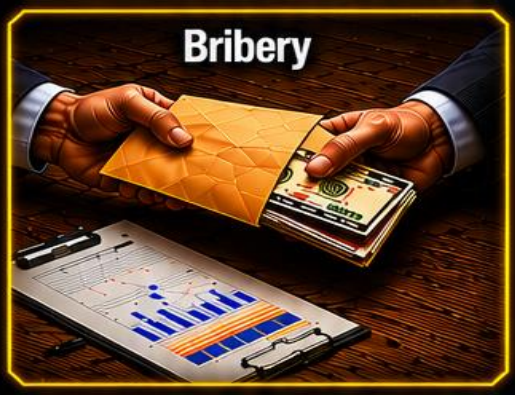
INSIDER THREAT INCIDENTS REPORT FOR

★ May 2026 ★



DON'T UNDERESTIMATE THE CAPABILITIES OF THE HUMAN OPERATING SYSTEM

Produced By

National Insider Threat
Special Interest Group

★

Insider Threat
Defense Group

TABLE OF CONTENTS

INSIDER THREAT INCIDENTS OVERVIEW

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **7,100+** 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 33** 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 MAY 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
ARE YOUR EMPLOYEES SELLING THEIR LOGIN CREDENTIALS / ACCESS TO THE NETWORK TO EXTERNAL HACKERS?

REPORT #1
A large share of UK employees have sold their corporate credentials over the past year, exposing their organization to cyber and financial crime, according to Cifas. The non-profit fraud prevention service revealed the findings in its latest Workplace Fraud Trends report, which is based on responses from 2000 UK employees working in companies with 1000+ staff.

13% of respondents admitted selling their logins over the past 12 months, or knew someone who had. The same share (13%) claimed they thought the act of selling credentials was "justifiable", rising even higher for senior managers (32%), directors (36%), C-suite executives (43%) and business owners (81%). (Source)

REPORT #2
The 2025 report from Check Point Software Research, showed 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.

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. (Source)

REPORT #3
The Flashpoint 2026 Global Threat Intelligence Report revealed hacking groups like Scattered Spider augment their efforts in recruiting malicious insiders. In 2025, Flashpoint observed 91,321 instances of insider recruiting, advertising, and threat actor discussions involving insider-related illicit activity. This change in tactics is far more efficient for attackers, as it is cheaper to recruit an insider to circumvent multi-million dollar security technology tools, than it is to develop a complex exploit from the outside. (Source)

REPORT #4
A 2026 report by Accenture's Cyber Intelligence Team also revealed that Dark Web recruitment of employees by hackers is increasing.

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)

EXAMPLES

- CrowdStrike Terminates Employee For Leaking Internal Data To Hackers For $25,000 Payment
- AT&T Employees Received $1 Million+ In Bribes To Install Malware / Key Logger On Company's Network - Costing AT&T $201 Million+
- IT Employee Sold Login Credentials To Hackers Who Stole $130 Million+ From PIX Brazil Banking Payment System
- Coinbase Damaging $400 Million Data Breach Involved Employees Paid By Cyber Criminals To Steal Data
- And More……

U.S. GOVERNMENT

Former CIA Officer Arrested For Stealing 300 Gold Bars Worth $40 Million+ From CIA - May 27, 2026

David Rush is a former CIA senior officer with top secret-level clearance.

Rush who held a management position, was charged with criminal theft of public money in a complaint filed in the Eastern District of Virginia. His lawyer didn't respond to a request for comment.

He was also accused of lying to his employers about his background for nearly two decades.

"After a CIA internal investigation identified potential violations of the law, CIA Director John Ratcliffe referred the information to the FBI for a law enforcement investigation," the written statement said. "The FBI is working closely with our partners at the CIA and the Department of Justice as we continue to investigate this matter fully. We are committed to following the facts, ensuring accountability, and pursuing justice in accordance with the law."

It wasn't clear how the investigation into Rush began, and it also wasn't clear when he left the CIA. His home was raided last week.

Rush applied to work with the government three times; in his first application, he said he graduated from Clemson University in 2000. In his second application, he added that he had a graduate degree from Rensselaer Polytechnic Institute. On his third try, in 2009, he succeeded, and he included those degrees and an aircraft test from the U.S. Naval Test Pilot School. In applications for promotions, he said he'd been a thesis adviser at the Air Force Institute of Technology. Rush also told employers he was a pilot for the Navy.

None of it was true, according to the charges; he didn't graduate from the schools, and investigators say the Federal Aviation Administration doesn't have a certificate or a pilot's license registered to Rush.

From November through March, Rush made several requests for funds, including for foreign currency and tens of millions of dollars in gold bars, according to an affidavit filed in federal court by an FBI agent investigating the case.

In a storage space near his office, investigators found only a portion of the funds. On May 18, federal agents searched Rush's home and seized roughly 300 gold bars worth more than $40 million, court documents said. Agents also seized about $2 million in U.S. currency and 35 luxury watches, mostly Rolexes, according to the affidavit.

The affidavit alleges Rush knowingly took part of the money he requested for work-related expenses to his home for personal gain. The court filing didn't specify which agency employed Rush, but the two people familiar with his employment history said he was with the CIA. (Source)

FAA Employee Arrested After Using Work Computer To Threaten To Kill President Trump - May 5, 2026

A Federal Aviation Administration employee (Dean DelleChiaie) was arrested after he allegedly threatened to harm the president and used a work computer to research his plans, prosecutors said.

Prosecutors allege DelleChiaie used his government computer to search the internet for how to get a gun into a federal facility. The suspect allegedly also made other incriminating searches on the device, including previous assassination attempts against Trump, the percentage of the population that wants the president dead and the phrase, "I am going to kill Donald John Trump," according to the criminal complaint.

The Secret Service met with DelleChiaie in February, and he allegedly admitted to conducting those searches on his work computer, according to the complaint. He also told the Secret Service he owned three firearms, including a handgun he kept inside a safe at home, prosecutors allege.

On April 21, DelleChiaie used his personal email to transmit a threat across state lines to the White House's email address, prosecutors said. The email had for a subject, "Contact the President," and said, "I, Dean DelleChiaie, am going neutralize/kill you -- Donald John Trump -- because you decided to kill kids -- and say that it was War -- when in reality -- it is terrorism. God knows your actions and where you belong," according to the complaint. (Source)

4 Individuals, Including 2 U.S. Postal Service Employees Pleads Guilty To Stealing $84 Million+ In U.S. Treasury Checks - May 5, 2026

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

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

Irby and Tucker removed the checks from the USPS facility and sold them to defendants Scott and Telewoda, who then advertised the stolen checks for resale on the cloud-based instant messaging application Telegram.

Upon receiving payment from interested buyers, Scott and Telewoda mailed the stolen Treasury checks to buyers around the country who attempted to cash the checks, without the knowledge or permission of the individuals to whom the checks had originally been issued.

Over the course of the scheme, Irby and Tucker sold Scott and Telewoda thousands of stolen Treasury checks whose face value exceeded $84 million.

Scott’s and Telewoda’s customers successfully negotiated approximately $11 million worth of these stolen Treasury checks at financial institutions. A grand jury returned a superseding indictment against the four defendants in May 2025; Irby was previously charged with — and has pleaded guilty to — a separate instance of mail theft involving another batch of Treasury checks that he stole and sold to an unnamed individual in August 2024. (Source)

2 U.S. Postal Carriers, Bank Manager & Convicted Felon Charged In $4.9 Million Bank Fraud And Mail Theft Scheme - April 30, 2026

2 former U.S. Postal Service mail carriers, a assistant bank manager, and a convicted felon face federal charges after participating in a scheme to steal valuable items from the mail, including a $4.9 million U.S. Treasury check.

Beginning in or about March 2020 and continuing through September 2025, Shanda Goode and Carnisha Hamilton, who were then employed as U.S. Postal Service City Carriers assigned to the Ralph McGill Post Office in Atlanta, Georgia, and the Marietta Main Post Office in Marietta, Georgia, allegedly stole mail containing checks, credit cards, gift cards, and other items of value in order to sell them to Francina z Sutton and other individuals.

On at least one occasion in December 2023, Hamilton stole three dozen pieces of mail containing checks and credit cards on a single delivery run. After obtaining the stolen mail, Sutton used the credit cards and cashed the checks for her own personal use.

Sutton also allegedly conspired with Tonya Bailey, who was an Assistant Financial Center Manager at a bank in Alpharetta, Georgia, to open bank accounts in the names of unsuspecting persons in order to deposit a $4.9 million U.S. Treasury check that had been stolen from the mail. In February 2023, Sutton entered Bailey's bank branch wearing a dark-colored mask and opened a bank account, with Bailey's assistance, in the name of an entity that resembled the name of the payee listed on the stolen check. Sutton and Bailey then deposited the stolen check into the new bank account. Two weeks later, Sutton returned to Bailey's bank branch wearing a surgical mask; drew two cashier's checks for $150,000 each from the account; and opened two new bank accounts, with Bailey's assistance, using stolen personally identifiable information. Sutton and Bailey then deposited $300,000 into the new accounts. (Source)

United States Postal Employee Pleads Guilty To Stealing 200 Pieces Of Mail Containing $700,000+ - May 20, 2026

Derrick Stewart, 34, of Baltimore, Maryland, pled guilty to federal mail theft by a postal employee, wire fraud, and aggravated identity theft stemming from conduct while he worked as a clerk at a mail processing and distribution center in Baltimore.

Beginning in September 2022, and continuing until December 2023, Stewart used his postal service position to embezzle mail, including checks. Stewart then falsely and fraudulently endorsed stolen checks with the identity theft victims' names and signatures.

Surveillance video captured Stewart depositing stolen and fraudulently endorsed checks into his personal bank accounts. Then on December 2, 2023, law enforcement executed a search warrant on Stewart after he exited a postal facility. During the search, law enforcement recovered almost 200 pieces of mail containing more than $700,000. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing $369,000+ Checks From Mail - May 5, 2026

Benita Randle was a supervisor at the St. Louis Processing and Distribution Center, which processes, sorts and distributes all non-parcel mail for the St. Louis metropolitan areas. She had access to all the mail at the center. Between September and October of 2023, Randle stole mail containing checks and gave that mail to Harrison, who opened the mail and removed the checks.

Randle's crime was uncovered when her leased Nissan Juke was repossessed for her failure to maintain insurance.

The car dealership found Harrison's backpack, which contained an AR-style handgun, cocaine, fentanyl and loose checks, and called the St. Charles Police Department. After officers arrived at the dealership, so did Randle, who falsely claimed that she did not handle mail in her job.

She later lied to investigators with the U.S. Postal Inspection Service and the U.S. Postal Service Office of Inspector General that she never drove the Juke and did not have access to mail.

Investigators determined that Randle had stolen 89 checks from mail that belonged to dozens of victims. They also found one counterfeit check that bore the same bank account and payor information as one of the stolen checks. The total face value of the 90 checks was $369,248. (Source)

U.S. Postal Service Employee Pleads Guilty To Embezzling $57,000 - May 26, 2026

Joyce Smith, 51 previously worked as the postmaster for a post office in Scott City, Kansas. Between January 2023 and February 2025, Smith embezzled approximately $57,400 from the USPS.

An audit revealed Smith stole approximately $10,600 in cash payments from customers and issued herself approximately $3,700 in money orders. Smith also embezzled approximately $3,400 that customers paid for their post office boxes.

Some customers made regular check payments for permits or mass mailings. Smith accepted the checks and provided the services to customers, but she did not log the receipts into USPS records. The USPS cannot account for checks for a total of $16,788 issued by the City of Scott City, $5,850 in checks issued by Scott County Landfill, and $17,108 in checks issued by a local newspaper. (Source)

Department Of Justice Contractor Employee Sentenced To Prison For Stealing Cell Phones Worth $1.3 Million & Selling Them/ Used Funds For Gambling, Vacations, SUV, Etc. - May 26, 2026

Between 2021 and 2025 Javan King worked as an information technology contractor for the Civil Rights Division at the Department of Justice (DOJ). During that period, he 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 the phones were shipped to King at DOJ, he sent them to phone reselling businesses. In total, the businesses paid him more than $1.3 million for the phones. He spent the proceeds on a variety of things, including gambling at MGM casinos and on FanDuel, vacations, private school tuition, and a down payment on a $92,000 Range Rover SUV.

The scheme came to light when a private citizen in Kentucky contacted the DOJ in late August 2025 noting that she had learned that an iPhone that she had purchased online belonged to the Department. (Source)

Former Centers for Disease Control & Prevention Supervisor Pleads Guilty To Stealing $190,000+ Of Agency Funds Using Fraudulent Invoices - May 22, 2026

From approximately August 2023 to February 2025, while employed as a Centers for Disease Control and Prevention (CDC) administrative professional, Gwendolyn Brandon created fraudulent invoices that appeared to be from vendors requesting payment for goods or services provided to the CDC.

The invoices triggered payments to an account she controlled. She used her role as a supervisor and her knowledge of CDC's invoice and credit card processing system to perpetuate the fraud by causing employees under her supervision, who were unaware of the fraud, to make the payments.

Through her scheme, she caused the CDC to pay at least 46 fraudulent invoices in amounts ranging from $2,230 to $9,970, resulting in the theft of $190,461.50 in government funds. (Source)

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

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

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

Deputy District Director To United States Congressman Charged For Fraudulently Obtaining $31,000+ Of Covid-Relief Benefits - May 6, 2026

The Deputy District Director to an Illinois United States congressman has been indicted on federal fraud charges for allegedly fraudulently obtaining more than $31,000 in unemployment insurance benefits during the Covid pandemic.

In May 2020, Moorer filed a fraudulent application for Pandemic Unemployment Assistance (PUA) benefits in which he claimed to have met Covid-related reasons for being unemployed, partially unemployed, unable to work, or unavailable to work. Moore's application was approved, and over approximately the next 16 months, he continued to submit fraudulent certifications of his purported unemployment to continue receiving the benefits, the indictment states. In reality, Moorer knew that he was in fact employed by the federal government as an aide to the Illinois Congressman at the time of his application and certifications. As a result of the fraud, Moorer obtained $31,887 in PUA benefits to which he was not entitled, the indictment states. (Source)

Finance Director For U.S. Government Agency Sentenced To Prison For Accepting $12,000 In Kickbacks To Steer $600,000 In Contracts To A Friend - May 27, 2026

Mathieu Zahui, 59, is the former Director of Financial Management at the U.S. African Development Foundation.

The U.S. African Development Foundation (ADF) is an independent federal agency established to support African-owned and African-led business enterprises.

Zahui joined ADF as a budget analyst in 2010 and rose over fifteen years to become its Finance Director, serving in effect as the agency's chief financial officer with authority to review and approve invoices paid with taxpayer funds. Beginning in December 2020, he also served as ADF's Contracting Officer Representative, responsible for monitoring contractors' performance and processing invoices, and received specific training on his obligation to avoid conflicts of interest.

Zahui used his position to benefit a friend and the friend's company.

In March 2020, Zahui directed ADF to award his friend's company a series of sole-source contracts, exempting it from competitive bidding, for purported logistical support services that the company never actually performed. The contracts, valued at about $173,640, $350,544, and $93,200, far exceeded the $100,000 cap on sole-source awards. Zahui approved invoices submitted by the company knowing they were illegitimate and unsupported by any actual work.

Zahui also arranged for other ADF contractors doing legitimate work to route their payments through his friend's company, allowing the friend to collect markups ranging from 17% to 66% for doing nothing. In one instance, Zahui directed a staffing company to issue a $120,000 invoice to his friend's company, which had no involvement in the underlying work. The friend's company then submitted a $140,653 invoice to ADF, and Zahui approved it, generating more than a $20,000 markup.

Over about three years, the friend's company submitted more than 20 such pass-through invoices and collected about $134,886 in markups for performing no legitimate work.

To avoid scrutiny from the Bureau of Fiscal Service, which was responsible for authorizing ADF payments, Zahui ensured that invoices consistently described the services as logistical support, even when they had nothing to do with logistics. In one instance, he directed another contractor to revise an invoice description to falsely reflect logistical services.

In return for steering the contracts and approving the fraudulent invoices, Zahui received $12,000 in eight separate cash payments from his friend.

When federal agents interviewed Zahui in January 2024, he denied receiving any benefits from his friend and downplayed the extent of their relationship, claiming they communicated only a few times a year. Phone records and emails later revealed they had in fact communicated nearly every day during some periods. In a second interview in February 2024, Zahui again lied to federal agents. The full extent of his conduct came to light only after investigators conducted an extensive review of his phone, emails, and ADF records. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

2 Defense Contractor Employees Arrested For Conspiring To Bribe A U.S. Army Employee With $1.25 Million For Department Of War Technology Innovation Contracts - May 20, 2026

The indictment, filed in the District of Hawaii on May 14 and unsealed on May 20, alleges that, from January 2021 to October 2022, Leonard Pick and Brian Kent conspired to bribe a U.S. Army employee with approximately $1.25 million over five years and fraudulently inflated government contracting costs to include the U.S. Army employee's bribe payments.

Pick and Kent orchestrated a bribery and major fraud conspiracy that corrupted the competitive procurement process for a Department of War technology innovation lab in the Pacific. The criminal actions specifically affected the construction and operation of the U.S. Army Pacific Command's Hawaii-Pacific Innovation Campus, which was intended to be a hub for testing new technologies for the Department of War.

The indictment further alleges that, from approximately September 2020, up to and including October 2022, defendant Kent further defrauded the government by inflating government contract costs to include approximately $680,000 in payments intended for and sent to Kent's personal consulting business. (Source)

U.S. Army Soldier Charged For Threatening To Walk Into Synagogue With AK Rifle & Kill Everyone - April 27, 2026

Jakob Marcoulier, was a 22-year-old soldier stationed at Fort Polk in Louisiana,

The FBI's National Threat Operations Center received an online tip in February 2026 about a Discord user named "el.bostino" who had made threats toward synagogues. FBI secured recorded audio from Discord in which the individual, later determined to be Marcoulier, made these threats, stating among other things that "after this deployment if the Jews still have reign over our government, I am going to walk into a synagogue with my AK, with a 75-round drum mag, and all of my extra mags, with my level four plates, and my haka helmet that's three plus, and I am going to kill every single Jew I know inside of that synagogue.

And that's my goal in life." Marcoulier went on to emphasize the seriousness of his threats, saying among other things that "you guys will never do anything about but I will. I just have to finish this, I have to go back overseas and do what I have to do. And then you'll see me in the news.

I promise you," and that "you guys don't want to do anything for the f[***]ing cause when it actually needs to happen … I'll still kill these mother[***]ers in order to make sure the white youth is f[***]ing secured." Marcoulier was arrested on April 23. (Source)

U.S. Department Of Veterans Affairs Employee Charged With Fraudulently Obtaining $41,000+ Of Covid-19 Benefits / Used Funds For Personal Expenses - May 5, 2026

Denise Baez, 51, had been employed full-time as a Medical Technician with the U.S. Department of Veterans Affairs since August 2021.

Baez submitted two applications seeking Paycheck Protection Program (PPP) loans. In those applications, Baez made false claims regarding gross income purportedly earned from a sole proprietorship. To support these false claims, Baez allegedly attached fraudulent tax documents as part of the applications. The PPP loan applications were approved and Baez received $41,666. Baez allegedly used that money on personal expenses.

However, in September 2021, Baez allegedly submitted loan forgiveness applications that falsely claimed the entire $41,666 was spent on payroll. Based on the misrepresentation the loans were forgiven. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former DOJ Prosecutor Charged With Stealing Confidential Investigation Documents About President Trump By Renaming Files To Avoid Detection & Sending To Personal Email - May 20, 2026

A former Justice Department prosecutor was charged with allegedly emailing confidential records tied to former special counsel Jack Smith's investigation into President Donald Trump.

Carmen Lineberger, 62, faces four criminal charges stemming from her handling of Smith's final report: one felony count of obstruction of justice, one felony count of concealing government records and two misdemeanor counts of theft of government property valued at less than $1,000.

Lineberger allegedly altered electronic file names of government records to conceal unauthorized transmissions of the documents to her personal email accounts. At the time, she was serving as the Managing Assistant U.S. Attorney for the Fort Pierce branch of the U.S. Attorney's Office for the Southern District of Florida.

Prosecutors alleged Lineberger concealed her actions by saving electronic copies of government records under misleading file names, including "chocolate cake recipe" and "bundt cake recipe," before sending them to personal Hotmail accounts.

U.S. District Judge Aileen Cannon previously blocked the public release of the volume of Smith's report related to the classified documents investigation involving Trump's Mar-a-Lago estate in January 2025.

Lineberger received a copy of Smith's report before Cannon ordered it sealed. Months later, she allegedly forwarded the report to her personal email account. (Source)

11 County Sheriff Employees Charged For Misusing $310,000+ Of Funds To Make Unauthorized Purchases For Personal Benefit - May 19, 2026

The indictment alleges that the defendants used the Kershaw County Sheriff's Office (South Carolina) narcotics credit card and seized cash fund to make unauthorized purchases for personal benefit. Purchases included construction materials, tools and equipment, security cameras, coolers, Apple products, automotive supplies and parts, hunting equipment, welding materials, and mechanic equipment. (Source)

Department Of Corrections Employee Pleads Guilty To Accepting $100,000 In Bribes To Distribute Contraband & Methamphetamine To Inmates / Used Funds To Buying Cars, Motorcycles, Etc. - May 15, 2026

Former California Department of Corrections and Rehabilitation employee, Keith Randle, pleaded guilty to possession with intent to distribute over 300 grams of methamphetamine to inmates at San Quentin Rehabilitation Center, formerly known as San Quentin State Prison.

Randle admitted to soliciting and accepting bribery payments in exchange for smuggling and distributing prison contraband, including methamphetamine, marijuana, and tobacco, to inmates at San Quentin. The scheme went on for years, dating back to at least January 2019 and continuing through August 15, 2024. Randle charged inmates and their associates approximately $1,000 per item he smuggled into the prison and initially received payments directly from inmates. However, fearing law enforcement might uncover his contraband and drug distribution scheme, Randle began to solicit and accept bribery payments from the associates of inmates rather than inmates themselves. On August 15, 2024, Randle was caught inside San Quentin with a hollowed out peanut butter jar containing 301 grams of methamphetamine, as well as marijuana. The peanut butter jar was painted brown and glued shut to appear full and unopened.

Randle profited significantly from his years-long bribery and drug distribution scheme. From January 2019 through April 2020, Randle was paid $31,000 from associates of inmates to his PayPal account in exchange for smuggling contraband into the prison. As another example, from July 2021 through August 2022, Randle received approximately $40,926 via Cash App from an inmate's wife in exchange for smuggling contraband to her husband at San Quentin. In 2023 and 2024, Randle primarily only accepted bribery payments in cash.

On October 1, 2024, federal law enforcement seized $55,210 in cash from Randle's two residences, all of which Randle admitted were proceeds from his bribery and drug distribution scheme. In total, Randle admitted to soliciting and accepting over $100,000 in bribery payments from inmates and their associates. With the illicit proceeds, Randle admitted to making numerous purchases, such as buying cars, motorcycles, and other assets. (Source)

Federal Prison Internal Affairs Investigator Sentenced To Prison For Accepting $3,200 In Bribes To Smuggle Narcotics Into Prison - May 12, 2026

Deon Scott, 41, is a former Internal Affairs Investigator for the Office of Professional Standards for the Shelby County Divisions of Corrections to federal prison in Tennessee.

Scott smuggled contraband into the Shelby County Divisions of Corrections, a facility which houses federal inmates, while employed as an Internal Affairs Investigator at the facility. Scott received at least $3,200 as payment for his unlawful conduct. Scott was immediately terminated from his position.

On November 17, 2025, Scott pled guilty to a one count information alleging that as a public official, he accepted money in exchange for smuggling contraband items, including narcotics, into the Shelby County Division of Corrections. (Source)

Chicago Police Sergeant Charged With Fraudulently Obtaining $41,000+ Of Covid-Relief Loans - May 5, 2026

A Chicago Police Sergeant (Brandi Wright) has been charged in federal court with fraudulently obtaining more than $41,000 in small business loans under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Wright engaged in fraud related to the Paycheck Protection Program (PPP), one of the sources of relief under the CARES Act.

Wright submitted two applications for PPP loans in 2021 on behalf of a bakery business she claimed to own but that did not actually exist. The applications contained materially false statements and misrepresentations about Wright's purported business, including gross revenue, payroll needs, and operational expenses, the information states.

Wright fraudulently obtained two loans totaling $41,662, which she intended to use for her personal benefit. (Source)

Former U.S. Border Patrol Agent Pleads Guilty To Spending His Official Duty Hours Running His Personal Business & Receiving $17,000+ Of Government Pay - May 18, 2026

Ramon Heriberto Cerda Jr., 41, a former U.S. Border Patrol Agent pleaded guilty in federal court to defrauding the U.S. government by spending his official duty hours running a personal business while submitting time cards and collecting bi-weekly government paychecks.

Cerda also owned and operated a business known as El Eagle Mail. On multiple dates in February and March 2025, Cerda was observed at his residence during scheduled work hours despite his duties requiring him to be in the field.

To further observe Cerda's activities, the FBI installed two surveillance cameras beginning on April 22, 2025, one providing a view of his home and the other providing a view of the El Eagle Mail business, located approximately 15 to 20 minutes away. Between April 22 and June 28, 2025, surveillance showed Cerda remained at his residence until approximately 2pm on weekdays, before traveling to the El Eagle Mail business where he remained until after 4pm. During the same time period, he submitted bi-weekly timecards reflecting that he worked for the USBP from 6am to 4pm, claiming a total of 399.58 hours of pay between April 22 and June 28, 2025. He received approximately $17,724.74 in pay for those reported hours.

In addition to the surveillance video, the FBI obtained cell site location data for both Cerda's government issued phone and his personal phone.

Analysis of the data also indicated Cerda was located at or near his residence during work hours and showed a lack of activity consistent with traveling to the Eagle Pass USBP station to pick up a government vehicle for his assigned transportation duties. Additional investigative methods also corroborated the surveillance video. (Source)

TSA Security Officer Sentenced To Prison For Fraudulently Obtaining $47,000+ Of Covid Pandemic Unemployment Assistance - May 21, 2026

Ismael Rosado, 40, 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 and weekly certifications claiming 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)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Oklahoma Department Of Human Services Employee Arrested For Stealing $2 Million From Energy Assistance Program Over 7 Years / Money Transferred Into Personal Bank Account - May 7, 2026

A now fired employee (Casey Letra) with the Oklahoma Department of Human Services (OKDHS) has been arrested and accused of stealing $2 million from the state's most vulnerable.

Letran worked for the Low Income Home Energy Assistance Program (LIHEAP). In Oklahoma, over 180,000 households use it to keep their utilities from getting shut off, especially during hot summers or cold snaps.

This investigation started after the State Auditor's Office reported oversight deficiencies within LIHEAP. During their fieldwork, state investigators found suspicious payments and notified the management at OKDHS, who then turned the case over to the DHS-Office of Inspector General (OIG). According to court documents, Letran was creating fake businesses within the DHS computer system and diverting LIHEAP funds to accounts connected to those entities.

The money was then transferred into his own personal bank accounts. Investigators say the alleged theft occurred between Sept. 1, 2017, and Aug. 1, 2024, while Letran was entrusted with managing those funds on behalf of the state, and that he stole over $2 million. (Source)

Dallas Housing Authority Employee Sentenced To Prison For Stealing $473,000+ of U.S. Government Funds - May 27, 2026

A former Dallas Housing Authority (DHA) maintenance supervisor, Joel Ipina, 50, who stole $473,641 from DHA was sentenced to 2 years in federal prison.

Ipina was employed by DHA from 1995 to 2024. DHA receives federal funding through the U.S. Department of Housing and Urban Development (HUD). As a maintenance supervisor, Ipina was responsible for approving maintenance work orders and selecting contractors to perform work on properties under his supervision.

From approximately August 2019 through February 2024, Ipina carried out a scheme to enrich himself by steering maintenance contracts to a company he owned and controlled without DHA's knowledge. As part of the scheme, he submitted fabricated competing bids to ensure contracts were awarded to his company and caused DHA to pay for work that was never performed. (Source)

Senior Vice President For Atlanta Housing Authority Sentenced To Prison For $83,000 Of Fraud With Help Of Family Members - May 22, 2026

Tracy Jones, a former Senior Vice President at the Atlanta Housing Authority, has been sentenced to prison and ordered to pay restitution for a scheme to fraudulently collect Section 8 housing assistance payments for her own rental property and family members, making fraudulent applications to collect pandemic relief funds, and committing mortgage fraud when refinancing her rental property.

Jones defrauded the program by using a series of falsified forms to have her family members admitted to the Section 8 program and then to receive Section 8 payments for them to live in her own rental house. To conceal her identity, Jones used a fake name and a shell business entity to execute housing authority documents. As a result, she improperly obtained more than $36,000 of Section 8 funds. Jones then obstructed subsequent investigations by submitting a false affidavit and convincing friends to lie and present false documents on her behalf.

At the same time, Jones used her shell business and another business to collect more than $27,000 from the U.S. Small Business Administration's COVID-19 pandemic relief programs, falsely claiming that the businesses were functioning, had multiple employees, and received over $56,000 of gross revenues in 2019. (Source)

Employee Who Worked For State Low-Income Home Energy Assistance Program Using Federal Funds Sentenced To Prison For Accepting $15,000+ In Bribes - April 30, 2026

Megan Tillery was employed with the Community Action Partnership in the second quarter of 2022 as the Community Intake Specialist. Tillery used her position to solicit bribes from individuals in exchange for applying Low-Income Home Energy Assistance Program (LIHEAP) funds to their accounts when they did not qualify for funding under the program. Tillery also solicited money from an individual who was qualified for LIHEAP funds. Tillery told the individual that he needed to pay her to reduce the utility bill.

The individual was not required to pay a fee to Tillery or Community Action Partnership to receive funds because he qualified for LIHEAP benefits. Between July 2022 and December 2023, Tillery received more than $15,000 in bribes.

LIHEAP provides federally funded assistance in the form of a grant to eligible households to reduce their energy costs. Alabama has designated the Alabama Department of Economic and Community Affairs (ADECA) as the entity responsible for receiving these federal funds and administering the LIHEAP program to the state. In Madison and Limestone Counties, ADECA has partnered with Community Action Partnership for that purpose. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Board Treasurer Pleads Guilty To $385,000 Of Wire Fraud Scheme - May 21, 2026

While serving as the school board treasurer in 2019, Ashley Benny, 41, was asked to research alternative investment options for the school district's unallocated savings.

Benny learned through a friend of a supposedly lucrative overseas "standby letter of credit" investment that carried no risk of loss. The school district agreed to Benny's suggestion and voted to transfer $385,000 to a company called "AgFluent." Prior to the board vote, Benny failed to disclose that she opened and controlled the AgFluent bank account and hoped to personally profit from the investment.

The investment was a scam, and the school district was defrauded out of $233,000 wired overseas by AgFluent.

Contrary to AgFluent's agreement with the school board, Benny then helped transfer the remaining school district investment funds to pay various other entities and expenses owed by a co-conspirator, including nearly $60,000 for the purchase of two semi-trucks and a $10,000 escrow payment on a failed land purchase deal. The school district never received any return on its $385,000 investment. (Source)

Executive Director At Virginia University Sentenced To Prison For Stealing $145,000+ Using False Invoices Scheme - May 1, 2026

Beginning in 2018, Billy Wooten served as an executive director for a private university based in Virginia. In his role, Wooten was responsible for purchasing food and other charitable items for university students. To fulfill his role, Wooten was entrusted by the university to bill invoices directly to the university and use a credit card that was paid for by the university.

Wooten tole more than $145,000 through a variety of schemes involving the doctoring false invoices and charging expenses to subordinates' credit accounts.

Beginning in or around 2023, Wooten began taking advantage of the university by purchasing large quantities of personal items and billing the invoices to the university. These items included sports memorabilia, groceries, and home improvements.

In one instance, Wooten acquired professional basketball trading cards for more than $17,000. He actively attempted to conceal his scheme by manipulating the invoice to make it appear as though it was for a local charitable cause and removed the contact information for the vendor before submitting it to the university for reimbursement.

In addition, Wooten also used another university credit card to perpetuate his fraud. Once Wooten's credit card had reached its maximum spending limit, he directed his subordinates to make purchases for him that were purportedly on behalf of the university. (Source)

Former Elementary School PTA Treasurer Pleads Guilty To Embezzling $100,000+ For Personal Financial Benefit - May 21, 2026

From August 2020, through July 2025, Holly Mikkelsen, was serving as the treasurer of the Summit Pointe Elementary School Parent Teacher Association (SPE PTA) in Kansas City, Missouri.

While serving as treasurer, Mikkelsen made unauthorized withdrawals from the SPE PTA's checking accounts at for her personal financial benefit. This included writing and signing SPE PTA checks fraudulently made out to herself and then presenting the checks for payment, withdrawing cash from automated teller machines, and transferring SPE PTA funds to other accounts controlled by Mikkelsen. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Treasurer Of Labor Union Sentenced To Prison For Embezzling $49,000+ / Used Funds For Personal Expenses - May 5, 2026

Joe Scott, 55, was the Treasurer of the International Union of Electrical Workers, Communication Workers of America, Local 81154, a labor union chapter based in Gardner, Mass., that represents union members from various employers in Massachusetts.

Scott used his position as Treasurer to embezzle approximately $49,559 from Local 81154, by making debit card expenditures, withdrawing funds and issuing checks, from union bank accounts, all for Scott's personal benefit. Scott used the money to pay for, among other things, storage costs, home internet and cell phone services, electrical and gas services, home improvement tools, dumpster rental and personal expense while on vacation. (Source)

BANKING / FINANCIAL INSTITUTIONS

Global Financial Services Company Employee Charged For $6.6 Million Wire Fraud Scheme Over 9 Years / Used Funds To Make $3.2 Million Of Credit Cards Payments, Etc. - May6, 2026

Between 2013 and December 2025, Ricardo Fontanilla worked at his company, a global financial services company which had its U.S. headquarters in Massachusetts, as a Security Administration Services employee. Fontanilla's role allegedly gave him access to the company's financial systems, which tracked borrowers' mortgage payments in connection with residential mortgage-backed securities—a kind of financial instrument that allows investors to purchase ownership in a pool of residential mortgage loans.

Beginning at least as early as 2016, Fontanilla allegedly altered the company's records to make it appear that the company was receiving excess payments from mortgage servicing companies that were collecting borrower payments. Fontanilla fraudulently transferred these supposedly "excess" payments back to one mortgage servicer company, and then falsely informed company representatives that the company had mistakenly refunded these amounts. In directing the mortgage service company to return the mistaken refunds to the company, Fontanilla allegedly directed the company to wire the funds to a personal bank account he controlled at Wells Fargo.

Records for the Wells Fargo account show Fontanilla received more than $6.6 million in wires from his company between 2016 and 2025 and that Fontanilla allegedly made payments from the account for more than $3.2 million in personal credit card payments to Capital One, JPMorgan Chase and American Express; $778,000 in mortgage and loan payments; more than $200,000 in cash and cash-equivalent withdrawals; spent more than $70,000 at Cartier locations in Italy, Spain, the Philippines and the United States; and purchased a vehicle for approximately $77,000 —amounts far exceeding the approximately $83,000 annual salary Fontanilla received from the his company. (Source)

Bank Employee Sentenced To Prison For Embezzling $413,000+ From Bank's Customers For 8 Years / Used Funds To Pay Her Credit Cards, Her Business, Etc. - May 6, 2026

Laura Parrish, was employed by the bank for more than seven years before her termination.

An investigation revealed that between November 2016 and January 2024, Parrish used customer funds to make payments on her personal credit cards and transfer funds to her external online financial account.

Parrish also opened personal credits cards in the names of other people and used the accounts of the bank's customers to make payments on those credit cards.

An investigation further revealed that between August 31, 2021, through April 18, 2023, Parrish embezzled funds from one family, including one family member who was deceased, in the approximate amount of $364,000. Parrish used these funds to make payments on her personal credit cards and loans to benefit herself, her business, Southern Roots and Blooms, or accounts held in the names of her husband, daughter, and other family members. On January 24, 2023, Parrish submitted a credit card application for a retail credit card using the name, date of birth, and social security number of one of the bank's customers. Parrish placed her address and phone number on the application and between February 2023 and January 2024, made payments totaling $15,000 on the credit card. This bank customer passed away in March 2023, and Parrish continued to embezzle funds from this account. Between July 2021 and January 2024, Parrish embezzled approximately $413,871.40 from eight bank customers. (Source)

Bank Manager Sentenced To Prison For Stealing $214,000+ From Bank / Used Funds For Gambling - May 6, 2026

Jonathan Lim was a manager of a bank branch in Downingtown, Pa., he took over responsibility for the regular administration of the branch's automated teller machine (ATM), which required accessing the ATM's interior. From about August 2019 through November 2019, on multiple occasions, Lim stole cash from the ATM and repeatedly falsified records to hide his crimes.

Lim resigned from the bank on November 24, 2019, and the ATM and branch were audited two days later. Auditors discovered that the ATM had a shortfall of more than $178,000 and the defendant's cash box was short by $36,000. In all, Lim embezzled approximately $214,000 from the bank branch and spent the majority of the money gambling. (Source)

Bank Employee Pleads Guilty To Stealing $125,000+ From Elderly Customer With Dementia - May 6, 2026

A former employee (Carlos Bras) of Santander Bank in Rhode Island has pleaded guilty in federal court to charges related to stealing more than $125,000 from the bank account of a 78-year-old customer with dementia.

Bras was employed by Santander Bank and had access to customer financial accounts. Beginning in or about May 2023, Bras accessed the account of the 78-year-old victim, who resided in an assisted living facility and had a court-appointed conservator in Massachusetts.

Bras admitted that he enabled online banking access to the victim's account, ordered checks sent to addresses he controlled, and obtained a debit card for personal use. He further admitted to conducting numerous unauthorized transactions, including transfers to his wife's account, and multiple wire transfers to a bank account in Portugal. (Source)

Jackson-Hewitt Tax Service Employee Sentenced To Prison For Embezzling $16,000+ - May 6, 2026

Tina Yager used her tax preparer position with a Jackson-Hewitt Tax Service in Republic, Missouri., to abuse the personal financial information of others to prepare and transmit fraudulent income tax returns.

Yager embezzled $16,850 collectives from the IRS and Missouri Department of Revenue collectively. Yager would file tax returns for customers of Jackson-Hewitt without their knowledge or approval. Yager would then have any refunds directed to her instead of the proper taxpayer. (Source)

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

University Of Maryland Medical Center Hospital Pharmacist Charged For Installing Spyware & Unauthorized Access To Computers For 8 Years - May 1, 2026

Matthew Bathula, 41, is charged with two counts of unauthorized access to a protected computer, and one count of aggravated identity theft while working as a Clinical Pharmacy Specialist at the Hospital,

Between July 2016 and September 2024, Bathula intentionally accessed the hospital computers without authorization and obtained information such as usernames, passwords, cookies, images, videos, and other data. Bathula also used various cyber intrusion techniques — such as keylogging, cookie managers, mailbox-rule creation, and file masquerading to obtain access to personal and professional accounts of people who were current or former employees, in a relationship with a current or former employee, and others affiliated with the hospital.

This enabled Bathula to access victims' online services such as Google Photos, iCloud Photos, Gmail, and Microsoft 365, and social media accounts. Additionally, the mailbox rule Bathula created automatically deleted incoming emails with the subject heading Critical Security Alert. This rule prevented the hospital cybersecurity personnel from knowing their accounts were compromised.

Bathula's repeated exportation of browser cookies allowed him to import cookies into an internet browser and access victims' accounts on other devices without their authorization. This enabled Bathula to maintain unauthorized access to victims' accounts on his personal electronic devices from locations outside of hospital network.

Between February 2023, and continuing through July 2024, Bathula installed a spyware software program on one or more the hospital computers. Through using the software, Bathula conducted video surveillance of people present at the hospital and recorded victims without their consent, including people engaged in breast pumping.

According to the security officials, the Hospital retained a cybersecurity firm, CrowdStrike, who identified files that were being saved to a USB drive in real time. Security officials connected online activity, system activity, security-badge activity, and physical location to identify a suspect. On or about September 28 or 29, 2024, the Hospital determined that Bathula was responsible for the security violations.

According to the class action civil complaint, the Bathula had access to hundreds of stationary computer stations within the Hospital, rooms where laptops were stored and computer stations equipped with webcams in private patient-exam rooms. The Respondent used his electronic access privileges to install keyloggers on hospital computers which captured the user names and passwords entered and sent them to the Bathula. The key logger also collected their personal usernames and passwords and sent them to the Bathula. Bathula maintained a list of user names and credentials which he used to access the plaintiffs' personal accounts where he downloaded and retained photographs, videos, and other personal information. (Source 1) (Source 2)

Pharmacy Technician Pleads Guilty To $5.6 Million Health Care Fraud Scheme & Illegal Distribution Of Oxycodone - April 30, 2026

Ali Naserdean, 32, of Dearborn Heights, Michigan, was a pharmacy technician at three metro-Detroit pharmacies.

From 2019 through 2022, Naserdean and his co-conspirator submitted false and fraudulent claims to health care benefit programs for prescription drugs that were not ordered by a doctor and never dispensed to the patient.

Naserdean and his co-conspirator used forged prescriptions from doctors to hide their scheme, when the patient had never seen the listed doctor and the medication had never actually been prescribed. Naserdean and his co-conspirator caused over $5.6 million of loss to Medicare, Medicaid, and Blue Cross Blue Shield of Michigan. Additionally, from 2019 through 2022, Naserdean provided unlawful prescriptions of oxycodone to drug traffickers in exchange for cash, without regard to whether the prescriptions were actually prescribed by physicians or dispensed in good faith. (Source)

New Jersey Hospital Employee Accused Of Stealing $2.5 Million Worth Of Medical Supplies & Reselling Them - April 7, 2026

Marci Staub, 44, is a former surgical technician at Cooper University Health Care in Camden, New Jersey.

Staub is charged with stealing $2.5 million worth of medical supplies and then reselling them in South Carolina. Staub is alleged to have impersonated a medical supply vendor as she sold the devices to the medical supply company. Prosecutors said detectives obtained financial records showing Staub received more than $427,000 in payments from reselling the items.

On Oct. 2, the hospital noticed that a large quantity of Medtronic Infuse bone graft devices and other supplies were missing and that its inventory did not match the documented number of products recorded as used. Hospital officials noticed they were refilling orders for the devices more frequently from December 2024 through July, despite not seeing an increase in patient care that would account for the additional usage.

During the investigation that followed, detectives from the Camden County Prosecutor's Office Major Crimes Unit reviewed surveillance footage from November to December 2025, showing Staub arriving at work with an

empty bag and then leaving with it filled. In December, the Camden County Sheriff's Office caught Staub leaving the hospital with medical supplies. Since then, she has been fired and was taken into custody. It is not clear whether she has legal representation. (Source)

Blue Cross Blue Shield Vendor Sentenced To Prison For $1.4 Million+ Behavioral Health Counseling Sessions Fraud Scheme - May 1, 2026

From January 2021 through December 2023, Natasha Allmon had an agreement with Blue Cross Blue Shield (BCBS) to provide behavioral health counseling services. During that time, Allmon submitted, and caused to be submitted, thousands of false and fraudulent claims to BCBS for behavioral health counseling sessions purportedly provided to family members.

Allmon routinely claimed to have provided 60-minute psychiatric treatment sessions to family members nearly every day of the year and, at times, claimed to have treated beneficiaries for more than 24 hours in a single day. In total, Allmon submitted approximately $1.4 million in claims for services, receiving close to $1.1 million in reimbursements from BCBS. Allmon was also ordered to pay nearly $1.1 million in restitution to BCBS. (Source)

Chief Financial Officer For Spinal Implant Company Pleads Guilty To Paying $540,000+ In Bribes To Doctors - May 12, 2026

Aditya Humad, 41, pleaded guilty to one count of conspiracy to violate the Anti-Kickback Statute. Humad was charged in September 2021 along with the company SpineFrontier, as well as Dr. Kingsley R. Chin, SpineFrontier's Founder, President and CEO.

Humad paid and conspired to pay over $540,000 in bribes to surgeons in the form of sham consulting fees for work they did not perform. Humad and Chin bribed surgeons to use SpineFrontier's products, and in turn, SpineFrontier received millions of dollars in revenue from surgeries the surgeons performed.

Humad entered into contracts with surgeons, agreeing to pay the surgeons between $250 and $1,000 per hour for purported consulting for SpineFrontier. In reality, however, Humad and Chin paid the surgeons for using SpineFrontier's products.

Although the surgeon-consulting program was purportedly directed at gathering technical feedback about SpineFrontier's products, Humad used the bribes they paid pursuant to that program, to induce surgeons to use SpineFrontier's products in surgeries that were paid for by federal health care programs such as Medicare, Medicaid and Veterans Health Administration. Additionally, the surgeons frequently spent only a small fraction of their reported time, if any, performing actual consulting. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

Employees Are Using Artificial Intelligence Software To Produce Pornographic Images Of Children & Employees

QUESTION

Is your organization monitoring the use of websites that use artificial intelligence to create pornographic pictures?

School District Employee Pleads Guilty To Using AI Technology To Produce 690 Sexual Abuse Images Of Children In His Care - May 7, 2026

William Haslach, 30, a former employee of a school district in Minnesota has pleaded guilty to production of child pornography and production of an obscene visual representation of child sexual abuse.

Haslach used his access to children to take non-explicit photos of children in his care. Haslach admitted to creating obscene visual representations of at least 91 minor victims in more than 690 morphed images through AI morphing. To date, there is no evidence that Mr. Haslach distributed or shared the images he created. (Source)

5 Women Are Accusing A Police Department Employee Of Taking Photos Of Them & Using AI To Make Pornographic Images - January 12, 2026

The complaint accuses the City of Chula Vista's Police Department and City of Chula Vista in California of negligence, claiming the city failed to implement proper safeguards to prevent this from happening.

Morgan Stewart is one of the attorneys representing the five women, ages 24 to 39. Stewart said prior to filing the complaint, his office gave the city of Chula Vista an opportunity to address the concern, but they refused.

According to Stewart, hard copies of the images were found on an employees desk, which led to an investigation. He said the investigation found that more photos had been made of his female colleagues.

Stewart said that although the investigation revealed the employee used the images for his own purposes, it remains unclear for how long the employee had been manipulating the images, raising concerns among the victims about the extent to which he may have shared them. "They have significant concern about the impact this could have on their lives, their careers, their other employment opportunities," Stewart said.
The accused employee is no longer employed by the police department. (Source)

Gartner Report States That AI Layoffs May Be Backfiring On Companies - May 22, 2026

A lot of workers have had the same uneasy thought lately: "Is AI coming for my job?" It is a fair question. Companies keep talking about automation, AI agents and lower costs. Some workers hear that and wonder whether their next performance review will come with a chatbot-shaped shadow in the room.

However, a new Gartner study suggests the story may be more complicated. Many companies are cutting jobs while adopting AI, but those cuts are not clearly producing better returns. Gartner says about 80% of organizations piloting or deploying autonomous business capabilities reported workforce reductions, yet those cuts did not appear to translate into a stronger return on investment.

The Gartner research looked at 350 global business executives at companies with at least $1 billion in annual revenue. The companies had already piloted or deployed AI agents, intelligent automation or autonomous technologies. The big takeaway is that companies that cut workers were not necessarily the ones getting the best results from AI. Gartner found that workforce reduction rates were nearly equal among companies reporting higher returns and those seeing only modest gains or worse outcomes.

Many executives have treated layoffs as the fastest way to show AI is "working." Cut headcount, reduce costs and point to the savings. On paper, that can look like progress. But Gartner's Helen Poitevin, a distinguished VP analyst, put it bluntly: "Workforce reductions may create budget room, but they do not create return." She said companies improving their return on investment are not eliminating the need for people. They are investing in skills, roles and operating models that let humans guide and expand autonomous systems. In other words, firing people may make a balance sheet look cleaner for a quarter. It does not automatically make AI useful. (Source 1) (Source 2)

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

Chinese Engineer Stole U.S. Military, NASA, FAA Source Code for Years Just by Asking for It

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

For 4 years, a Chinese aerospace engineer set up email accounts impersonating real U.S. researchers and engineers, then emailed researchers and employees at NASA, Air Force, Navy, Army, FAA, and faculty at major universities across the U.S. asking for source code and proprietary software. They handed him exactly what he asked for, and possibly violated US laws in the process. (Source)

What Is Elicitation?

Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, on the internet, in writing or at a conference an employee is attending.

Conducted by a skilled collector such as a hacker or other individuals, elicitation will appear to be normal social or professional conversation. A person may never realize that they were the target of elicitation or that they provided meaningful and very sensitive information.

Has your organization provided elicitation awareness training to your employees on the elicitation threat? A casual conversation by one of your employees with someone who is looking to gather non-public information about your organization (Data, Network, Trade Secrets, Business Development Plans, Etc.), could be the beginning of an intelligence gathering mission by external parties, that could result in very damaging actions being taken against your organization.

FBI Elicitation Brochure
DCSA Elicitation Brochure
DCSA Awareness Brochure On Targeting By Foreign Intelligence Elements At Conferences
DNI Elicitation Brochure

California Mayor Charged With Acting As Illegal Agent For The People's Republic Of China - May 11, 2026

Eileen Wang, 58, Mayor in Arcadia, California is charged with acting in the United States as an illegal agent for the People's Republic of China (PRC). Wang was elected in November 2022 to the Arcadia City Council, a five-person governing body from which the mayor is selected on a rotating basis.

From late 2020 through 2022, Wang and Mike Sun, 65, worked at the direction and control of PRC government officials and coordinated with U.S. based individuals to promote the PRC's interests by, among other things, promoting pro-PRC propaganda in the United States. Sun is serving a four-year federal prison sentence after he pleaded guilty in October 2025 to acting as an illegal agent of a foreign government.

Wang and Sun worked together to operate U.S. News Center, a website that purported to be a news source for the local Chinese American community. Wang and Sun received and executed directives from PRC government officials to post pro-PRC content on the website.

Wang admitted in her plea agreement that she did not notify the Attorney General that she was acting in the United States as an agent of the PRC, that she was located in the United States when she engaged in these acts. (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

30 Individuals To Include Corporate Attorneys & Other Financial Professionals Charged In Global Insider Trading Scheme Netting Tens Of Millions In Illicit Profits - May 6, 2026

Charges were unsealed against 30 defendants in connection with a large-scale, decade-long insider trading scheme that netted tens of millions of dollars in illicit profits. The defendants, who include corporate attorneys and other financial professionals, are alleged to have stolen and used confidential information on nearly 30 merger and acquisition deals from several of the nation's premier law firms.

19 defendants were arrested and will make appearances in federal court in Los Angeles, Calif., Fort Lauderdale, Fla. and New York, among other locations. Two defendants located in Russia and Israel are considered fugitives.

The defendants and other co-conspirators sought to keep law enforcement from learning about the scheme by, among other means, using burner phones, encrypted applications, coded language, ncluding about "flights," and in-person meetups where conspirators turned off their electronic devices or put them elsewhere before communicating with each other. (Source)

Company Accountant Sentenced To Prison For Embezzling $322,000+ - May 13, 2026
Juanita Holtschnieder, 58, while working as the accountant for G2 Material Handling, embezzled monies from the United States and G2 by redirecting automatic deposits set up within the business.

Holtschnieder used her trusted position to reroute deposits, intended for the bank accounts of the U.S. Treasury and G2's business account, to her personal account. Holtchneider then created false documents that she submitted to her employer that effectively hid her embezzlement. Holtschneider's scheme to defraud was only detected after the Internal Revenue Service detected failure by the business to submit regular payments for collected employment taxes. Holtschneider was ordered to pay $322,098.70 in restitution, with $289,607.70 paid to the U.S. Government, and an additional $32,491.00 paid to G2 Material Handling. (Source)

John Deere Dealership Employee Pleads Guilty To Embezzling $76,000+ - May 25,2026
Sarah Louis, 38, a former employee of an agricultural and turf utility vehicle company pleaded guilty to embezzling more than $76,000 from the company.

According to arrest documents, company officials reported to police in February 2024 that Louis had been stealing the funds since December 2021. The thefts came to light after company officials were contacted by a vendor who said he got a 1099 tax statement from the company for 2023. The vendor said he could not remember doing any work for the company that year.

An internal audit revealed a check for $3,284.16 dated Aug. 10, 2023, and made payable to Louis. A more thorough audit uncovered 29 checks that "were manipulated," totaling $71,308.04 that Louis stole from the business, an arrest affidavit alleges.

Waco police investigators obtained a grand jury subpoena for Louis' Wells Fargo bank account statements from December 2021 to March 2024, which revealed 11 of the checks that were stolen were deposited into her account along with "large cash deposits" on dates the other checks were cashed.

Under the terms of the plea agreement, Louis also pledged to make $76,308 in restitution to her former employer. A judge will review the plea agreement. A sentencing is set for July 29, 2026. Third-degree felonies are punishable by up to 10 years in prison. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY BECAUSE OF FINANCIAL PROBLEMS, FOR PERSONAL ENRICHMENT, TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING ADDICATIONS
Fuel Company Chief Financial Officer Charged With Embezzling $12 Million Over 8 Years / Used Funds For Gambling - May 1, 2026
Robert McCloughy previously served as a Revenue Agent for the Internal Revenue Service. He was arrested yesterday for embezzling over $12 million and money laundering as a Chief Financial Officer and Controller for a fuel company based in New Jersey.

In 2009, McCloughy was hired by a New Jersey-based fuel company where he served interchangeably as the CFO and Controller. From around March 2017 through March 2025, McCloughy misappropriated approximately $12 million from his company, separate and apart from what he was paid as a salary.

He did so through at least two methods: (1) causing the company's payroll company to pay him unauthorized expense" reimbursements and (2) causing unauthorized transfers to be made from the company's bank accounts to his personal bank accounts.

To hide the fraud, McCloughy made false entries in thec company's books and records. Then, once McCloughy received the misappropriated funds, he engaged in money laundering transactions, including gambling large sums at online sportsbooks and casinos. (Source)

Atlanta Hawks' Basketball Team Senior Vice President Of Finance Sentenced To Prison For Embezzling $3.7 Million / Used Funds For Travel, Diamond Ring, Etc. - April 29, 2026

Lester Jones joined the Accounting and Finance Department of ATL Hawks, LLC (The Hawks) in 2016. Following his promotion to Senior Vice President of Finance in August 2021, Jones became the most senior accounting executive for the Hawks after the Chief Financial Officer.

Beginning in early 2021, Jones became the sole administrator of the Hawks' corporate credit card account with American Express.

In this role, Jones supervised the Hawks' corporate American Express credit card program; served as American Express's sole contact with the Hawks in the event of payment issues, delays, and card suspensions; and determined when and to which employees corporate credit cards should be issued.

Jones was the only Hawks employee with full visibility into the number of corporate credit cards, the identities of the cardholders, account balances, and other program details. Jones also began serving as administrator of the Hawks' electronic reimbursement platform, supervising employees who handled expense reimbursements.

From a date unknown and continuing through in or about June 2025, Jones used his position to defraud the Hawks out of approximately $3.7 million dollars.

Jones accomplished his scheme in two ways: (1) by submitting or directing the submission of dozens of fraudulent expense reimbursement requests to cause the Hawks to reimburse him for fictitious business expenses; and (2) by charging personal expenses to corporate credit cards and covering it up through false representations to other Hawks employees, including to his subordinates in the Accounting and Finance Department. Those personal expenses included approximately $80,000 in overseas travel to the Bahamas and Thailand, $99,800 in apparel at Saks Fifth Avenue, a $115,795.01 diamond ring, $21,888.90 in Omega watches, and over $160,000 in tickets to concerts and other events. (Source)

Account Manager At Beverly Hills Business Management Firm Charged With Embezzling $2 Million+ From Celebrity Client / Used Funds For Personal Expenses - May 6, 2026

A former account manager at a high-end Beverly Hills business management and tax firm was charged with embezzling more than $2 million from one of the firm's celebrity clients. Musoke is believed to have fled to Uganda, where he has dual citizenship with the United States.

Musoke was employed as an account manager at a full-service business management and tax firm identified in court documents as company a. This Beverly Hills-based firm primarily served high-net-worth celebrities in the entertainment industry.

In this role, Musoke was entrusted with managing the complete financial and business affairs of company a's elite clientele. His job was to help clients with asset protection, investment strategies, and financial planning to help them preserve and grow their wealth.

The victim, identified in the indictment as Individual A, is a well-known television host and producer and had been a company a client for nearly 20 years. Musoke was Individual A's account manager and had full access to Individual A's financial accounts, including control of his debit cards.

From December 2019 to June 2023, Musoke gained unauthorized access to debit cards and the associated personal identification numbers (PINs) connected to Individual A's business bank account. Without Individual A's knowledge or consent, Musoke fraudulently used Individual A's debit cards to withdraw approximately $1,733,688 at a bank's ATMs, spend $165,270 on Amazon purchases, incur $191,543 in personal travel expenses, and spend more than $160,000 on other personal expenses. In total, Musoke embezzled more than $2 million from Individual A. Company a terminated Musoke in July 2023, after the fraud was discovered. (Source)

Virginia Department Of Human Resources Management Employee Sentenced To Prison For Stealing $1.5 Million+ Over 4 Years / Used Funds For Plastic Surgery, Luxury Lifestyle, Etc. - May 13, 2026

Linda Brown, 43, was sentenced four years in prison for stealing more than $1.5 million from the Commonwealth of Virginia Campaign (CVC), the officially sanctioned non-profit charity fundraising program for Virginia's more than 120,000 state government employees.

From 2017 through 2023, the Virginia Department of Human Resources Management employed Brown to administer the CVC. The CVC promised that Virginia state government employees could safely and easily

donate to their preferred causes throughout the year via credit card payments, mailed checks, and by payroll remittances deducted directly from employee paychecks. Brown was supposed to steward these funds and make corresponding payments to charities designated by donors.

Between January 2019 and August 2023, Brown embezzled more than $1.5 million of the over $5.3 million donated by state government employees. Instead of paying the charities designated by donors, Brown stole this money for personal spending.

For example, Brown paid $10,400 in fraud proceeds for a plastic surgery procedure. Brown also used stolen charity funds to pay for a pedicure at a spa in Las Vegas. She fraudulently used charity funds for multiple flight tickets to destinations around the country, stays at luxury hotels, a luxury apartment in Houston, designer clothing and shoes, beauty and cosmetic products, and food and alcohol.

Brown also concealed her embezzlement from the CVC by attempting to replenish the funds she had stolen with a $494,469 U.S. Small Business Administration-backed business loan, which Brown obtained by making false statements to the lender. (Source)

Company Account Charged With Embezzling $1.2 Million From Her Company For 8 Years / Used Funds For Herself & Relatives - May 11, 2026

Kari Bertels, 44, is charged with using her company credit card to make purchases for herself and relatives from 2018 to 2026, including $19,815 in beauty products from Red Aspen, $16,512 in fitness coaching, $42,407 in DoorDash deliveries, $59,994 in Amazon purchases, $15,000 in airfare for herself and relatives for domestic and international trips, $27,044 from Instacart, $14,331 in jewelry from Diamonds Direct, and $14,110 at a Sandals resort.

Bertels was an accountant and a senior financial analyst at the St. Louis County company. Her responsibilities included approving expenses reports and paying the company credit card bills and other business expenses with the company checking account, the indictment says.

She concealed her embezzlement by refusing to submit monthly expense reports for the unauthorized credit card purchases, re-directing the credit card statements from work to her home and dividing the payments for her unauthorized credit card purchases into smaller amounts in the accounting system. (Source)

Comptroller For 2 Companies Sentenced To Prison For Embezzling $759,000+ / Used For Luxury Goods, Vehicles, Concerts & Sporting Events - May 14, 2026

Daniella Vasquez, 48, worked as a comptroller for two separate companies between May 2021 and September 2022, where her responsibilities included issuing payments.

During her tenure with both employers, Vasquez embezzled $759,235.74, issuing unauthorized payments to herself and her husband, Thomas Vasquez, as well as to companies for personal expenses. She spent much of the embezzled funds on luxury goods, vehicles, concerts, and sporting events, which she flaunted on social media. (Source)

Company Bookkeeper Sentenced To Prison For Embezzling $166,000+ From Company / Used Funds For Personal Expenses - May 12, 2026

Fort Peck Manufacturing, Inc., (FPM), with assistance from its bank, discovered Parker Hawk was taking money from the company.

In late 2023, FPM learned their bank account had a negative balance based on some questionable transactions, including checks with wholly round numbers and no taxes withheld. All the questionable checks were signed by Hawk.

A review of the bank statements indicated a number of checks written and signed by Hawk to non-FPM employees. Hawk also used the company credit card to make online purchases, including from Amazon, and initiated other unauthorized electronic payments, including to Apple, CashApp, PayPal, and Western Union.

Law enforcement interviewed the non-FPM employees to whom Hawk wrote checks and they said she requested they cash the checks, and they would keep some of the money while Hawk kept the rest.
Hawk embezzled approximately $166,156.47 from FPM between 2021 and 2023 ($98,644.28 in fraudulent checks and $67,512.19 in fraudulent electronic transactions). Gray Hawk was ordered to pay $131,901.57 in restitution. (Source)

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

Financial Director For Media Brand Management & Consulting Company Convicted For Stealing $7.9 Million+ Over 10 Years To Finance His Business - May 13, 2026

Jordan Khammar pleaded guilty to wire fraud and money laundering for his role in a decade-long scheme to defraud a multinational media, brand management, and consulting company and steal over $7.9 million.

Khammar was hired as a financial consultant in 2006. He became the company Finance Director with certain access to and control over a wide range of its financial accounts and systems including those tied to banking, accounting, bookkeeping, and payroll functions. Between January 2015 and May 2025, Khammar abused that access and control to engage in a scheme to the company out of millions of dollars.

During a 10 years period, Khammar initiated over 300 wire transactions sending himself more than $7.9 million that he was not entitled to. Khammar took multiple steps to conceal his scheme from company by manipulating its books and records, circumventing internal controls, and limiting other employees' and consultants' access to the company financial systems and accounts.

Khammar created over 100 false entries in the company's general ledger to disguise his fraudulent wire transfers as purportedly legitimate payments for company expenses including corporate credit card bills, taxes, and costs associated with renovating its Brooklyn office.

Khammar wired most of the stolen money to an account held in the name of Olive Tree Ventures, Inc. (Olive Tree), a company that he founded, owned, and controlled. From the Olive Tree account, he dispersed a large portion of the funds to finance his independent business ventures including his media production company, Sideswipe Media, Inc., to purchase hundreds of thousands of dollars-worth of real estate in Florida and Ohio, and to further pay himself and a variety of personal expenses. (Source)

Former Director Food Services For Public Schools Pleads Guilty To Stealing $11,000 Of Food & Equipment For His Side Business - May 14, 2024

Patrick Van Cott, 64, was the former Director of Food Services for the Plymouth Public Schools in Massachusetts, from 2003 until June 2025. Starting in approximately 2014, he also operated a seasonal business called the "Snack Shack" on Sandy Neck Beach in Barnstable, Mass. Cott stole food and commercial kitchen equipment for use and sale at his private business

Van Cott admitted that, between 2014 and June 2025, he defrauded the Plymouth Public Schools by taking food and equipment purchased with funds, including U.S. Department of Agriculture (USDA) funds, and using it to run the Snack Shack.

The equipment Van Cott ordered with school funds included two $2,200 refrigerators; a $3,950 two-door freezer; two 12-inch hot plates; a 24-inch griddle; a chargrill; a fryolator; shelving; a sandwich prep table; a convection oven; and hanging chalk boards. In addition, every summer starting in approximately 2014, Van Cott collected condiments, diced chicken, hot dogs, cooking oil, snacks, paper goods, coffee, food products and other miscellaneous items paid for by the Plymouth Public Schools or supplied by the USDA, then used and sold those items at the Snack Shack. Additionally, once or twice per week every summer starting in 2014, Van Cott directed Plymouth Public Schools cafeteria workers to slice at least nine pounds of deli turkey and 4.5 pounds of deli ham which he then sold at the Snack Shack. Van Cott also ordered over $3,000 in premium burger patties with school funds, which he intended to and did sell in menu items at the Snack Shack. (Source)

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Agriculture Company Employee Arrested For Stealing $1.5 Million Using Fraudulent Invoices Since 2014 - May 20, 2026

Police Officers arrested 49-year-old Patrick McCarty at his home. McCarty worked for Wilbur-Ellis, an agriculture supply company that provides products and services to farmers and ranchers. McCarty worked for the local branch in Minot North Dakota. Police said he used his position there to get around the company's normal checks and balances.

Wilbur-Ellis started looking into things after spotting issues with a couple of invoices from a business called PM Trucking. That review uncovered about 157 invoices going back to 2014 for deliveries that police say never happened.

Detectives say the payments meant for PM Trucking were actually being mailed to McCarty's home, which was listed in the system as the trucking company's address. The checks were then deposited into a Minot bank account registered to both PM Trucking and McCarty. (Source)

Site Manager For Logistics Company At Grocer's Distribution Center Charged With Stealing $250,000+ From Grocery Chain - May 20, 2026

Richard Lind, 30, worked as the site manager for a logistics company at the grocer's distribution center. Lind's employer supplied the physical labor and heavy equipment to unload trailers containing the grocer's inventory, as well as software for tracking shipments.

Lind defrauded the grocery chain by creating false records for inventory shipments that had never occurred and false invoices seeking payment from the trucking companies for unloading those shipments, the indictment says. The trucking companies then sought reimbursement from the grocery chain. Lind voided the false records to conceal his scheme from his employer.

He used the electronic payment authorization codes that resulted from his scheme to obtain cash payments at truck stops, triggering more than 600 fraudulent payments totaling more than $250,000, the indictment says. (Source)

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

IT Contractor Sentenced To Prison For Hacking Employer's Network In Retaliation For Termination / Caused $860,000+ In Damages - May 21, 2026

On May 14, 2021, Maxwell Schultz was terminated from his position as a contract employee in his company's information technology department. Shortly after, he accessed the company's network by impersonating another contractor to obtain login credentials.

Schultz ran a PowerShell script that reset approximately 2,500 passwords, locking thousands of employees and contractors out of their computers nationwide. Schultz also searched for ways to delete logs, PowerShell window events and cleared multiple system logs. The attack to the company's system caused more than $862,000 in losses, including employee downtime, customer-service disruptions and labor needed to restore the network. Schultz was ordered to pay $862,516.74 in restitution. As part of his plea, Schultz admitted to conducting the attack because he was upset about being fired. (Source)

Cargo Handling Company Employee Arrested For Leaking Sensitive Logistical Data To individuals Involved In Drug Related Crime - May 27, 2026

The Royal Netherlands Marechaussee detained a 24-year-old Amsterdam-based cargo worker at Schiphol on Tuesday, May 19, on suspicion of unauthorized access to computer systems and the leaking of confidential company information.

According to the ongoing investigation, the suspect allegedly used his access to a cargo handling company's systems at the airport to leak sensitive logistical data to individuals involved in drug-related crime.

The suspect is believed to have extracted critical data from company systems and passed it on to criminal networks. Drug trafficking groups reportedly used this information to facilitate the covert movement of narcotics through Schiphol, avoiding detection. (Source)

THEFT OF ORGANIZATIONS ASSESTS / DESTRUCTION OF PROPERTY

Company Engineer Sentenced To Prison For Stealing & Selling $986,000 Of Parts And Also Manufacturing & Selling Counterfeit Versions Of His Employer's Products - May 19, 2026

Shaun Brouwer, 47, worked as a mechanical engineer for an Illinois-based manufacturer of high-performance network infrastructure solutions, including network jacks. Brouwer stole proprietary information from the company and paid three vendors in China to manufacture jack modules and other products and falsely brand them as authentic products of Brouwer's former employer. Brouwer then arranged for the counterfeit products to be sold online.

Brouwer also sold approximately 11,267 authentic jack modules and other products that his employer had sent him after Brouwer falsely represented that he would use them at trade shows.

Brouwer admitted in a plea agreement that he sold a total of approximately 160,039 counterfeit and authentic products without the company's authorization, causing a loss to the company of approximately $986,519.

Brouwer further acknowledged that he asked a vendor in China to create fake payment documents to lower the perceived value of some of the counterfeit items in order to avoid attracting attention from U.S. customs officials and avoid paying additional customs duty fees.

As part of his schemes, Brouwer also fraudulently applied for and received a loan under the Covid-relief Paycheck Protection Program (PPP). In 2020, Brouwer received a $20,832 PPP loan for a purported side business and dispersed more than $10,000 of it to the online marketplace in China for counterfeit goods. (Source)

Terminated Amazon Employee Arrested For Slashing The Tires Of 29 Delivery Vehicles & Stealing Key Fobs - May 5, 2026

A former Amazon employee (Anthony Gillio) was arrested after being accused of slashing the tires of 29 delivery vehicles and stealing 23 key fobs. The business owner spoke to deputies and told them that a recently terminated employee, identified as Anthony Gillio, 22, was questioning his termination and could be connected to the vandalism, LCSO said.

Detectives investigated and were able to find Gillio with a license plate reader, which showed he had been in the area of the Amazon facility at the time of the incident, according to LCSO. Gillio was taken into custody. As detectives continued to investigate, they determined that following the vandalism, Gillio threw the missing key fobs, the knife he used and a pair of gloves into the Caloosahatchee River, LCSO said. Detectives searched the riverbed and located eight key fobs, a knife and a set of gloves. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Walgreen's Store Manager Sentenced To Prison For Role In 7 Inside Job Robberies That Stole $28,000+ - May 7, 2026

London Teeter, 22, of the District of Columbia, was sentenced to prison for her role in a series of 7 inside-job robberies in Washington, DC where she was employed as a store manager.

Teeter, and three co-conspirators devised a scheme to carry out armed robberies of the Walgreens store in Chinatown nearly once a month, beginning in July 2023, when either she or her co-conspirator were working. As a store manager, Teeter knew the timing of cash transfers within the business. In each robbery, a masked gunman entered the store, forced an employee into the manager's office or accessed the manager's office using a code provided by Teeter or her co-conspirator.

The gunman then robbed the employees and fled through a rear exit. Teeter and her co-conspirator took turns pretending to be the victim manager on duty, knowing that the robberies would be captured on internal surveillance.

In response to the robberies, the Chinatown Walgreens hired armed Special Police Officers to protect the business. Teeter was aware that armed Special Police Officers would be present during the robberies and that a co-conspirator robbed the officers of their firearms during the robberies.In the plea agreement, Teeter admitted that the co-conspirators stole and split at least $28,983. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Health Care Center Nursing Director Sentenced To Prison For Stealing Fentanyl For Her Own Use - April 29, 2026

The government alleged in court documents that on January 19, 2023, Kailyn Smotherman was discovered to have been tampering with controlled substances at the Garfield County Health Center, where she worked. After a search of her office, staff and law enforcement found numerous vials of fentanyl that had been tampered with (caps removed and replaced) or had been emptied. They discovered other controlled substances that had been replaced along with supplies for tampering with the containers of the controlled substances.

The discovery of Smotherman's conduct occurred when staff had entered her locked office to retrieve a narcotics log.

The office was in disarray and had hospital stock narcotics present, an IV pole, tourniquets, needles, IV equipment, replacement vial caps, replacement medication labels, and what appeared to be blood on many surfaces.

A search warrant was executed and multiple types of drugs were recovered, in liquid and tablet form, from Smotherman's desk, floor, trash and filing cabinets. Law enforcement also found items from the pharmacy med room that had been tampered with.

Staff reported being concerned patients may have received saline solution instead of pain medication in the months preceding the search of Smotherman's office on January 19, 2023.

A forensic chemist with the Food and Drug Administration conducted an analysis of the controlled substance containers confiscated from Smotherman's office for tampering and/or adulterating of substances and concluded such tampering and adulterating had occurred. (Source)

OTHER FORMS OF INSIDER THREATS

Terminated Chick-fil-A Employee Arrested For Stealing $80,000+ Through Fraudulent Refund Scheme - April 30, 2026

A former Chick-fil-A employee (Keyshun Jones) is accused of stealing more than $80,000 through a fraudulent refund scheme, police stated. In November 2025, police said Jones was recorded on surveillance video standing behind the counter at the restaurant from where he'd been terminated a month earlier.

Jones allegedly used the restaurant's register to ring up 800 orders of mac and cheese trays and then refunded them to his personal credit cards. Authorities said the refund totaled just over $80,000.
Jones evaded arrest after multiple attempts to locate him and was taken into custody on April 17, according to police. (Source)

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

Terminated Employee Pleads Guilty To Detonating Explosive Device Under Former Supervisor's Vehicle At His Residence - May 13, 2026

Michael Takacs, 44, admitted to denotating an explosive device under a vehicle that was parked at his former supervisor's residence.

After being terminated from his employment in or around April 2025, Takacs manufactured an improvised explosive device, commonly referred to as an IED, using explosive chemicals and a remote pyrotechnic device he purchased and filling the IED with shrapnel, including nails. In the early morning hours of July 26, 2025, Takacs transported the IED from Pennsylvania to his former supervisor's personal residence in Delran, New Jersey and placed it under a vehicle parked in the driveway. While transporting the IED, Takacs took steps to conceal his identity by removing the license plate from his vehicle, leaving his personal cell phone at his house, and wearing a mask on his face. Ultimately, Takacs remotely detonated the IED in an effort to intimidate his former supervisor and to damage and destroy the vehicle. (Source)

Disgruntled Athletic Club Employee Drove Car Packed With Explosives That Detonated Into Club & Dies - May 3, 2026

A disgruntled former employee of the Multnomah Athletic Club drove a car packed with explosives into the exclusive facility on the edge of downtown Portland early Saturday morning, causing massive damage before dying in a fiery wreck, two law enforcement sources with direct knowledge of the situation told The Oregonian / OregonLive.

Investigators believe that the former employee rented a black Nissan Rogue on Friday, which he used to drive into the building, careening around the first floor before setting off the explosive devices, believed to be a mix of propane tanks and pipe bombs, according to one of those sources.Some of the devices detonated and some did not, Sgt. Jim DeFrain, who heads the Metro Explosive Disposal Unit for the police bureau, said at a Saturday afternoon press conference. (Source)

Taco Bell Employee Arrested For Shooting A Customer For Using A Free Water Cup To Get Soda - May 4, 2026

D'Mari Patterson, an employee at a Taco Bell in West Palm Beach, Florida, was arrested after a dispute over a water cup escalated into a shooting inside the restaurant. Police say he fired multiple shots and injured two women.

Police responded around noon on April 27 to the Taco Bell on Military Trail and 45th Street after reports of gunfire. Investigators said three women entered the restaurant and asked for a free water cup. One of them allegedly used it to fill soda at a fountain, which triggered a verbal confrontation with Patterson, a 20-year-old employee.

Witness cellphone video captured the argument inside the dining area. Police said the video shows Patterson shouting, followed by the sound of a firearm being shot inside the restaurant. One woman was shot and fell to the ground, while another was grazed. A third woman ran outside.

Police said Patterson followed her and fired again, missing her but breaking a window near the entrance. Customers inside the restaurant ran for safety as confusion spread.

Some later told police they only realized what was happening after hearing additional shots and seeing damage near the entrance. The three women drove themselves to JFK North Medical Center. Two were treated for minor injuries and released, while the third was not injured, according to police.

After the shooting, Patterson called 911 and told dispatchers a customer had jumped behind the counter. He admitted firing the weapon and said he stored it in a management office before officers arrived, according to the arrest report. Patterson also claimed he believed the women were armed. However, investigators said no weapons were found, and surveillance footage did not support a self-defense claim. Police said the women appeared to be leaving when the second shot was fired. (Source)

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

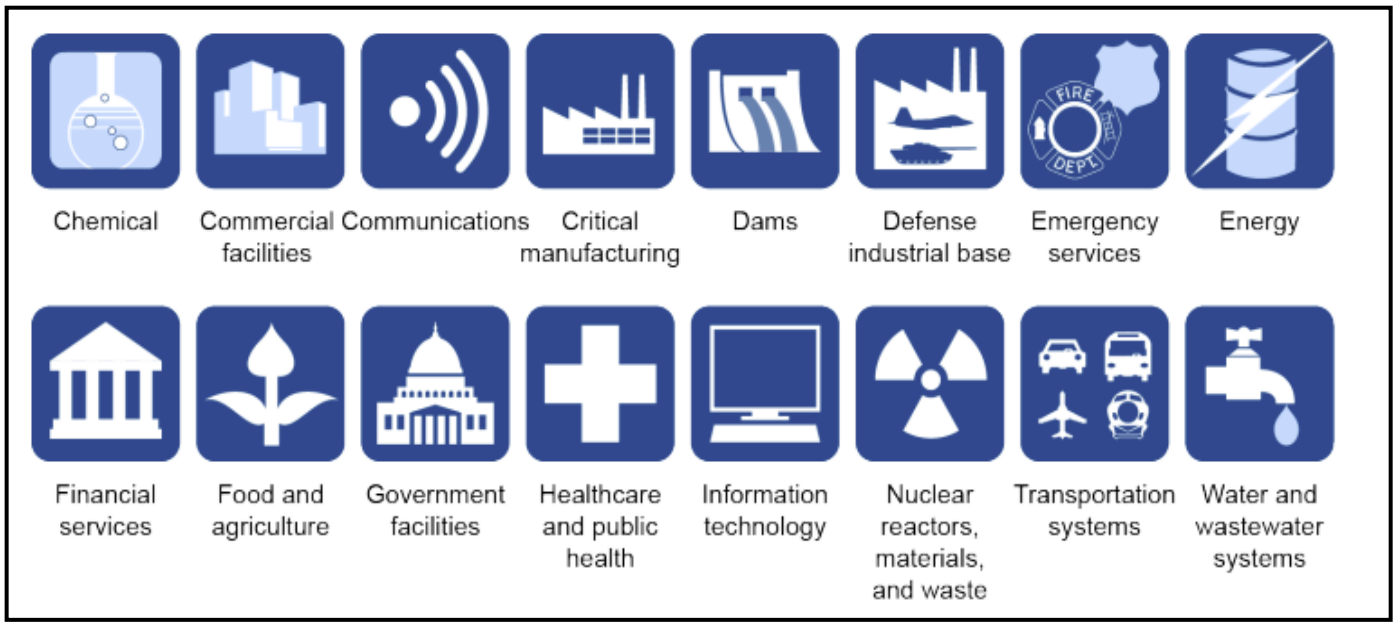
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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

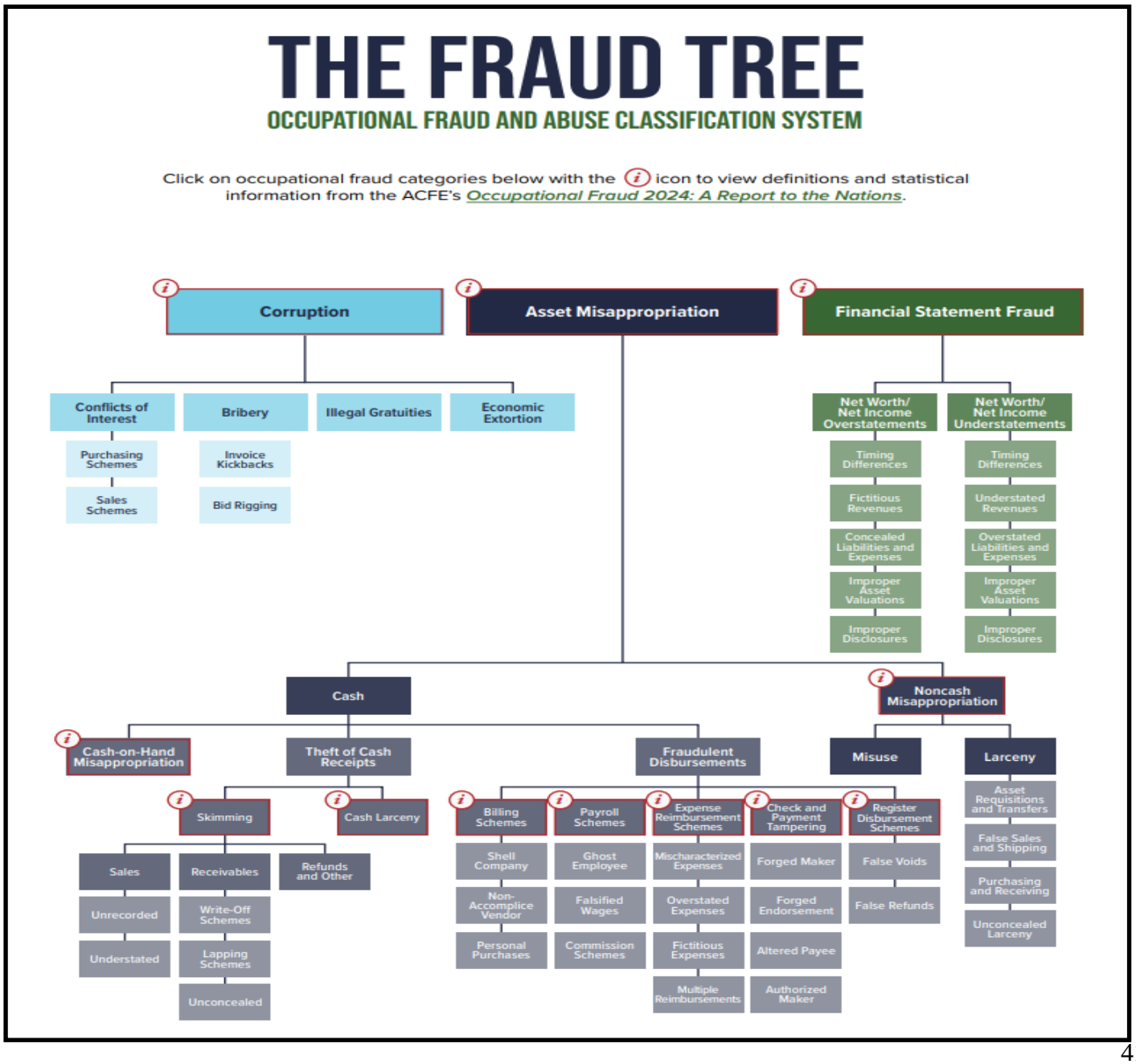
Other Tools

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

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

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

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

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

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

Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021
On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank's boardroom however the entire bank suffered smoke damage.

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

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

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

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

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

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

WORKPLACE VIOLENCE
Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024
Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

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

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

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

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

Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022

A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

A jury initially awarded more than $7 billion in damages in July, but the judge lowered that number to roughly $1.1 Billion.

Roy Holden, the former employee who murdered Thomas, performed a service call at her home in December 2019. The next day, while off-duty, he went back to her house and stole her credit cards as he was fixing her fax machine, then stabbed her to death before going on a spending spree with the stolen cards.

The attorneys also argued that Charter Spectrum hired Holden without reviewing his work history and ignored red flags during his employment. (Source) (Source)

Former Nurse Charged With Murder Of 2 Patients At Hospital, Nearly Killing 3rd By Administering Lethal Doses Of Insulin - October 26, 2022

Jonathan Hayes, a 47-year-old former Nurse at Atrium Health Wake Forest Baptist Medical Center in Winston-Salem, North Carolina, has been charged with 2 counts of murder and 1 count of attempted murder.

O'Neill said that on March 21, a team of investigators at the hospital presented him with information that Hayes may have administered a lethal dose of insulin to one patient and indicated there may be other victims.

The 1 count of murder against Hayes is related to the death of 61 year old Jen Crawford. Hayes administered a lethal dose of insulin to Crawford on Jan. 5. She died three days later.

The 2 count of murder is in connection with the death of 62-year-old Vickie Lingerfelt, who was administered a lethal dose of insulin on Jan. 22. She died on Jan. 27.

Hayes is also charged with administering a near-lethal dose of insulin to 62-year-old Pamela Little on Dec. 1, 2021. Little survived and Hayes faces one count of attempted murder.

Hayes was terminated from the hospital in March 2022, and he was arrested In October 2022. (Source)

Hospital Nurse Alleged Killer Of 7 Babies / 15 Attempted Murders - October 13, 2022

A neonatal nurse in the U.K. who allegedly murdered 7 babies and attempted to kill 10 more wrote notes reading, "I don't deserve to live," "I killed them on purpose because I'm not good enough to care for them. I am a horrible evil person."

Lucy Letby, 32, who worked in the Neonatal Unit of the Countess of Chester Hospital, left handwritten notes in her home that police found when they searched it in 2018, prosecutor Nick Johnson stated during her trial in October 2022.

Johnson argued that Letby was a constant, malevolent presence in the neonatal unit. Of the babies Letby allegedly murdered or attempted to murder between 2015 and 2016, the prosecution said she injected some with insulin or milk, while another she injected with air. She allegedly attempted to kill one baby three times.

Johnson told jurors the hospital had been marked by a significant rise in the number of babies who were dying and in the number of serious catastrophic collapses" after January 2015, before which he said its rates of infant mortality were comparable to other busy hospitals.

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours. Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans - May 11, 2021

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VAMC) in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

Indianapolis FedEx Shooter That Killed 8 People Was Former FedEx Employee With Mental Health Problems - April 20, 2021

Police say the 19 year old Indianapolis man who fatally shot 8 people at a southwest side FedEx Ground facility in April had planned the attack for at least nine months.

In a press conference, local and federal officials said the shooting was "an act of suicidal murder" in which Bandon Scott Hole decided to kill himself "in a way he believed would demonstrate his masculinity and capability while fulfilling a final desire to experience killing people."

Hole worked at the FedEx facility between August and October 2020. Police believe he targeted his former workplace not because he was trying to right a perceived injustice, but because he was familiar with the "pattern of activity" at the site.

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house.

Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check.

Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder - September 22, 2020

On August 12, 2003, Richard Wilbern walked into Xerox Federal Credit Union, located on the Xerox Corporation campus, and committed robbery and murder. Wilbern was not caught until 2016 for robbery and murder, and was sentenced this week to life in prison.

Richard Wilbern walked into Xerox Federal Credit Union (XFCU) and was wearing a dark blue nylon jacket with the letters FBI written in yellow on the back of the jacket, sunglasses and a poorly fitting wig. Wilbern was also carrying a large briefcase, a green and gray-colored umbrella and had what appeared to be a United States Marshals badge hanging on a chain around his neck.

Wilbern was employed by Xerox between September 1996 and February 23, 2001 as which time he was terminated for repeated employment related infractions. In 2001, Wilbern filed a lawsuit against Xerox alleging that the company unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. Wilbern also maintained a checking and savings accounts at the Xerox Federal Credit Union. Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy.

In March 2016, a press conference was held to seek new leads in the investigation. Details of the crime were released as well as photographs of Wilbern committing the robbery. Anyone with information was asked to call a dedicated hotline.

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

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

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

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

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

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

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

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

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

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

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

CTTP = China Thousand Talents Plan

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

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

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 (**7,100+ 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)

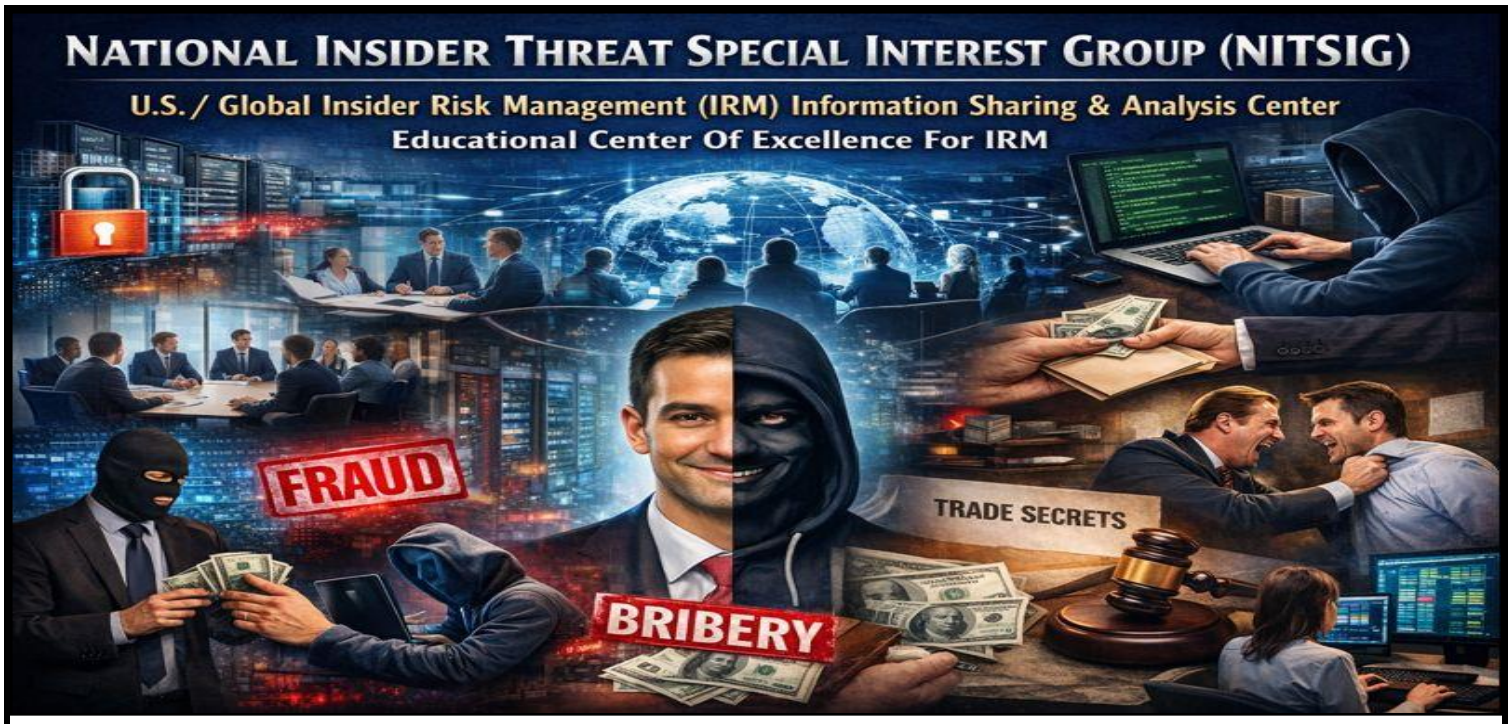
Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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 Table Top Exercises For Individuals Managing & Supporting Program
- ✓ 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