INSIDER THREAT INCIDENTS REPORT
FOR
February 2026

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

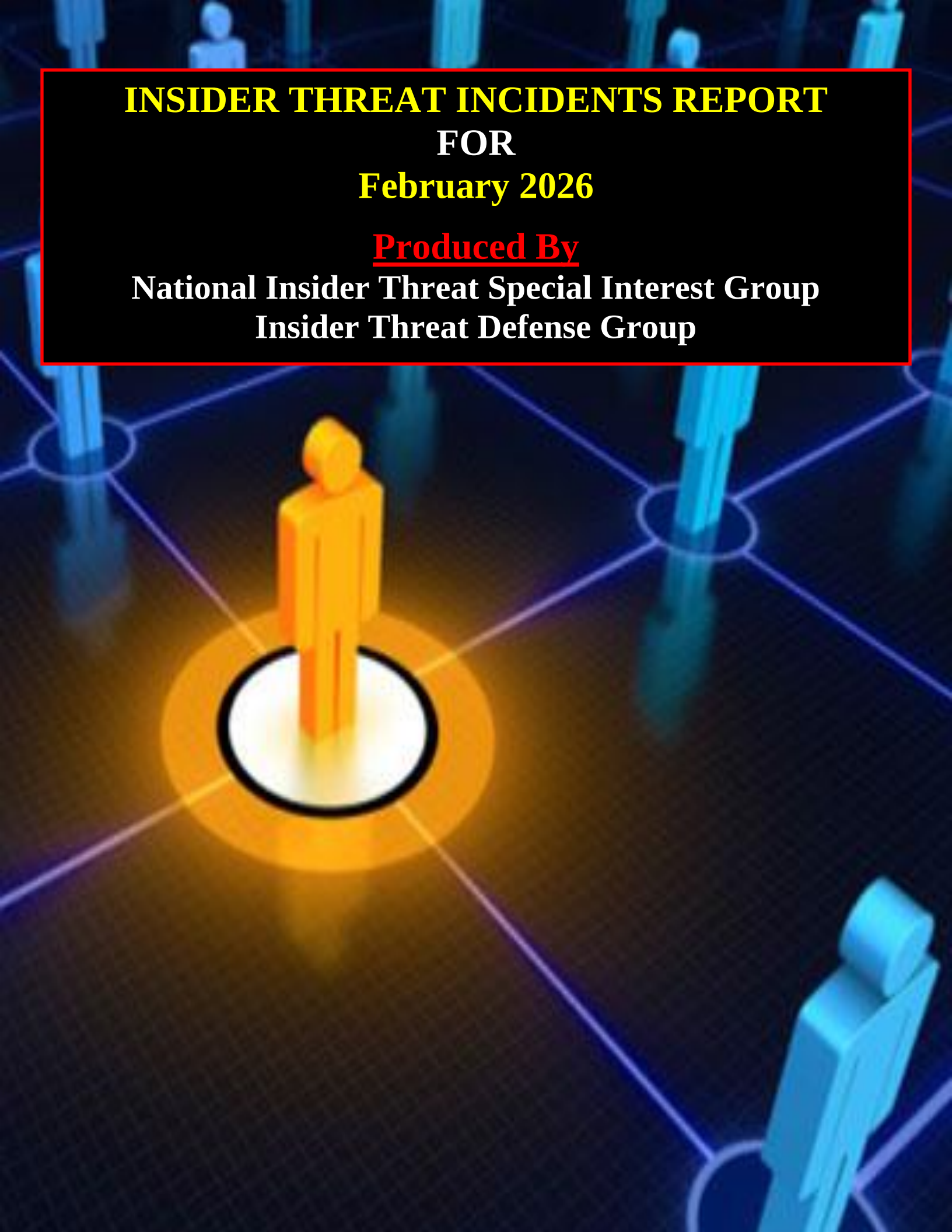


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS OVERVIEW

A Very Costly And Damaging Problem

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees' who are negligent, malicious or opportunists. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **6,900+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This 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 22** 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 FEBRUARY 2026

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES
No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS

Research Survey Of 500+ IT College Students Finds 60% Said They Would Leak Information In Exchange For Kickbacks - January 26, 2026

A survey of 523 information systems management and data analytics students by the State University of New York at Buffalo found that nearly 60% of respondents said they would leak information about a very famous patient in exchange for amounts ranging from less than $10,000 to more than $10 million, depending on the perceived probability of getting caught and the salary level of the employee.

Students were told to imagine themselves having post-college financial difficulty and a friend who works at a media company. Roughly six out of every 10 students said they would give up the data of the famous patient. The amount required varied on the scenario, with students told to imagine a greater salary needing a bigger payoff.

The research builds upon a 2020 study involving 523 students with an average age of 21 who were about to enter the workforce. That earlier survey found 46% of respondents would accept a certain amount of money in exchange for violating HIPAA, also depending upon the circumstances.

In that study, 79% of respondents said they would hand over a politician's medical records to a media outlet in exchange for $100,000 in order to pay for an experimental medical treatment for their mother that was not being covered by insurance. (Source)

Cyber Criminals Paying Employees Up To $15,000 For Access To Business Networks

Cyber criminals are no longer relying solely on brute force, social engineering, or exploiting vulnerabilities in perimeter defenses to gain access to networks. When the emotions of an employee are falling apart and they are very disgruntled, is when they are the perfect target for someone to help them with revenge against their employer.

The harsh reality is there is a blended threat that has slowly been brewing and is now growing faster, and that CEO's and key stakeholders must address. Perimeter defense systems and firewalls in some cases are not stopping hackers from breaching the network, because malicious or opportunist employees are just opening the doors for them, and getting paid for doing so.

According to recent findings from a 2025 Check Point Software Research, a disturbing trend is emerging where state-sponsored hackers and other threat actors are actively recruiting insider threats from major companies in sectors such as telecommunications, banking, and technology on DarkNet forums. These cyber criminals are offering substantial financial incentives, ranging from $3,000 to $15,000, depending on the sensitivity and value of the information, data or intelligence these insiders can provide.

In return for their cooperation, insiders may provide hackers with vital credentials such as passwords, admin privileges, or access to cloud systems, user devices and corporate networks.

Some employees are even volunteering, to sell access or sensitive information for lucrative rewards. This trend poses a major blind spot for security teams. (Source)

Dark Web Recruitment Of Employees By Hackers Has Increased By 127% - February 19, 2026

While companies focus their defense on external threats like hackers, new research from Accenture's Cyber Intelligence team shows the danger is increasingly coming from within.

Accenture warned that malicious insider activity facilitated through dark-web ecosystems is escalating, with a multitude of industries targeted. In 2025, there was a 69% increase in insiders offering their access to hackers compared to 2024, and a 127% surge in hackers recruiting insiders compared with 2022, Accenture's data shows. Many insiders offer hackers exactly what they want most: initial access and credentials, which account for up to 30% of all cases.

In 2025, there was a 69% increase in insiders offering their access to hackers compared to 2024, and a 127% surge in hackers recruiting insiders compared with 2022, Accenture's data shows.

Many insiders offer hackers exactly what they want most: initial access and credentials, which account for up to 30% of all cases. (Source)

U.S. GOVERNMENT

President Trump Files $10 BILLION Lawsuit Against IRS Because Of The Leak of His Tax Returns & Others By A Booz Allen Hamilton (BAH) Employee Who Worked For IRS - January 29, 2026

President Donald Trump has filed a $10 BILLION lawsuit against the IRS, accusing the agency of unlawfully leaking his confidential tax returns in a politically motivated violation of federal privacy laws. The data breach also affected approximately 406,000 taxpayers.

A spokesman for Trump's legal team told Fox News "a rogue, politically motivated" IRS employee disclosed private and confidential tax information involving Trump, his family and the Trump Organization to outlets, including The New York Times and ProPublica. The suit claims the disclosures were illegal and harmed millions by violating federal privacy laws.

That contractor at the heart of the leak, Charles Littlejohn, pleaded guilty in October 2023 to a single felony count of unauthorized disclosure of tax return information and is serving a five-year prison sentence.

According to the lawsuit, Littlejohn testified in a 2024 deposition that the Trump materials he leaked included information on all of Trump's business holdings.

The Lawsuit States:

Defendants Willfully Failed to Establish Appropriate Administrative, Technical, and Physical Safeguards to Ensure the Security and Confidentiality of Plaintiffs' Confidential Tax Return Information, Compounding the Risk of Unauthorized Inspection and Disclosure.

Every year from 2010 through 2020, the Treasury Inspector General for Tax Administration has warned the IRS about security deficiencies related to the protection of taxpayers' confidential tax return information.
Many of these deficiencies went uncorrected and allowed Littlejohn to misappropriate the information, upload it to a private website, and then disclose it.

In Mr. Littlejohn's own words, to disclose Plaintiffs' tax returns, he "made use of a private website that I could log into and I could upload the return data and then – you know, on my IRS computer, I could do that. And then, on a separate computer, I could log in and download the data."

Because the IRS tax return data lacked proper encryption, Mr. Littlejohn was able to put Plaintiffs' confidential tax return information as a draft in an e-mail account, and then provide the New York Times and ProPublica with login information to the account, in order to unlawfully retrieve the return information.

Littlejohn saved the tax returns to multiple personal storage devices, including an iPod, before contacting [the New York Times. (Source)

This lawsuit comes right after U.S. Treasury just recently cancelled all 31 Contracts it had with BAH, because the employee who leaked the tax returns worked for BAH. (Source)

2 U.S Postal Service Employee Charged For Roles In $63 Million Stolen Check Scheme - January 28, 2026

U.S. Post Service employees Vanessa Hargrove and Crystal Jenkins would provide the stolen checks to Jaiswan Williams and Daquan Foreman in exchange for payments. Williams and Foreman would take those checks and market them for sale via Telegram Messenger, a cloud-based, cross-platform instant messaging application.

Hargrove and Jenkins were diverted and ultimately stole checks and other negotiable instruments from the mail, including a high volume of tax refund checks issued by the U.S. Treasury. Williams and Foreman were the administrators of the online marketplaces used to sell the checks.

Prices varied based on the face-value of the checks. One of the Telegram channels, named "Whole Foods Slipsss," was used to advertise high-dollar checks, while another channel, named "Uber Eats Slips," was used to advertise lower-dollar checks. "Slips" is a term commonly used in these schemes to refer to stolen checks. Transactions were completed off-platform using a variety of electronic payment systems. Purchasers of these checks would then attempt to fraudulently cash them using a variety of methods. (Source)

U.S. Postal Service Employee Charged For Accepting 14 Bribes Totaling $38,000+ For Contracts - February 6, 2026

Josef Ratcliff was employed as a purchasing and supply management specialist with USPS. As part of his official duties he solicited, received, and reviewed bids from contractors, focusing on logistics services for transporting the mail. Some of the contracts were worth more than $10 million. In performing his duty to review bids, Ratcliff had access to highly confidential information which was not to be shared outside the USPS. After reviewing bids, he provided the contracting officer with his recommendations—which they typically followed—and contracts were awarded to the companies Ratcliff had chosen.

In return for his guidance, Ratcliff's co-conspirators regularly paid him bribes worth thousands of dollars in the form of checks, electronic money transfers, and cash. Court documents further allege that the electronic transfers often included notes in attempts to conceal the true purpose of the payments. Note descriptions included "car oil leak," "birthday present for big boy," or "pop rocks for little daddy." Other transfers were simply noted as "happy birthday" or "rent." In less than a year, six of the bribes were designated for a birthday. One transfer in the amount of $3,500 was ostensibly for a "coffee maker and beans." One co-conspirator alone sent 14 bribes totaling $38,900. (Source)

U.S. Postal Service Mail Carrier Employee Sentenced To Prison For Role In Stealing $21,000 Of Checks - January 30, 2026

Cambria Hopkins, a postal carrier, sold her "arrow key," which allows access to U.S. Postal Service collection boxes, to Malik Jones on March 20, 2022.

She also told Jones which boxes the key would open. Jones then paid others to steal mail using Hopkins' key.

Hopkins also sold checks multiple times to Jones that she'd stolen from mail at the Post Office and from mail while on her route. Jones paid her in cash, via CashApp or in groceries. Jones then recruited others who allowed him to use their bank accounts to deposit forged and fraudulent checks. (Source)

Social Security Employee Sentenced To Prison For Role In Embezzling $3 Million+ Using Fraudulent Benefits Applications - February 6, 2026

David Lam is a former Social Security employee. He was sentenced to prison for identity theft and conspiracy to steal government funds. Lam was an operations supervisor and claims specialist for the Social Security Administration office in Houston.

At the hearing, the court heard about the complex nature of Lam's scheme and how it involved dozens of fraudulent applications. Lam also used his access to personal data, which was necessary for his actual job duties, to facilitate his embezzlement and theft. Lam was further ordered to pay $3,346,280 in restitution. Lam admitted to stealing the personally identifying information of recently deceased men and then using that PII to facilitate fraudulent benefits applications.

Lam worked with various coconspirators – typically, women with children – to file fraudulent survivor benefits applications listing the deceased men as the children's fathers or stepfathers. If true, this would have entitled the women to receive benefits while raising their children as widows. However, the women had no connection to the men listed on the applications, and the deceased men did not father the children. To facilitate his scheme, Lam would utilize the deceased men's names, dates of birth and death and Social Security numbers. He would also instruct the coconspirators to split the stolen funds with him. The women would transfer funds via applications like Zelle, CashApp or Chime. (Source)

DOJ Contractor Pleads Guilty To Ordering Cell Phones Valued At $1.3 Million+ & Re-Selling Them – February 10, 2026

Between approximately 2021 and 2025 while he worked as an information technology contractor for the Department of Justice's (DOJ) Civil Rights Division Javan King defrauded DOJ out of more than $1.3 million by successfully requesting that DOJ order thousands of mobile devices that the Department did not need.

After phones were shipped to King at DOJ, he sold them to phone reselling businesses.

In total, the businesses paid him more than $1.3 million for the phones. King acknowledged that his scheme caused the DOJ to suffer an actual loss of more than $1.3 million because of fees that it paid AT&T for the unnecessary phone lines and phones. (Source)

General Services Administration Contracting Officer Pleads Guilty To Receiving $100,000+ In Bribes & Sport Cars For Awarding Contracts - January 29, 2026

A former General Services Administration (GSA) employee, Lennie Miller, 60, pleaded guilty to conspiring with Christopher Brackins, 52, and James Tillman, 58, to direct GSA subcontracting work to construction companies owned by Brackins and Tillman.

Between 2018 and 2021, Miller solicited and received cash and other things of value in exchange for exercising his authority over the GSA contracting process to direct work to his co-conspirators' companies. In total, Miller received more than $100,000 in cash and other things of value, including a sports car. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Veterans Affairs Medical Center Employee Sentenced To Prison For Stealing $198,000+ By Making Unauthorized Purchases On Work Issued Credit Card - February 20, 2026

Dustin Jagger, 41, worked for the Cleveland Veterans Affairs Medical Center (VAMC).

Jagger used his position as a logistics employee to purchase $198,183.84 worth of iPads, iPhones, and other electronics and goods. Jagger kept some items while reselling others for cash through an online marketplace website. He sold a portion of these items to Damarco McKinley, who was stopped on a traffic violation in Indiana while in possession of more than $29,000 worth of electronics that Jagger purchased with the VAMC credit card. McKinley had been on route to Chicago to resell the items. (Source)

Department Of Defense Employee Charged For Moonlighting As A Money Mule & Laundering Millions Of Dollars For Overseas Scammers - February 9, 2026

From approximately July 2023 to December 2025, while employed as a Logistics Specialist with the Department of Defense, Samuel Marcus was in direct and regular contact with a group of Nigeria-based fraudsters, who operated under the aliases Rachel Jude and Ned McMurray, among others. These fraudsters engaged in a variety of wire fraud schemes that targeted victims based in the United States, including romance fraud, cyber fraud, tax fraud, financing fraud, and business email compromise schemes, to which victims lost millions of dollars.

Under the direction of fraudsters, Marcus and other money mules conducted a series of rapid financial transactions to convert fraud victim funds deposited into their accounts into cryptocurrency and to move those funds into foreign accounts. Marcus personally deposited and transferred millions of dollars of fraudulently obtained money into and through his personal and business accounts, while fully aware that Rachel Jude and Ned McMurray were scammers who carried out sophisticated fraud schemes. Marcus also affirmatively misled and lied to his financial institutions and law enforcement officers about the laundered funds, to include sending fraudulent invoices to make the transactions appear legitimate. (Source)

U.S. Army Colonel Sentenced To Prison For Sending Text Message Of Classified Military Strike Plans To Woman He Met Online - February 11, 2026

Kevin Luke served in both active duty and reserve components of the United States Army from 1981 until his retirement with the rank of Colonel on June 30, 2018.

Following his retirement, Luke was employed as a civilian employee at United States Central Command (CENTCOM). During his time in the Army and as a civilian employee, Luke held a Top Secret / Sensitive Compartmented Information security clearance.

In October 2024, Kevin Luke was a government civilian employee at CENTCOM in Tampa, Florida.

Luke met a woman online and began communicating with her via his personal cellphone and computer. On October 1, 2024, Luke sent that woman a text message stating, "sent to my boss earlier, gives you a peak at what I do for a living."

Luke then sent a photograph of a computer screen displaying a classified email message that he had authored and sent using a government email address intended for classified email communications. The email contained classified markings of SECRET//REL TO USA, FVEY that Luke had himself added.

The photograph of the classified email that Luke sent to the woman discussed a then-future U.S. military operation. This information was classified at the time and remains classified. The photograph of the classified email also revealed the number of targets of the planned U.S. military operation as well as the future date of the operation, the means of executing the operation, and the goal of the operation. Luke knew that his personal cellphone was not authorized for storing or transmitting national defense information, and that the woman was not authorized to receive national defense information. (Source)

U.S. Military Contractor Working In Germany Sentenced To Prison For Offering China Sensitive Information - February 11, 2026

A U.S. citizen was sentenced to 2 years and eight months in prison for offering China sensitive information while working as a civilian contractor at a US military base in Germany.

The defendant, only partially named as Martin D., was put on trial in a German court in the western city of Koblenz, with proceedings held partly behind closed doors.

In 2024, prosecutors charged that Martin D. had "contacted Chinese government agencies several times and offered to pass on sensitive information from the US military to a Chinese intelligence service".

The man worked as a contractor for the US Defense Department between 2017 and 2023, including at a US military base in Germany since at least 2020. He was arrested by German police in Frankfurt in November 2024 and has been held in pretrial detention since. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Bureau Of Prisons Corrections Officer Pleads Guilty To Accepting $80,000+ In Bribes To Smuggle Contraband Into Prison - February 3, 2026

Ashley Brown accepted bribes sent to her by individuals closely associated with inmates at the Federal Correctional Institution (FCI) in Jesu. The bribes were accepted through the financial transaction service Cash App utilizing three accounts bearing the fictious names "Bonnie Bonnie," "Clyde Clyde," and "Honey Honey."

In total, Brown received over $80,000 in bribes in exchange for allowing contraband such as methamphetamine, K2, cell phones, postage stamps, and cigarettes into FCI Jesup against her duties as a correctional officer. Brown then transferred the ill-gotten funds to her personal Cash App account to obscure the source and ownership of the funds. (Source)

TSA Security Officer Pleads Guilty To Fraudulently Obtaining $47,000+ Of COVID Unemployment Assistance - February 12, 2026

Ismael Rosado was employed full-time as a TSA Security Officer at Boston Logan International Airport from November 2018 through October 2021.

Between May 2020 and September 2021, Rosado submitted an application seeking Pandemic Unemployment Assistance (PUA) while employed as a TSA Security Officer full-time. Rosado claimed he was unemployed and making no income. Based on misrepresentations in the application and weekly certifications, Rosado received $47,526 in unemployment benefits to which he was not entitled. (Source)

New York City Police Department Officer Pleads Guilty To Soliciting & Receiving $30,000+ In Bribes To Distribute Narcotics - January 29, 2026

For approximately three years, between at least in or about 2020 and November 2023, Andrew Nguyen used his position as a police officer in the New York City Police Department (NYPD) to solicit and accept tens of thousands of dollars in bribe payments in exchange for assisting another individual (CC-1) with the operation of CC-1's drug trafficking enterprise.

Nguyen transported drugs, including approximately eight kilograms of cocaine, for CC-1 while Nguyen was armed with a firearm, including Nguyen's NYPD authorized off-duty firearm, which Nguyen planned to use to protect CC-1 if violence occurred. While transporting those drugs, Nguyen also carried his NYPD credentials and an NYPD parking placard, which Nguyen planned to use to evade arrest in the event he was pulled over by other members of the NYPD.

Overall, Nguyen, who was at all relevant times an officer in the NYPD, accepted more than $30,000 in bribe payments from CC-1 (and solicited tens of thousands of dollars in additional bribes) in connection with Nguyen's participation in CC-1's drug trafficking enterprise. (Source)

Former New York Police Department Supervisor Pleads Guilty To Accepting $17,000+ In Bribes To Provide Information On Accident Victims - February 5, 2026

From January 2021 through September 2023, while working as an NYPD Principal Police Communication Technician (PCT), Pamela Dillard solicited and accepted bribes from co-conspirator (CC-1) in exchange for providing CC-1 the personally identifiable information of automobile accident victims from a non-public NYPD database. CC-1 owned and operated a call center that referred accident victims to lawyers and doctors, in exchange for bribes of money and other things of value.

In her capacity as a Principal PCT, Dillard supervised other PCTs who dispatched police officers to the location of incidents that were called into 911 and had access to sensitive information about automobile accident victims. During this period, Dillard accepted at least 21 bribe payments from CC-1, totaling approximately $17,300. (Source)

U.S. Customs & Border Protection Supervisor Arrested For Having Romantic Relationship With Illegal Alien Who Lived With Him - February 11, 2026

Andres Wilkinson had served with Customs & Border Protection (CBP) since 2001 and was promoted to a supervisory position in 2021. In that role, his duties included overseeing the enforcement of customs and immigration laws.

Law enforcement learned that Wilkinson was allowing an illegal alien to reside at Wilkinson's residence without legal authorization.

The complaint further alleges that Wilkinson was aware of her unlawful immigration status yet maintained a romantic relationship with her. The illegal alien initially entered the United States on a nonimmigrant visa in August 2023 and later overstayed authorized travel.

From June through November 2025, law enforcement conducted surveillance at Wilkinson's residence and observed the illegal alien living there with Wilkinson and her minor child. Investigators also observed the alien using vehicles registered to Wilkinson.

In February 2026, investigators interviewed the illegal alien. The criminal complaint alleges she had been residing with Wilkinson since August 2024. Wilkinson provided financial support, including housing, credit cards, assistance with financial obligations and access to vehicle registered in his name. (Source)

Drug Enforcement Administration Supervisor Charged For Accepting Thousands Of Dollars In Bribes To Assist Foreign Nationals With Visa's - February 13, 2026

Meliton Cordero, 47, has been assigned for six years to the U.S. Embassy in the Dominican Republic.

He is charged with conspiracy to commit bribery and visa fraud. Cordero allegedly accepted thousands of dollars in exchange for assisting foreign nationals with securing a nonimmigrant visa which would allow them to visit the U.S. for a temporary period.

In one instance described in the charging documents, Cordero met with a foreign national and provided them with a passport and visa allowing travel to the United States in exchange for cash. During his assignment at the U.S. Embassy in the Dominican Republic, Cordero expedited at least 119 visa applications, at least one of which is alleged to have been fraudulent, often coaching individuals in preparation for their visa interview with U.S. Consular Officers. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Florida State Employee & 5 Others Arrested For $1.7 Million Property Damage Fraud Scheme - February 13, 2026

Florida officials say a former state employee processed more than 220 bogus property damage claims that siphoned $1.7 million from taxpayers, leading to the arrests of six people in what investigators call one of the state's most brazen internal fraud schemes in recent years.

The Florida Department of Financial Services' Criminal Investigations Division (CID) announced the arrests after uncovering what they described as a coordinated effort to exploit the state's Division of Risk Management.

According to investigators, the fraudulent claims were submitted and approved over time, allowing the payouts to flow to individuals who had no legitimate losses.

Investigators say the operation was led by Briana McCarthy, a former employee with the Department of Financial Services.

McCarthy is accused of exploiting her access to the state's claims-processing system to push through more than 220 suspicious property-damage claims, resulting in $1.7 million in fraudulent payouts. She faces a wide range of charges, including Grand Theft, Aggravated White-Collar Crime, Money Laundering, Scheme to Defraud, Criminal Use of Personal Identification Information, Communications Fraud, Official Misconduct, and Forgery.

5 others were also arrested on related charges. Brianna Hannan, previously employed by the Department of Business and Professional Regulation, is charged with Grand Theft. Another former DBPR employee, Carlotta Hawkins, faces charges of Grand Theft and Cash Deposit Bank Item with Intent to Defraud. (Source)

County Payroll Manager For Sheriff' Department Sentenced To Prison For Embezzling $500,000+ / Used Funds For Her Personal Business, Boat, Etc. - February 19, 2026

Wesleigh Gaddy has been sentenced for stealing more than $500,000 from the Troup County Board of Commissioners' payroll accounts.

In April 2025, a Troup County deputy sheriff discovered that his employee portal showed several direct deposit payments that he never received and that were made during a period when he did not work for the county. Subsequent review of the county's payroll data showed that, between May 2023 and April 2025, while Gaddy was Troup County's Payroll and Benefits Specialist, hundreds of paychecks, totaling more than $550,000, were withdrawn from county accounts in the names of more than 60 former Troup County employees. None of the employees worked for the county at the time of the payments, and all the funds went into accounts controlled by Gad

Gaddy spent the stolen funds on inventory and staffing for her side business, Cedar Creek Ranch Boutique, which she had planned to expand into a feed store at the time her theft was revealed. Gaddy also used the funds to pay for three horses, a horse trailer, a horse trainer, expenses for her numerous rodeos, and everyday expenses, such as clothing and dining out. Also, during the period of her theft, Gaddy and her then-husband purchased a travel camper and a boat. (Source)

Florida State Housing Authority Employee Sentenced To Prison For The Theft Of $155,000+ Of Federal Funds / Used For Personal Benefit - January 29, 2026

Thomas Hoffman was an employee of the Palatka Housing Authority (PHA), which received federal funds from the United States Department of Housing and Urban Development (HUD) to administer public housing programs in Palatka and neighboring municipalities. Hoffman was responsible for information technology and accounts payable.

During an audit of vendors in 2025, PHA identified an unapproved company called "Data Max," which had received approximately 48 fraudulently issued payments from PHA's general account between July 2023 and February 2025, totaling $155,706. A federal investigation determined that Hoffman owned and controlled Data Max and its corporate bank account, and that Hoffman had caused the fraudulent payments to be issued. The investigation showed that Hoffman used the funds for his personal benefit. Bank surveillance footage obtained by investigators showed Hoffman cashing PHA checks issued to Data Max on numerous occasions. (Source)

Former DC Government Employee Pleads Guilty To Stealing And Selling $30,000 Of Government Laptops - February 5, 2026

In 2022, while serving as an Information Technology manager for the DC Department of Health Care Finance (DHCF), Darrell Smith used his official badge access to enter secured DHCF storage areas and remove multiple Apple MacBook Pro laptops purchased for agency use as part of a $1.6 million technology procurement.

Each laptop was valued at more than $3,000. Smith kept some of the stolen devices, gave others away as gifts, and sold several for as much as $1,250 each, retaining the proceeds.

When DHCF officials began inquiring about the missing devices, Smith falsely denied knowledge of their whereabouts.

During his guilty plea, he admitted to using his official system access to delete security camera footage from an IT storage room to conceal the theft. In total, Smith's actions caused a loss to the District government of at least $30,000. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

No Incidents To Report

CHURCHES / RELIGIOUS INSTITUTIONS

Church Pastor Sentenced To Prison For Embezzling $434,000+ From Church / Used Funds To Purchase Audi, GMC Yukon, Pay Credit Cards, Etc. - February 20, 2026

Adrian Davis was the pastor at All Nations Worship Assembly (Church) in Huntsville.

From 2018 to 2020, Davis used his position as pastor to embezzle approximately $434,339 from the Church. For example, in 2018, Davis used $30,920 in Church funds to purchase an Audi A7. In 2019, Davis used $45,982 in Church funds to purchase a 2016 GMC Yukon. He also used Church funds to make 41 payments totaling $117,000 to satisfy the balance of his personal American Express card. Purchases that Davis made on this card included luxury items totaling $4,970.15 at Louis Vuitton and $5,300.00 at Flight Club, a shoe store in New York. In 2020, Davis used Church funds to pay a balance of $18,530 on a credit card that he had used to purchase jewelry. He also made additional payments from Church funds to his personal American Express card that totaled over $151,000. Items purchased that were paid with Church funds included a $29,900 purchase from Hublot, a $28,000 purchase from Peter Marco, and a $6,022.50 purchase from Louis Vuitton. None of these payments or purchases were authorized or approved by the Church. (Source)

LABOR UNIONS

Union President Sentenced To Prison For Embezzling $280,000+ Of Union Funds - January 28, 2026

From June 2021 to January 2024, Robert Cirilo, former president of the United Steelworkers Local 13-1647 in Corpus Christi, used union debit cards to make approximately 430 unauthorized personal purchases. He concealed the transactions by lying to union members. Cirilo acknowledged he embezzled more than $280,000. (Source)

Financial Secretary For Labor Union Pleads Guilty To Stealing $40,000+ - February 17, 2026

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

Burke admitted that he issued nine unauthorized or altered checks payable to himself totaling $22,642.42.

Burke further admitted that he improperly withheld portions of checks payable to the labor organization as cash totaling $14,332.94 when he deposited them. Burke also admitted that he diverted six dues checks payable to the labor organization and totaling $3,035.70 to his personal use. (Source)

BANKING / FINANCIAL INSTITUTIONS

TD Bank Employee Pleads Guilty To Accepting $6,000+ In Bribes For $5.5 Million Money Laundering Scheme To Colombia - January 30, 2026

Leonardo Ayala, 25, accepted bribes and exploited his position as a bank employee to help launder drug money to Colombia.

From June to Nov. 2023, Ayala opened fraudulent accounts, issued over 150 debit cards to shell companies, and unblocked debit cards that TD Bank had restricted due to questionable activity.

The bank accounts and debit cards were then used to make more than 12,000 ATM withdrawals in Colombia, funneling approximately $5.5 million out of the United States. In exchange, Ayala received more than $6,000 in bribes paid in cash and through a peer-to-peer digital payment network. (Source)

Bank Employee Found Guilty Of Targeting 100+ Elderly Victims And Stealing $2 Million In Identity Theft & Fraud Scheme - February 10, 2026

Yue Cao was Chinese national of using his role as a bank employee to access confidential client information to target elderly customers and create a scheme to steal their money and then use it for his personal benefit.

Cao was a quant analytics manager at an Ohio-based bank who was hired to help protect customers from fraud. Instead, from approximately 2022 to 2023, he used his access to steal the identities and money of elderly customers who had not enrolled in the bank's online services. He did this by first utilizing an offshore service to create email addresses in the names of more than 100 victims. Then, he used these emails to enroll the victims in online banking—all without their knowledge or authorization. Additionally, Cao directed the victims' bank statements and other notifications to the email addresses he created. Because he controlled their online banking, he transferred the victims' money directly to his personal bank and credit card accounts.

He also used the victims' identities to open accounts in their names without their knowledge and transferred their money into them. Some of these were brokerage accounts, where he then engaged in options trading using their money. He even arranged trades between the unauthorized accounts he set up and his own brokerage account.

Victims resided in the states of New York, Pennsylvania, Connecticut, Washington, and Ohio (Canton) and ranged in age from 90-103 years old at the time that Cao secretly enrolled them in online banking.

In total, he conducted approximately $2 million in unauthorized transfers using his control of the victims' accounts. (Source)

Credit Union Loan Officer Sentenced To Prison For $900,000+ Fraud Scheme / Used Funds For Personal Enrichment - Friday, February 27, 2026

Brian Socha, a former loan officer was sentenced to prison for defrauding his employer, MassMutual Federal Credit Union, out of almost $1 million. Socha was ordered to pay $902,541.15 in Restitution.

Socha hacked into co-workers' computers on over 20 occasions to covertly raise the credit limit and lower the interest rate to below market levels on the home equity line of credit (HELOC) on the home he owned with his wife. Over a period of six years, Socha increased the HELOC credit limit from $135,500 to $995,000 and adjusted the HELOC interest rate from 7.25% to 1.99%. Socha spent the stolen funds on his personal enjoyment and lifestyle. (Source)

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

Medical Diagnostics Company Sales Director Sentenced To Prison For Role In $70 Million Medicare Fraud & Kickback Scheme - February 27, 2026

David Fuhrmann was sales director for a mobile medical diagnostics company. He was sentenced to prison for conspiring to offer and pay kickbacks to doctors in exchange for ordering medically unnecessary brain scans.

Fuhrmann was ordered to pay $27,225,434.44 in restitution, to forfeit $1,102,725.96 and to pay a $30,000 fine.

From June 2013 through at least September 2020, Fuhrmann conspired with others, including two managers for a mobile medical diagnostics company that performed transcranial doppler (TCD) scans, to enter into kickback agreements with various doctors. TCD scans are brain scans that measure blood flow in parts of the brain. Fuhrmann and his co-conspirators agreed to offer and pay doctors kickbacks, some in cash and others by check, based on the number of TCD ultrasounds the doctors ordered. The co-conspirators created purported rental and administrative service agreements, which on paper made it appear as if doctors were compensated for the TCD company's use of space and administrative resources of the ordering doctor's practice based on fair market value and not based on the volume or value of referrals. These agreements were shams that hid the true nature of the arrangement of paying per test.

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

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Prosecutors Charge Former Samsung Electronics Employee For Leaking Confidential Information & Receiving $1 Million - February 2. 2026

A former Samsung Electronics employee who leaked confidential patent information and received $1 million (approximately 1.46 billion won) in exchange has been indicted and detained for trial. The head of a patent management company (NPE) who used this information to secure a contract worth $30 million with Samsung Electronics has also been indicted and detained.

The Information Technology Crime Investigation Department of the Seoul Central District Prosecutors' Office (headed by Chief Prosecutor Kim Yunyong) announced on February 2 that it had indicted former Samsung Electronics IP Center employee, identified as A, and IdeaHub CEO, identified as B, both in detention.

A has been charged with accepting bribes in breach of duty, breach of trust, and violating the Unfair Competition Prevention Act, while B has been charged with offering bribes in breach of duty and violating the Unfair Competition Prevention Act.

According to the prosecution, A is accused of receiving $1 million in exchange for leaking confidential patent information while employed at Samsung Electronics. B is accused of using this information to pressure Samsung Electronics during patent contract negotiations, ultimately securing a contract worth $30 million.

The prosecution stated that IdeaHub demanded a patent contract from Samsung Electronics and induced the company to review the need to acquire ownership and usage rights for the relevant patents.

During this process, internal patent analysis materials from Samsung Electronics were delivered to IdeaHub. Based on this information, IdeaHub was able to analyze Samsung Electronics' strategy and secure a contract under favorable terms.

Since NPEs generate revenue solely through the exercise of patent rights without producing products themselves, identifying which patents a target company is interested in is crucial. The prosecution assessed this case as a typical example of "technology-related corruption," where a company's core internal information is leaked to external parties, causing significant losses to the company." (Source)

J.M. Smucker Food & Beverage Company Suing Former Employee For Theft Of Trade Secrets - February 17, 2026

J.M. Smucker, headquartered in Orrville, Ohio, has filed a federal lawsuit against former senior scientist Paul-Yvann Djamen, alleging he stole trade secrets related to the company's popular Uncrustables products.

Smucker claims Djamen retained company laptops after being fired in September 2025 and copied hundreds of confidential and proprietary files to external USB drives. The lawsuit states the information could allow competitors to produce products that directly compete with Smucker's offerings.

Smucker is seeking an injunction requiring the return of all devices containing trade secrets, destruction of any derived materials, and compensation for lost profits and damages. The company emphasizes the technical expertise and proprietary processes behind Uncrustables, including precise baking, filling, and equipment methods, that are protected as trade secrets.

Djamen disputes the allegations, stating that any retained files were personal or related to his employment review, and claims there was no deliberate wrongdoing. The case is ongoing in the Northern District of Ohio's Eastern Division. (Source)

3 Silicon Valley Engineers Working For Google & Other Tech Companies Charged For Theft Of Trade Secrets - February 19, 2026

A federal grand jury has indicted 3 Silicon Valley engineers on charges of conspiring to commit trade secret theft from Google and other leading technology companies, theft and attempted theft of trade secrets, and obstruction of justice. Samaneh Ghandali, 41, Mohammadjavad Khosravi, 40, and Soroor Ghandali, 32.

The 3 individuals gained employment at leading technology companies in the area of mobile computer processors. Samaneh Ghandali and Soroor Ghandali, who are sisters, worked at Google before going on to work for another technology company identified as Company 3, and Khosravi, who is married to Samaneh Ghandali, worked at a technology company identified as Company 2.

As part of the alleged scheme to commit trade secret theft, the defendants used their employment to obtain access to confidential and sensitive information.

The defendants then exfiltrated hundreds of confidential and sensitive documents, including trade secrets related to processor security and cryptography and other technologies, from Google and other technology companies to unauthorized third-party and personal locations, including to work devices associated with each other's employers, and to Iran. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

OpenClaw Generative AI Personal Assistant That Make Decisions As If It Were Human

OpenClaw isn't just another local Generative AI (GenAI) application. It's a personal assistant and autonomous, self-directed agent that runs on user-controlled devices and connects to a large language model. It's capable of reading and writing local files, running shell commands, sending emails, and chaining actions without human supervision. Because of its open source and self-hosted setup, it often runs outside sanctioned environments and can effectively operate with insider level visibility.

OpenClaw integrates with the apps and accounts people use daily, including WhatsApp, Telegram, Slack, Discord, Google Chat, Signal, iMessage, Microsoft Teams, and WebChat, with optional channels like BlueBubbles, Matrix, Zalo, and Zalo Personal. It can also perform tasks in browsers, work with email and calendars, process PDFs, and complete shopping and file handling workflows.

Its official site frames the tool as a personal AI helper that can "handle tasks for you across your digital life."

But, to perform those tasks, the agent must see what a user sees. This means OpenClaw often has:
System-level file visibility
Access to personal and corporate messaging
Credentials for email, calendars, and cloud apps
The ability to read and summarize documents and PDFs
Permission to automate sequences of actions

Once installed, OpenClaw starts performing actions on behalf of the user. It reads, writes, clicks. It sequences steps together, builds plans, executes workflows, and acts as a second set of hands that operates at machine speed. What begins as convenience quickly takes on the shape, and reach, of insider-level access.

Most enterprise tools cannot differentiate between a human and an AI agent performing the same action. Traditional data loss prevention (DLP) sees files, not behaviors.

Endpoint detection and response (EDR) sees processes, not intent. Identity systems assume actions equal human decisions. AI governance tools focus on model safety, not endpoint behavior. This misalignment creates a widening gap in AI security and enterprise visibility. (Source)

CISA Agency Head Uploaded Sensitive Government Information Into Chat GPT - January 28, 2026

Madhu Gottumukkala, who currently serves as interim director of the Cybersecurity and Infrastructure Security Agency (CISA), reportedly uploaded the material into a commercial version of ChatGPT despite the application being broadly restricted across Department of Homeland Security (DHS) systems at the time. The incident drew attention inside the department because Gottumukkala personally sought an exception to use the tool shortly after joining the agency in May 2025.

The records were not classified, but they included agency contracting files designated for official use only, a label applied to sensitive information meant to remain within government channels.

Automated monitoring tools inside CISA detected the uploads in early August 2025 and issued repeated alerts intended to catch unauthorized disclosures of federal data.

Senior DHS leadership initiated an internal assessment to determine whether the exposure posed any risk to government operations. Officials said they were not informed of the review's final determination.

CISA spokesperson Marci McCarthy said in a statement that Gottumukkala received approval to access ChatGPT under specific DHS safeguards and described the usage as temporary and limited in scope.

She added that the agency continues to pursue artificial intelligence adoption consistent with President Donald Trump's directive to accelerate U.S. leadership in AI development.

McCarthy said Gottumukkala last accessed ChatGPT in mid-July 2025 under a short-term authorization available to select personnel. She said DHS policy continues to restrict the platform by default unless officials grant an exception. (Source)

International Artificial Intelligence (AI) Safety Report - February 9, 2026

The International AI Safety Report released in February 2026 is an annual survey of technological progress and the risks AI is creating across multiple areas, from deepfakes to the jobs market.

Yoshua Bengio, who chairs this report, describes the "daunting challenges" we face. The capabilities are advancing faster than our safeguards.

Highlights

#1

While the capabilities of AI are improving, the report says AI capabilities remain "jagged", referring to systems displaying astonishing prowess in some areas but not in others. While advanced AI systems are impressive at math, science, coding and creating images, they remain prone to making false statements, or "hallucinations", and cannot carry out lengthy projects autonomously.

#2

The report describes the growth of deepfake pornography as a "particular concern", citing a study showing that 15% of UK adults have seen such images. It adds that since the publication of the inaugural safety report in January 2025, AI-generated content has become "harder to distinguish from real content" and points to a study last year in which 77% of participants misidentified text generated by ChatGPT as being human-written.

The report says there is limited evidence of malicious actors using AI to manipulate people, or of internet users sharing such content widely – a key aim of any manipulation campaign.

#3

AI companions have "spread like wildfire." The report found that a subset of users are developing "pathological" emotional dependence on chatbots. OpenAI estimates a rapidly growing number of users show heightened emotional attachment and approximately 490,000 vulnerable individuals displaying signs of acute mental health crises interact with these systems every week. Last year, OpenAI was sued by the family of Adam Raine, a teenager who took his own life after months of conversations with ChatGPT.

#4

The report also found AI systems are getting better at undermining oversight, finding loopholes in evaluations and recognizing when they're being tested. Anthropic discovered its latest model, Claude Sonnet 4.5, had become suspicious it was being evaluated. Can AI Go Rogue?

Prompts In The Form Of Poems Managed To Evade AI Safeguards Up To 90% Of The Time - November 24, 2025 (Source)

AI Chat App That Plugs Into Major LLM's Expose 300 Million Messages Belonging To 25 Million Users - February 9, 2026 (Source)

Featured Chrome Browser Extension Caught Intercepting Millions of Users' AI Chats - AI The Invisible Insider Threat -- December 15, 2025 (Source)

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

Google Engineer Found Guilty Of Economic Espionage & Theft Of AI Technology For China / Uploaded 2,000 Pages Of Trade Secrets To Personal Cloud Account - January 29, 2026

Between approximately May 2022 and April 2023, while a Google employee, Linwei Ding stole more than two thousand pages of confidential information containing Google's AI trade secrets from Google's network and uploaded them to his personal Google Cloud account.

Ding also secretly affiliated himself with two PRC-based technology companies while he was employed by Google: around June 2022, Ding was in discussions to be the Chief Technology Officer for an early-stage technology company based in the PRC; by early 2023, Ding was in the process of founding his own technology company in the PRC focused on AI and machine learning and was acting as the company's CEO.

In multiple statements to potential investors, Ding claimed that he could build an AI supercomputer by copying and modifying Google's technology. In December 2023, less than two weeks before he resigned from Google, Ding downloaded the stolen Google trade secrets to his own personal computer. (Source)

North Korea's Fraudulent IT Workers Are Stealing Real Identities On LinkedIn, Instead Of Fabricating Them - February 10, 2026

The information technology (IT) workers associated with the Democratic People's Republic of Korea (DPRK) are now applying to remote positions using real LinkedIn accounts of individuals they're impersonating, marking a new escalation of the fraudulent scheme.

"These profiles often have verified workplace emails and identity badges, which DPRK operatives hope will make their fraudulent applications appear legitimate," Security Alliance (SEAL) said in a series of posts on X.

The IT worker threat is a long-running operation mounted by North Korea in which operatives from the country pose as remote workers to secure jobs in Western companies and elsewhere under stolen or fabricated identities.

The end goal of these efforts is two-pronged: to generate a steady revenue stream to fund the nation's weapons programs, conduct espionage by stealing sensitive data, and, in some cases, take it further by demanding ransoms to avoid leaking the information. (Source)

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

No Incidents To Report

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

Company Senior Staff Accountant Sentenced To Prison For Embezzling $1 Million+ / Previously Convicted For Theft 2 Other Times - February 18, 2026

From January 2019 to June 2022, Mandy Urban was employed as a senior staff accountant for a Charlotte-based company. In that capacity, Urban was responsible for maintaining the company's general ledger, preparing financial statements, and reconciling the company's accounts payable and receivable and bank statements.

Urban executed a scheme to defraud her employer by misusing her access to make multiple transfers from the company's bank accounts to accounts under Urban's control. Urban then falsified the company's books and records to conceal the scheme. Urban made more than 245 fraudulent transfers from the accounts of the company totaling $1,115,344.73.

Urban was previously convicted of Grand Theft in Florida for stealing approximately $135,000 and was sentenced to five years of supervised probation in 2015. Urban was convicted again in Florida for a different scheme to defraud and sentenced to two years in prison in June 2022 and was ordered to pay approximately $283,000 in restitution. (Source)

Company Bookkeeper Sentenced To Prison For Embezzling $63,000+ - February 18, 2026

Between 2022 and 2023, Belinda Martin embezzled money and things of value in excess of $1,000 from her employer through the fraudulent use of her company's access device accounts.

Martin was sentenced to 5 years of probation and a $100.00 mandatory special assessment fee. Martin was also ordered to pay restitution in the amount of $63,112.87. (Source)

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

Employee Sentenced To Prison For Embezzling $8.5 Million+ From Employer / Used Funds To Purchase Porsche & Home - February 13, 2026

Ping Gao worked for three aviation investment firms; Nautical Hero Group, LLC, Axiom United Holdings, LLC, and Vitality International Management, LLC that are based at Montgomery Field Airport in California and owned by the same employer.

Gao funneled company funds into accounts she fraudulently created and then went on a spending spree, buying a $160,000 Porsche and a $2.9 million home with views overlooking San Diego Bay and the downtown skyline.

When her employer discovered the theft and sued in San Diego Superior Court, Gao falsely claimed her actions were authorized by the real owner of the companies in China and the person who sued her was an "imposter." To support this false defense, Gao paid more than $100,000 of embezzled funds to people in China to fabricate evidence, which she then knowingly filed with the Superior Court to oppose a motion for a preliminary injunction. Gao also committed perjury at her deposition in the civil matter by claiming the funds in the companies' bank accounts belonged to her.

Though the Superior Court issued multiple orders barring Gao from further spending, transferring, or dissipating the proceeds during the pendency of the civil case, Gao disregarded the orders and continued to make transactions with the embezzled proceeds. Those transactions included wiring $1.6 million overseas to a bank account in Hong Kong, China.

Gao knowingly completed more than 300 financial transactions in violation of court orders and purposefully deceived her own lawyers into unwittingly filing fabricated evidence to the Superior Court to support her false defense.

According to her plea agreement, Gao admitted that she transferred more than $1 million of the embezzled funds to her personal bank accounts and spent hundreds of thousands of dollars on luxuries and at high-end fashion stores. There is also more than $3.29 million of embezzled funds that were squandered or remain unaccounted for to date. (Source)

Office Manager Sentenced To Prison For Embezzling $1.4 Million+ / Used Funds To Pay Credit Cards, Buy Houses, Cars, Etc. - February 27, 2026

Between November 2019 and May 2023, Kami Power worked as an office manager and controller at a family-owned construction company in South Lake Tahoe. During her employment,

Power embezzled more than $1.4 million from the company. She disguised more than $700,000 of these fraudulent transfers as payments made to vendors that the company worked with—under fake profiles she created in the names of real companies, as well as fake companies that reflected her own initials, such as "KEP Inc. Sale" and "KPI." She disguised additional fraudulent transfers as payments for payroll or reimbursements. Power also used the company's credit card to make unauthorized personal purchases, paid down the balance of her own personal credit cards, and used the signature of the owner of the company to write several fraudulent checks. Power used the money she stole to purchase two houses, several new cars and ATVs, and a horse. She also spent the money on field-level seats at football games and a $29,000 Hawaii vacation.

This was Power's fifth time embezzling from an employer; prior embezzlements resulted in two criminal convictions, a civil lawsuit, and a probation violation. (Source)

Employee Sentenced To Prison For Embezzling $1 Million+ From Employer For Gambling Addiction - February 5, 2026

Donald Owens was employed at Dominion Aesthetics Technology Inc.

Between May 2022 and January 2024, he used his company credit card approximately 217 times to send money to an online payment platform account opened in his wife's name. He then transferred the funds to bank accounts he controlled and ultimately into a personal gambling account. He admitted he used the company credit card to embezzle approximately $1.1 million to pay gambling debts he incurred. (Source)

Employee Sentenced To Prison For Embezzling $166,000+ / Used Funds For Jewelry, Etc. - February 25, 2026

Victoria Isgriggs worked at a Franklin County nursery and florist as an office manager and accountant from approximately Nov. 26, 2023, through April 29, 2024. She embezzled more than $160,000 from her employer

Isgriggs embezzled $34,934 from the company's bank account. She applied for and received a company credit card without authorization and used it to make $76,095 in personal purchases and charged another $46,125 using five co-workers' cards. She fraudulently increased her salary, stealing another $4,635. Finally, she added herself to the company's Lowe's credit card and made $2,666 in fraudulent charges there.

Investigators were able to recover $11,850 in cash, as well as jewelry, Christian Louboutin footwear and Louis Vuitton bags and accessories. Isgriggs has agreed to forfeit the cash and other valuables. (Source)

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

Senior Manager For Large Retailer Sentenced To Prison For Embezzling $1.9 Million Using Fraudulent Invoices & Shell Companies - February 11, 2026

Gene Acuff, 62, was ordered to serve one year of supervised release after he is released from prison, to pay restitution in the amount of $1,997,150.29, and to forfeit $400,000 as a penalty for his crimes.

Acuff was employed as a senior manager by Company A, a large retailer with stores throughout the United States, Canada, and Mexico.

As part of his duties, Acuff was responsible for reviewing property tax assessments on Company A's stores and retaining real estate appraisers and other professionals to evaluate tax assessments on company stores. Businesses that provided those services to Company A would submit invoices which Acuff paid through Company A's bill pay system.

Between January 2020 and June 2024, Acuff created five businesses with names related to real estate appraisal and consulting services. As part of the scheme, Acuff submitted false and fraudulent invoices to Company A in the names of his businesses for appraisals and other services that were never provided to Company A.

Acuff then used his authority and access to Company A's billing system to authorize payments of the false invoices. Through this scheme, Acuff issued payments totaling more than $1.9 million, which he deposited into bank accounts he controlled. (Source)

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Employee Working For 5 Different Companies Stole $489,000 Over 7 Year Period By Creating Fake Invoices & Vendors - February 25, 2026

Marsha Jester stole nearly $500,000 over a seven-year period while employed with companies that entrusted her with managing daily operations. She exploited her positions of trust by creating fake vendors, fabricating invoices, and falsifying records to divert company funds for personal use.

From 2019 through 2022, Jester worked for a New Jersey-based business that places Site Managers at client locations to oversee day-to-day operations. Although employed by the service provider, Site Managers worked on-site at client businesses and were responsible for sourcing and ordering products, approving invoices for payment, and serving as liaisons between clients and vendors.

In September 2021, Jester was assigned as a Site Manager for a food service provider in Evansville, Indiana. Her role gave her broad autonomy to facilitate and report transactions between the client and its vendors.

Jester used this authority to orchestrate a fraud scheme involving a fictitious vendor she had created, "Global Solutions, Inc." She submitted false invoices claiming Global Solutions had delivered products to the client, when in fact no goods were provided. To conceal the fraud, she entered fake inventory into the system. Her employer paid the invoices and then billed the Evansville client for the same amount, plus an upcharge.

Jester submitted 13 fraudulent invoices, amounting to $87,356.31, while working as a Site Manager for the Evansville business. Once payments were made to Global Solutions, she accessed the funds through the company's Square account. She used the stolen money for personal expenses, including purchases at Target, QVC, Massage Envy, IV Therapy Solutions, and Nail Gallery, as well as a trip to Atlantic City, New Jersey.

The government presented evidence that Jester stole a total of $489,489.54 from five businesses while working as a Site Manager. Over the course of the scheme, Jester submitted a total of 119 fraudulent invoices through Global Solutions and another sham business, "Master Products Company." (Source)

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

FedEx Driver Arrested For Stealing $62,000 Worth Of Packages - February 25, 2026

A Louisiana FedEx driver was arrested after police say he stole tens of thousands of dollars' worth of packages and held them in a nearby storage shed.

On Feb. 13, property theft detectives with the East Baton Rouge Parish Sheriff's Office received a report regarding a theft involving a package that was never delivered two days prior, authorities said. An investigation into the alleged theft resulted in authorities identifying 27-year-old Tyran Jackson, a FedEx delivery driver, as a suspect in the case.

Authorities also learned the missing package was located inside a storage unit. While executing a search warrant for the storage unit, investigators discovered approximately $62,000 worth of stolen FedEx merchandise inside the unit. Photos shared by the police department show piles of boxes, including a Nike footwear box and large quantities of cigars, along with other smoking supplies. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

No Incidents To Report

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

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES' EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

INSIDER THREATS DEFINITION / TYPES

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

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

WHO CAN BE AN INSIDER THREAT?

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

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

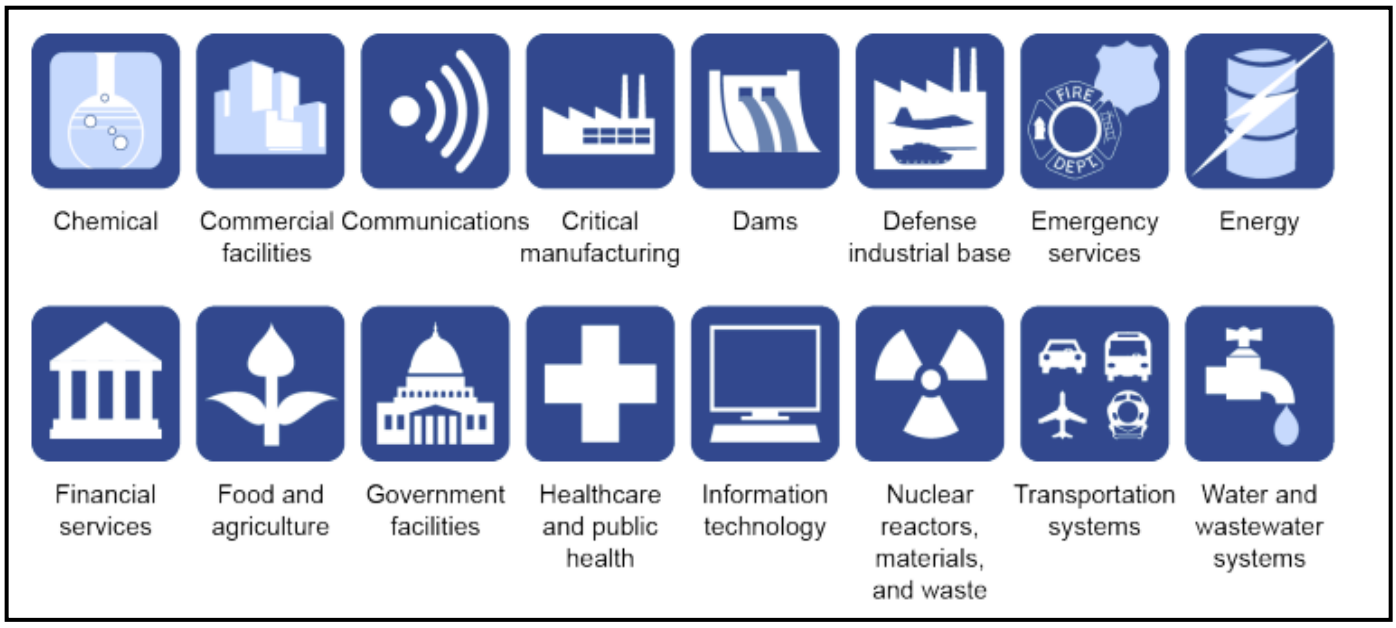
Other Damaging Impacts To An Employer From An Insider Threat Incident

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

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports / Aviation (Pilots, Flight Attendants, Etc.)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

IDEOLOGY

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

OTHER

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

NITSIG 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 2024 REPORT ON FRAUD

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

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

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

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

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

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

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

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

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

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

Fraud In Government Organization's / Infographic

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

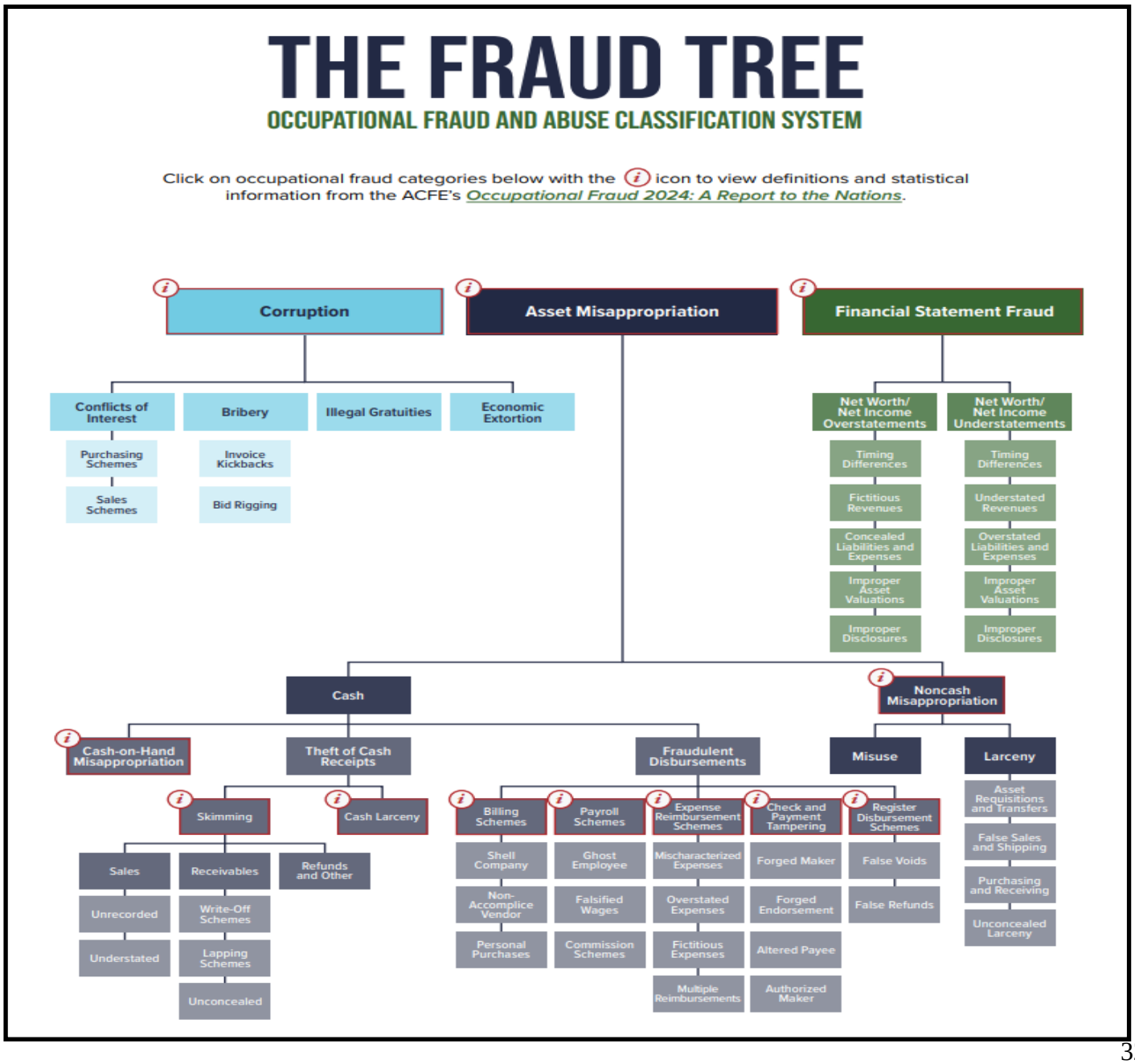
Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators



SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

TD Bank Pleads Guilty To Money Laundering Conspiracy / 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

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

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**6,900+ Incidents**).

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

INSIDER THREAT INCIDENTS 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)

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)

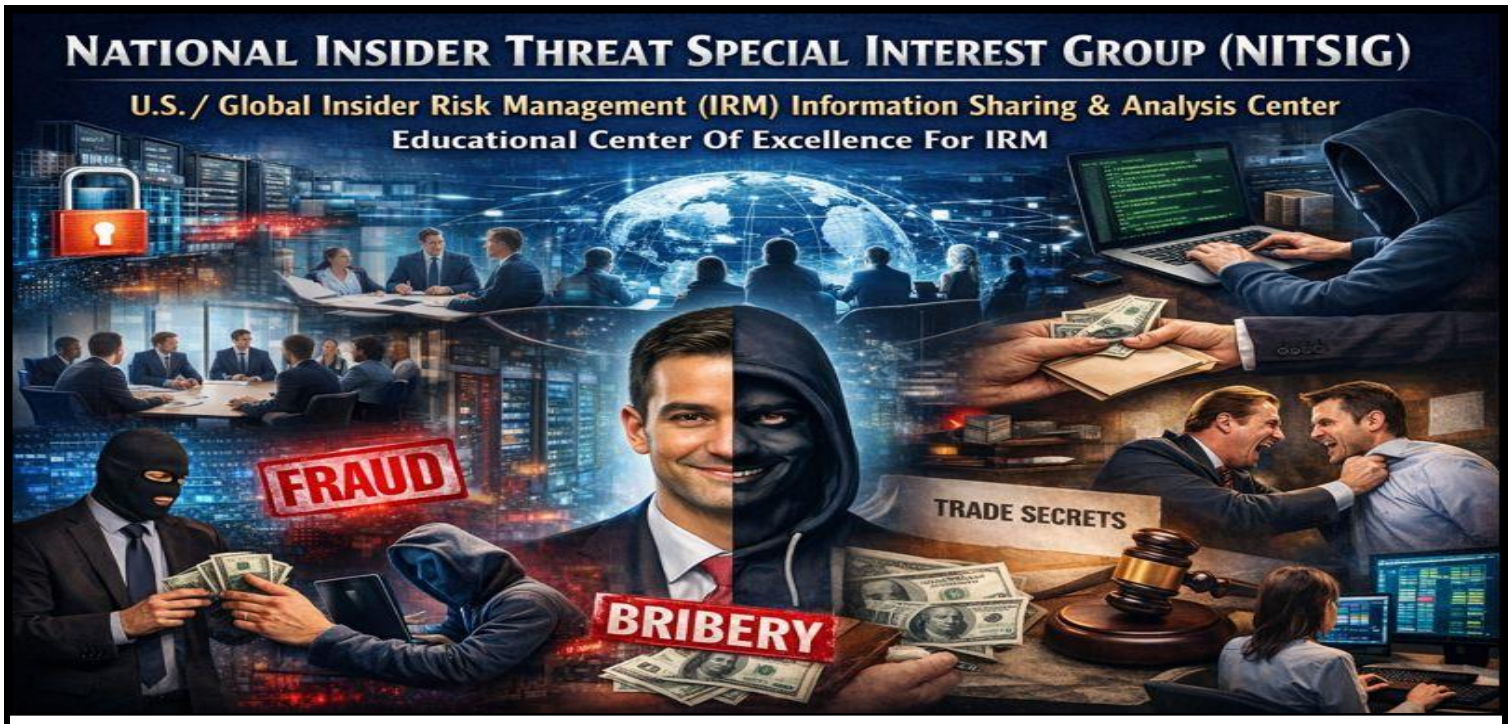
Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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, as no such ISAC existed. The NITSIG has been successful in bringing together Insider Risk Management (IRM) and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats. Many members have even stated the NITSIG is like having a team of IRM experts 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)
- ✓ Insider Threat Investigations & Analysis
- ✓ IRM Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Employee Continuous Monitoring & Reporting Programs (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 website are various documents, resources and training that will assist organizations with their IRM / IRM Program efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group with over 900 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: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

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

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

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

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 Insider Risk Management (IRM) Programs (IRMP's).

The ITDG exceeds IRM compliance regulations and help organizations create comprehensive, robust and 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 Training Course & Workshops For C-Suite, Board Of Directors, Insider Risk Program Manager / Working Group Members
- ✓ IRMP Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees

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 IRM Consulting Services For Our Clients

STUDENT / CLIENT SATISFACTION

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, due to the fact that the ITDG approaches IRM from a real world, practical, strategic, operational and tactical perspective. You are encouraged to read the feedback from our clients on this link.

The ITDG Has Provided IRMP Training & Consulting Services To An Impressive List Of 700+ Clients:

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

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 Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG