World Learning is a nonprofit global development and exchange organization that delivers educational and professional training programs around the world. It was also a recipient of United States Agency for International Development (USAID) and U.S. Department of State funds through various grants, contracts, and negotiated indirect cost rate agreements totaling several million dollars.

From approximately 2015 to 2022, Graham orchestrated a scheme to submit false invoices to World Learning for reimbursement of hundreds of thousands of dollars of expenses. As part of that scheme, Graham arranged for goods and services to be delivered to third-party organizations and then arranged for World Learning to pay for these goods and services via electronic transfers of funds from its bank account or use of World Learning's credit cards. Graham falsified invoices submitted by vendors for payment of the goods and services to make them appear as though World Learning was the recipient of the goods and services. By defrauding World Learning, the Government contends Graham was also misappropriating funds the nonprofit received from USAID and the State Department. (Source)

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

No Incidents To Report)

THEFT OF ORGANIZATIONS ASSESTS / DESTRUCTION OF PROPERTY

Company Senior Director Of Engineering Sentenced To Prison For Using Company Credit To Purchase $4 Million Worth Of Apple Products Over 8 Years & Then Sold Them - July 22, 2026

While serving as a long time employee of Big Ten Network (BTN), as a senior director of engineering, Weston Goldstein, 48, was responsible for procuring electronic devices for BTN and its employees. Over approximately eight years, Goldstein used company credit cards and the company's procurement process to purchase electronic devices—namely Apple products—for his family members, for an Apple device reseller in Pennsylvania, and to sell to third parties through online marketplaces such as eBay and Mercari.

Between January 2016 and August 2023, Goldstein purchased approximately $4,008,719.91 of Apple products using BTN funds and then sold them through various means for approximately $1,100,000. Goldstein used his position and exploited decreased oversight during the COVID-19 pandemic to commit the years-long fraud.

Goldstein spent approximately $630,000 of the illicitly-obtained proceeds for his own benefit on things like restaurants, merchandise, and automotive expenses. Goldstein paid the remaining amount approximately $470,000 to an individual that Goldstein claimed was extorting him after the two began an online relationship. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

8 Individuals Including Current & Former NYC Correction Officers, Texas Parole Officer, & NYC Transit Authority Employee Charged In $3 Million+ Check Fraud Scheme - July 20, 2026

These individuals where for a fraud scheme relating to deposits of falsified checks and the production of fraudulent Social Security cards.

Several of the defendants are current or former government employees. Christopher Walker is a New York City Correction Officer and made at least one fraudulent deposit while wearing his Department of Correction uniform. Valeria Waldron is a former New York City Correction Officer and was more recently employed as a parole officer with the Texas Department of Criminal Justice. Steven Boyce is a track worker with the New York City Transit Authority. Aaron Warren and Tara Dildy are also former New York City Correction Officers.

In total, the defendants created and/or deposited over $3 million worth of fictitious checks and obtained over $500,000 in fraudulent proceeds. The defendants spent their stolen cash on luxury handbags, plastic surgery, and tropical vacations, among other personal expenses. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Hospital Nurse Loses Nursing License For Forging Prescriptions For Percocet & Oxycodone - July 10, 2026

Brooke Haller, 41, previously worked as a registered nurse at a hospital in Kansas City, Kansas. She used her position to gain access to a nurse practitioner's prescription pad and Drug Enforcement Administration (DEA) number. In March 2024, Haller began to use this information to write forged prescriptions for herself using the names of her relatives for Percocet and Oxycodone, which she filled and paid for at pharmacies in Kansas and Missouri.

An investigation was initiated in October 2024, after a pharmacy called the hospital to inquire about an Oxycodone prescription allegedly written by a nurse practitioner. The nurse practitioner advised she only writes electronic prescriptions. The victim indicated she had never spoken to Haller nor had she given Haller her prescription pad and DEA number.

When Haller realized her scheme was falling apart, she tried to cover up her crimes. She called the hospital several times pretending to be from the pharmacy indicating the pharmacy staff questioned the validity of the prescription by mistake. Haller spoofed the pharmacy's phone number and used several vocal disguises, including pretending to be "Peter", but the hospital staff recognized her voice.

Haller later admitted to DEA investigators that she fraudulently wrote 13 prescriptions. She obtained 90 Percocet tablets and 540 Oxycodone tablets from a pharmacy in Kansas and 1,350 Oxycodone tablets from a Missouri pharmacy. (Source)

OTHER FORMS OF INSIDER THREATS
No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS
No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION
No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS
No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER
No Incidents To Report

ORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'
EMPLOYEES' INVOLVED IN TERRORISM
No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
www.insiderthreatincidents.com

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 NITSIG.

WHO CAN BE AN INSIDER THREAT?

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees (**1** - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (**2** - Failure By Action, Behavior Or Response) (**3** - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- ☐ Opportunist Employees (**1** - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (**2** - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (**3** - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- ☐ Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- ☐ 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)
- ☐ Artificial Intelligence Agents That Can Act Without Human Oversight & Authorization (Sharing Sensitive Data, Making Decisions, Etc.)

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

There can be many different types of Insider Threat incidents that are 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 Employers 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

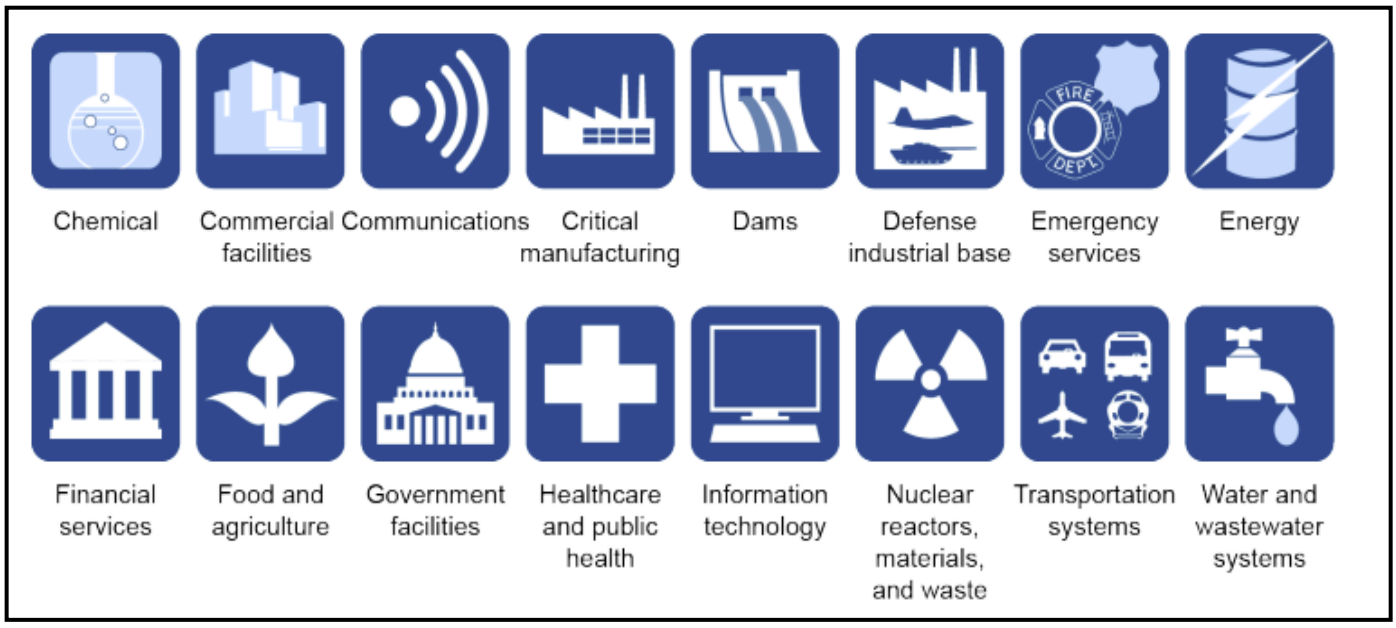
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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 Special Report: Employee Personal Enrichment Using Employers Money
Release Date: November 2025
You might be amazed at the many reasons employees steal money from their employers. Employees may not be disgruntled, but have other motives such as financial gain as outlined below.

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.) This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives. This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

What Do Employees' Do With The Money They Steal From Their Employers?
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 2026 REPORT ON FRAUD

If you manage or support an Insider Risk Management Program (IRMP), you should read this report. If there is someone else within the organization who is responsible for fraud, the IRMP Manager should be collaborating with this person very closely.

Could your organization rebound / recover from the severe financial impacts of a fraud incident?

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

Association of Certified Fraud Examiners 2026 Occupational Fraud Report Overview

This report to analyzes 2,402 real cases of occupational fraud that were investigated between January 2024 and September 2025. The findings presented in this report can be used by anti-fraud professionals, organizational management, and others to improve their fraud prevention, detection, and response efforts in several ways. These cases span organizations of all sizes, across a broad range of industries, and in every major geographic region.

As in prior editions, this report explores occupational fraud across six key dimensions: the methods by which frauds are committed, the financial impact of those schemes, the ways frauds are detected, the characteristics of victim organizations, the profiles and behaviors of perpetrators, and the outcomes of cases once misconduct is uncovered.

A primary goal of this report is to identify the frequency and cost of the various types of occupational fraud. Asset misappropriation schemes, or those in which an employee steals or misuses the employing organization's resources, were once again the most common category of occupational fraud, occurring in 90% of our study's cases and causing a median loss of USD $100,000, which was the lowest of the three categories.

Corruption was half as common as asset misappropriation, occurring in 45% of cases in the study and causing a median loss of USD $150,000. Although financial statement fraud, an intentional misstatement or omission of material information from the victim organization's financial reports, was the rarest form of occupational fraud (6% of cases), it was the most costly with a median loss of USD $1,000,000.

Types Of Organizations Impacted By Fraud

Private companies were victimized by the largest percentage of frauds in our study, accounting for 44% of cases with a median loss of USD $140,000. The least victimized organizations in our study were nonprofits 10%, which also incurred the lowest median loss USD $69,000. Government organizations fell in the middle of both spectrums, with 16% of cases impacting this category and a median loss of USD $110,000.

Fraud At Federal / State Levels

This report shows the majority of government organizations victimized by the frauds in our study were at the national level 37%, followed closely by local 32% and state / provincial 27% governments. National-level governmental organizations also suffered the highest median losses at USD $150,000, followed by state / provincial at USD $121,000 and local at USD $79,000. The significant and elevated fraud risk at the national level of government indicated by these results is likely related to the fact that national governments receive more funding and have complex organizational structures and operations, which could create more opportunities for occupational fraud.

The report provides a wealth of information on the types, sizes and industry of the victim organizations that experienced fraud, the perpetrators position, tenure, department, age, gender, education, etc. as referenced below. The report provides other information on collusion by employees, behavioral red flags of fraud, etc.
Download Report

REPORT INFOGRAPHICS
ACFE 2026 Occupational Fraud Report Key Findings
The Global Cost Of Fraud
Fraud In Banking & Financial Services
The Effectiveness of Providing Fraud Awareness Training
Profile Of A Fraudster
Collusion By Fruad Perpetrators
Behavioral Red Flags Of Fraud Perpetrators

Highlights Of The Association of Certified Fraud Examiners 2026 Occupational Fraud Report
This report provides undisputable evidence that collaboration between the Human Resources (HR) Department and the Insider Risk Management Program is critical, as referenced below. (**See Pages 69-70**)

Human Resources Red Flags
In addition to behavioral indicators, we asked whether perpetrators experienced job-related conditions that might have might have been a factor in their decision to commit fraud. These circumstances, referred to as HR-related red flags, include expressions of concern about job security, adverse performance evaluations, demotions, denial of raises or promotions, and reductions in compensation or benefits.

The report shows that 45% of perpetrators experienced at least one HR-related red flag prior to or during the fraud. The most commonly reported conditions were poor performance evaluations (12%), fear of job loss (12%), and being denied a raise or promotion (11%).

Behavioral Red Flags (BRF's) For Fraud
The report shows that 75% of fraudsters displayed at least one of the 8 most common behavioral clues listed below, and each of these BRF's were observed in at least 9% of cases. Fraudsters livening beyond their means has consistently been the most common behavioral red flag since we began tracking this data in 2008

39% Living Beyond Means
29% Financial Difficulties
17% Unusually Close Association With Vendor / Customer
12% Control Issues, Unwillingness To Share Duties
11% Irritability, Suspiciousness, Or Defensiveness
11% Bullying Or Intimidation
9% Wheel - Dealer Attitude
9% Divorce / Family Problem

Employee Background Checks
One of the most straightforward ways an organization can protect itself from fraud is to avoid hiring someone with a history of fraud-related misconduct. As such, effective background checks are an important part of a comprehensive fraud prevention program. This report showed that 64% of the victim organizations in our study conducted a background check on the perpetrator prior to hiring them, with 88% of those background checks coming back without any red flags.

However, 12% of the background checks did reveal at least one red flag before the perpetrator was hired, illuminating a gap in the protective value of background checks as an anti-fraud control. (**See Page 48**)

Hotline Reporting / Fraud Awareness Training

Organizations had 50% lower losses and 40% faster detection with a hotline. Whistleblowers are still the best detection method. Tips have been the most common detection method in every edition of this fraud report. (**See Page 51**)

Internal Control Weaknesses That Contribute To Fraud

Analyzing the root cause behind a fraud can help organizations both identify weaknesses that could lead to other violations and ensure that steps taken following the fraud truly remedy the factors that allowed it to occur. We asked respondents about the primary internal control weakness that contributed to the frauds they reported. This report showed 33% frauds occurred due to the victim organization lacking internal controls, with another 19% resulting from an override of existing internal controls. The next most common weakness cited was a lack of management review 18%. Collectively, these three weaknesses accounted for 70% of all frauds in our study. Other factors that contributed to fraud; Poor tone at the top 7%, Lack of competent personnel in oversight roles 7%, Other 6%, Lack of independent checks / audits 4%, Lack of employee fraud education 3%, Lack of clear lines of authority 2%, Lack of reporting mechanism <1%. (**See Page 49**)

Did Organizations Modify The Anti-Fraud Controls Following A Fraud Incident?

This report shows that 80% of organizations modified their controls following the detection of the fraud. Among the organizations that did modify their controls following the fraud, the most common changes pertained to management review, with 40% of victim organizations modifying their existing reviews and 37% implementing new reviews. More than half of the organizations also updated their approaches for data monitoring and analysis and for surprise audits. These three controls all focus on proactive fraud detection, indicating that victim organizations prioritized improvements in catching fraud faster and increasing the perception of detection among employees. (**See Pages 45-46**)

Perpetrators Position

According to our data, a perpetrator's level of employment within their organization correlated to the median loss and duration of the fraud. Frauds carried out by perpetrators at higher levels of authority caused higher losses and lasted longer, as has been the case in previous editions of this study.

This report showed that frauds carried out at the owner / executive level only represented 16% of the cases submitted but caused by far the highest median losses, at USD $475,000, which was more than nine times as much as employees USD $50,000, and more than three times as much as managers USD $125,000. Frauds carried out by employees and managers were much more common, each representing 41% of the cases submitted.

Similarly, perpetrators with higher levels of authority carried out fraud schemes that took longer to detect, according to our data. The median duration of frauds perpetrated by employees was only 8 months, just over one-third as long as those perpetrated by owners and executives (23 months); managers' frauds had a median duration of 14 months. (**See Page 51**)

Perpetrators Tenure With Employer

To assess how a perpetrator's employment tenure relates to occupational fraud risk, we asked survey respondents to report how long the primary perpetrator had been employed by the victim organization at the time the fraud occurred.

This report shows losses increased steadily with tenure, with schemes committed by individuals who had worked for the organization more than ten years resulting in the highest median losses USD $200,000. However, longer tenure did not equate to higher frequency; our findings indicate that, while extended tenure is associated with more-costly frauds, a majority of occupational fraud is committed by employees who have been employed at a victim organization fewer than five years. (**See Page 53**)

Schemes Based On Perpetrators Department

This report provides insight into the most common fraud schemes in high risk departments: Operations, Accounting, Sales, Customer Service, Executive / Upper Management, Administrative Support, Finance and Purchasing. (**See Pages 54-56**)

Perpetrators Position Based Gender

To further examine how gender relates to occupational fraud risk, we analyzed the frequency and median losses of frauds committed by male and female perpetrators across different levels of organizational authority. This report show female perpetrators were most frequently observed at the employee level, where they accounted for 36% of cases. Across all authority levels, frauds committed by females were associated with lower median losses than those committed by males. The greatest differences in both frequency and loss severity between genders occurred among owners and executives, indicating that gender disparities in fraud impact are most pronounced at the highest levels of authority. (**See Page 60**)

Perpetrators Age

Analysis revealed a clear relationship between a perpetrator's age and the financial impact of occupational fraud. This report shows median losses increased with age, with perpetrators over the age of 60 causing median losses of USD $850,000, which was more than 47 times greater than the median losses associated with perpetrators under the age of 26 USD $18,000.

Despite the high losses linked to older fraudsters, they accounted for a relatively small share of cases. Instead, perpetrators between the ages of 31 and 50 were responsible for the majority of frauds in our study, collectively accounting for 70% of reported cases. These findings indicate that, while fraud committed by older individuals tends to be more costly, occupational fraud most frequently originates from mid-career employees. (**See Page 61**)

Perpetrators Education Level

Analysis of perpetrators' education levels indicates that occupational fraud is most often committed by individuals with higher levels of formal education. More than 60% of the perpetrators in our study held at least a university degree. As illustrated in Figure 49, median losses increased consistently with higher levels of education, suggesting that perpetrators with greater educational attainment tend to cause more-costly frauds, likely reflecting their access to more-complex roles, responsibilities, or organizational resources .(**See Page 62**)

Collusion By Multiple Perpetrators

This report showed that in the fraud cases in our study, collusion was almost evenly split between those committed by a single perpetrator 51% and those involving two or more individuals acting together 49%.

Although collusive schemes occurred slightly less frequently than single-perpetrator frauds, they were associated with higher median losses than schemes carried out by one individual (USD $55,000). Losses increased further as the number of perpetrators grew, with frauds involving three or more individuals resulting in median losses more than twice as high as those involving only two perpetrators.

These findings suggest that collusion can significantly amplify fraud impact, likely due in part to the increased ability of multiple perpetrators to bypass anti-fraud controls when working together. (**See Page 63**)

Perpetrators Employment History / Criminal Background

Beyond criminal history, we also examined whether perpetrators had previously faced internal punishment for fraud-related conduct and, if so, where that action originated. This report shows prior discipline was uncommon among perpetrators in our study: 85% had no known history of fraud-related disciplinary action before the scheme occurred. Among the remaining cases, a small proportion involved individuals who had previously been terminated for fraud (6%), while others had received non-termination disciplinary sanctions (8%).

For perpetrators with a documented history of fraud-related discipline, responsibility for that action varied across employers. More than half had been disciplined by the same organization victimized in the reported case, while 33% had faced consequences at a previous employer. An additional 12% had been disciplined by both a former employer and the victim organization.

This report shows most perpetrators in our study had no known history of fraud-related criminal charges or convictions at the time of the offense. This finding suggests that traditional criminal background checks alone would not have prevented the majority of the frauds analyzed. Notably, however, 4% of cases involved perpetrators with a prior fraud conviction—either because that information was not identified during the hiring process or because it did not preclude their employment. These results highlight the limitations of relying solely on criminal history screening as a fraud prevention measure. (See Pages 66-67)

Internal Actions Taken Against Perpetrators

After a fraud examination has identified the perpetrator(s) involved in the scheme, the first step for most organizations is determining what internal punishments are appropriate and necessary. Termination is (and has been) the most common punishment, with 68% of perpetrators being terminated following the investigation of their fraud. A small portion of cases result in no punishment 4% or only a written or verbal warning 6%. (**See Page 73**)

Internal Punishment By Perpetrators Position

Within our survey responses, fraudsters can be found in every position in an organization. Their level of authority can affect the extent and impact of the fraud as well as the internal punishments they tend to receive. Owners and executives were terminated in only 52% of reported cases, while fraudsters working as managers 68% and employees 75% were more frequently removed. Similarly, owners and executives received no internal punishment for the fraud they perpetrated in 12% of cases, while managers and employees received no punishment more rarely 2% each. (**See Page 74**)

Litigation Against Perpetrators

Along with internal punishments, many organizations decide to pursue legal action against fraudsters. Private civil lawsuits and criminal referrals to law enforcement are the primary vehicles organizations use to pursue recoveries and punish fraudulent acts. We asked survey respondents whether the organizations victimized by fraud filed a civil lawsuit against the perpetrator and how the lawsuit concluded.

Organizations filed civil lawsuits in only 25% of reported fraud cases, though the suits that were filed were successful, either through a settlement or a judgment for the victim, in 82% of cases. (**See Page 75**)

Criminal Referrals Against Perpetrators

Fraud is a crime prosecuted by the government, but it's up to organizations to decide whether to refer cases they investigate internally to law enforcement. We asked survey respondents whether the victim organizations in their cases made a criminal referral, whether prosecution was pursued, and whether the prosecution was successful. Overall, organizations were much more willing to refer fraud cases for criminal prosecution compared to pursuing their own civil actions, with 54% of respondents reporting that the case was sent to law enforcement. Fraud prosecutions were generally successful, with 48% of defendants pleading guilty or no contest, 24% of defendants convicted at trial, and only 2% of defendants acquitted at trial. Most cases were pursued by law enforcement after being referred, with only 14% of respondents reporting that prosecutors declined to pursue the case. (**See Page 75**)

Reasons For Not Referring Fraud Case To Law Enforcement

Not all fraud cases are referred to law enforcement for further investigation and prosecution. To better understand the decision-making of the 46% of organizations who did not refer to law enforcement, we asked survey respondents what were the reasons. This report shows the most common response was that internal discipline was deemed sufficient punishment of the perpetrator 51%, followed by the fear of bad publicity 35% and private settlements being reached 20%. (**See Page 76**)

Recovering Fraud Losses

Organizations must weigh the benefits of internal punishments, costly legal actions, and settlement agreements against the potential for recovering assets lost to fraud. The results of our current survey and surveys past show an unfortunate trend of organizations failing to recover any fraud losses. This report showed 56% of the organizations in our study were unable to recover anything following the fraud. While 29% of organizations managed a partial recovery, only a small portion of respondents 15% reported a full recovery for the victim organization. (**See Page 77**)

Organization That Received Fines Because Of Employee Fraud

Organizations victimized by fraud might be fined or penalized by regulators in their jurisdiction due to the fraud uncovering or resulting from a compliance failure. We asked survey respondents whether the victim organization in their case had received such a fine and analyzed the results by scheme and the type of organization. This information can be helpful for organizations to understand how occupational fraud might result in a finding of noncompliance and help them make decisions concerning their internal compliance initiatives.

This report shows that 11% of organizations victimized by asset misappropriation schemes received a fine. Comparatively, in cases of financial statement fraud, 22% of victim organizations reported receiving a fine. Government agencies reported receiving fines most frequently 13%, while publicly traded companies received fines in the smallest percentage of cases 7%. (**See Page 78**)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

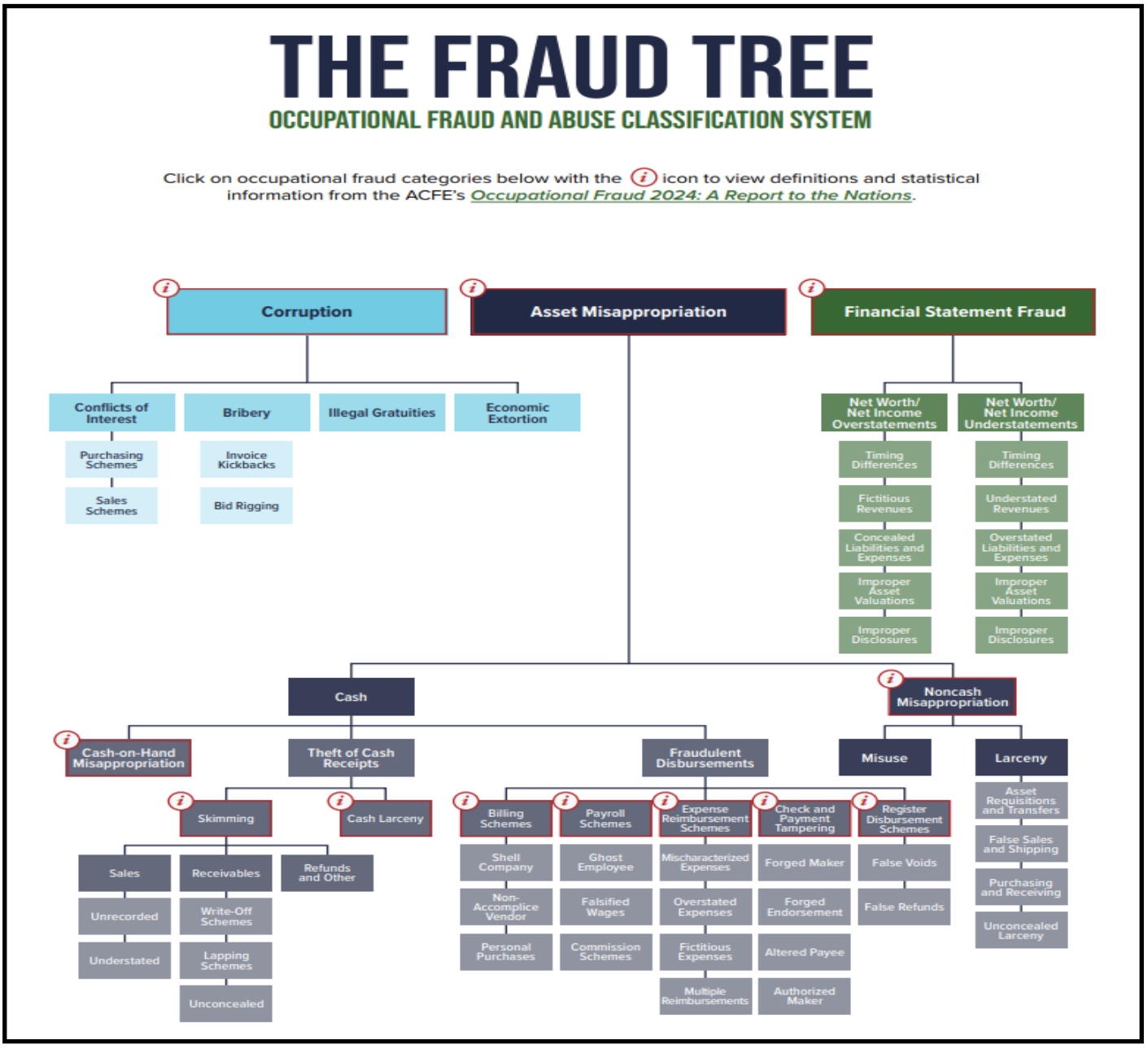
Other Tools

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 / Employees Accepted $57,000+ In Bribes / 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+ / GS Agrees To Pay $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 Fraudulent 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)

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)

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 / DATA BREACHES

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)

South Korean Company Data Breach Caused By Employee Exposed Information On 34 Million Users / Company Must Compensate $1.1 BILLION To Affected Users - December 28, 2025

South Korean online retail giant Coupang said it will offer 1.69 trillion South Korean won ($1.17 billion) in compensation to 34 million users affected by a massive data breach disclosed last month.

The company said in a statement that it planned to provide customers with purchase vouchers totaling 50,000 won for various Coupang services. Former customers who closed their Coupang accounts following the data breach are also eligible to receive the vouchers.

Harold Rogers, interim CEO for Coupang Corp., described the move as a "responsible measure for our customers," and said the company would "fulfill its responsibilities to the end."

The data breach, which was revealed on Nov. 18, 2025 led to the resignation of CEO Park Dae-jun earlier this month.

Coupang founder Kim Bom said in a separate statement that the company had failed to communicate clearly from the outset of the incident. The U.S.-based chairman acknowledged his apology was "overdue," explaining that he initially believed it was best to communicate publicly and apologize only after all the facts were confirmed.

Kim added that the company has recovered all the leaked customer information through cooperation with the government, as well as the storage devices belonging to a suspect behind the data breach.

He also said the customer information stored on the suspect's computer was limited to 3,000 records and that it was not distributed or sold externally.

As the police continued their investigations in Coupang's offices, they uncovered that the primary suspect was a 43-year-old Chinese national who was a former employee of the retail giant. The employee had joined Coupang in November 2022, and was assigned to an authentication management system and left the firm in 2024. He is believed to have already left the country. (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)

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)

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)

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)

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)

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

Disgruntled Employee Charged For Setting Fire To 1.2 Million Square Foot Warehouse Causing Approximately $500 Million In Damage - April 9, 2026

A massive fire tore through a nearly 1.2 million-square-foot warehouse in Ontario, California, in the early hours of April 7, 2026 escalating into a six-alarm blaze that took hours to control. Flames and heavy smoke were seen billowing from the facility as more than a hundred firefighters rushed to the scene. The warehouse, which stored large quantities of paper-based consumer goods, suffered extensive damage, with parts of the structure collapsing as the fire spread rapidly. The fires Chamel Abdulkarim set quickly consumed the building, resulting in its destruction and causing approximately $500 million in damage.

Abdulkarim, a 29-year-old employee from Highland, California, worked at the facility through NFI Industries, a logistics partner for Kimberly-Clark. He is now accused of being responsible for starting the fire that destroyed a major distribution centre serving millions of consumers.

According to an affidavit filed with the federal criminal complaint, early in the morning on April 7, Abdulkarim filmed himself setting fire to multiple pallets of paper goods inside of a large distribution center in Ontario. As he lit the fires, he stated, "If you're not going to pay us enough to [expletive] live or afford to live, at least pay us enough not to do this [expletive]."

Abdulkarim posted videos of himself on social media setting the fires. He further made statements to others on the telephone and via text messages related to his motive for setting the building on fire, including the following: "I just cost these [expletive] billions," "1% is a [expletive] joke," and "All you had to do was pay us enough to live. Pay us more of the value WE bring. Not corporate. Didn't see the shareholders picking up a shift." (Source)

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)

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)

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

NITSIG INSIDER THREAT SPECIALIZED REPORTS

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

INSIDER THREAT INCIDENTS E-MAGAZINE
2014 To Present / Updated Daily
The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**7,300+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X
Updated Daily
https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

INSIDER THREAT INCIDENTS MONTHLY REPORTS
July 2021 To Present
http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SPECIALIZED REPORTS
Produced By:
National Insider Threat Special Interest Group (NITSIG)
Insider Threat Defense Group (ITDG)

Practical Guide For Securing Buy-In From CEO's & Stakeholders For Insider Risk Management Program / May 2026
The purpose of this guide is to put some clarity into describing the Insider Threat problem, the Return On Investment (ROI) for creating an Insider Risk Management (IRM) Program (IRPM) and eliminate the confusion that still plaques many organizations from developing or maturing their program.

IRMP's often lack CEO support because they are frequently misperceived as expensive, productivity-stifling, employee witch hunt programs that provide unclear ROI. These misconceptions are based on misinformation and false assumptions.

What will be described in this guide is a practical and real world approach to better educate the CEO and key stakeholders on having a more comprehensive understanding of the mission, scope and costs for an IRMP. The guidance in this document will focus on IRM from a 360 degree perspective, not just a technical perspective as many other guides do. (Download Report)

Employee Personal Enrichment Using Employers Money / November 2025
You might be amazed at the many reasons employees steal money from their employers.

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.)

This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives.

This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

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

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

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

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

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

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

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

Why Insider Threats Remain An Unresolved Cybersecurity Challenge
Produced By: IntroSecurity: NITSIG - ITDG / June 2025
The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

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

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

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

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

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

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

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

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS
https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed. The comprehensive reports and guidance provided by the NITSIG, quickly fueled the NITSIG memberships growth to become the largest U.S. / Global Insider Risk Management ISAC.

The NITSIG has been successful in bringing together a diverse group security professionals and individuals managing and supporting Insider Risk Management (IRM) Programs from the: U.S. Government Agencies, Department Of War, Intelligence Community Agencies, Critical Infrastructure Providers, Law Enforcement, 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 protecting their organizations assets against the severe impacts that can be caused by **Just 1 Employee**, **Multiple Employees In Collusion** or **Employees In Collusion With External Co-Conspirator(s)**. Many members have even stated the NITSIG is like having a team of IRM experts consultants at their disposal **FREE OF CHARGE**.

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;

- ✓ IRM Program (Development, Management, Evaluation & Optimization)
- ✓ IRM Program Working Group / Hub Operations
- ✓ Insider Threat Investigations & Analysis
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Vulnerability Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Employee Continuous Monitoring & Reporting Programs (Benefits, Guidance, Solutions)
- ✓ 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. The meetings are held at various locations throughout the U.S. See this link for some of the great speakers we have had at our meetings.

NITSIG Insider Threat Symposium & Expo (ITS&E)

ITS&E events (1 Day) provide attendees with outstanding speakers who have expert knowledge of developing, managing, evaluating and optimizing IRM Programs. The NITSIG has held 5 ITS&E events (2015, 2017, 2018, 2019 and 2025) at the Johns Hopkins University Applied Physics Laboratory, in Laurel, Maryland.

The ITS&E features expert speakers, engaging panel discussions, interactive sessions, vendor technologies and solutions, and networking with IRM practitioners. (2025 ITS&E)

NITSIG IRM Resources

Posted on the NITSIG IRM Website are various documents, resources and training that will provide guidance to assist organizations with their IRM / IRM Program efforts. The website is a public repository of documents containing guidance for IRM and security practitioners to use for expanding their knowledge of protecting their organizations assets against Insider Threats.

NITSIG LinkedIn Group

The NITSIG has created a LinkedIn Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with **950+** members enables 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.

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. AB members will provide oversight, educational, strategic and operational guidance to support the mission of the NITSIG, and also help to facilitate building collaborative relationships with individuals that manage or support IRM Programs.

Please contact me with any questions regarding the NITISG or IRM.

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

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

Since 2009, the Insider Threat Defense Group (ITDG) has provided **700+** organizations and **1000+** students with the core skills / advanced knowledge, resources and technical solutions for developing, managing, evaluating and optimizing their organizations Insider Risk Management (IRM) Programs (IRMP's).

The ITDG exceeds IRM compliance regulations and help organizations create comprehensive, robust and cost effective IRMP's.

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.

IRMP TRAINING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRMP Stakeholders Training Course & Workshop / Table Top Exercises
- ✓ IRMP Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees
- ✓ Customized IRMP Training For Our Clients

CONSULTING SERVICES OFFERED

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

BACKGROUND ON ITDG EXPERTISE IN THE FIELD OF INSIDER RISK MANAGEMENT

Insider Risk Management Program 360 Framework & Assessment Methodology (IRMP360FAM™)

Since 2009, the ITDG has been involved in U.S. Government, Department of Defense (DoD) and Intelligence Community Agencies (ICA's) Insider Threat Program (ITP) efforts.

From 2009 to 2011, the ITDG was under contract with the DoD Insider Threat Counterintelligence Group (ITCIG) to provide guidance in various areas of IRM. The DoD ITCIG in collaboration with other agencies (NCIX - NCSC, NSA, CIA, NGA, NRO,) were instrumental in developing what is known as National Insider Threat Policy (NITP).

The ITDG Insider Risk Management Program (IRMP) Framework was initially developed in 2014 with the help of individuals managing and supporting ITP's for the DoD and ICA's.

The IRMP Framework has undergone several enhancements over the years and provides comprehensive guidance for IRMP Development, Management, Evaluation and Optimization, for both the U.S. Government and private sector businesses. It is continuously being evaluated and updated due to the ever changing Insider Threat landscape. The IRMP Framework is practical, real world, cost effective, proven, unique and holistic.

Since 2014, the IRMP Framework has served as the backbone for our training and consulting services. The ITDG is a visionary in the field of IRM. In 2014, the ITDG was one of the first companies to offer comprehensive ITP Development / Management Training to the U.S. Government and defense contractors, who were required to implement programs based of off NITP and the NISPOM Conforming Change 2 Regulation.

The IRMP Framework encompasses 11 critical domains for IRM and an IRMP. Our methodology addresses Insider risks and threats from an enterprise cross functional perspective, and from a non-technical and technical perspective. No one in an organization is positioned to see every single employee risk factor or behavioral indicator. Ensuring that enterprise security foundations are in place, and that there is universal alignment and collaboration with key stakeholders and the IRMP, is a critical element for detecting, responding to, investigating, preventing and mitigating Insider risks and threats.

Our IRMP Framework covers Insider Risk Management from A to Z, to enhance the security foundations of the organization, and to prevent operational disruptions, downtime, loss of productivity, loss of income, loss of assets, prevent workplace violence, legal exposure, etc. from the negligent, disgruntled, malicious and opportunist actions of employees.

The ITDG has empowered organizations with the ability to implement, manage and optimize a comprehensive and cost effective IRMP, transforming the Insider Threat problem from a siloed **REACTIVE** task into a shared **PROACTIVE** organizational responsibility.

CLIENT SATISFACTION / COMPANY RECOGNITION

The comprehensive nature of our IRMP Framework and 15+ years of IRMP expertise, is what separates us from other providers of IRMP training and consulting services. ITDG training courses have been taught to over **1000+** individuals. Our students and clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM.

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

Our client satisfaction levels are in the **EXCEPTIONA**L range. You are encouraged to read the feedback from our clients on this link.

The ITDG Has Provided IRMP Training & Consulting Services To An Impressive List Of 700+ Clients:
White House, U.S. Capital Police, 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)

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.
IRMP Evaluation & Optimization Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Threat Vulnerability Assessor & Mitigation Specialist
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG