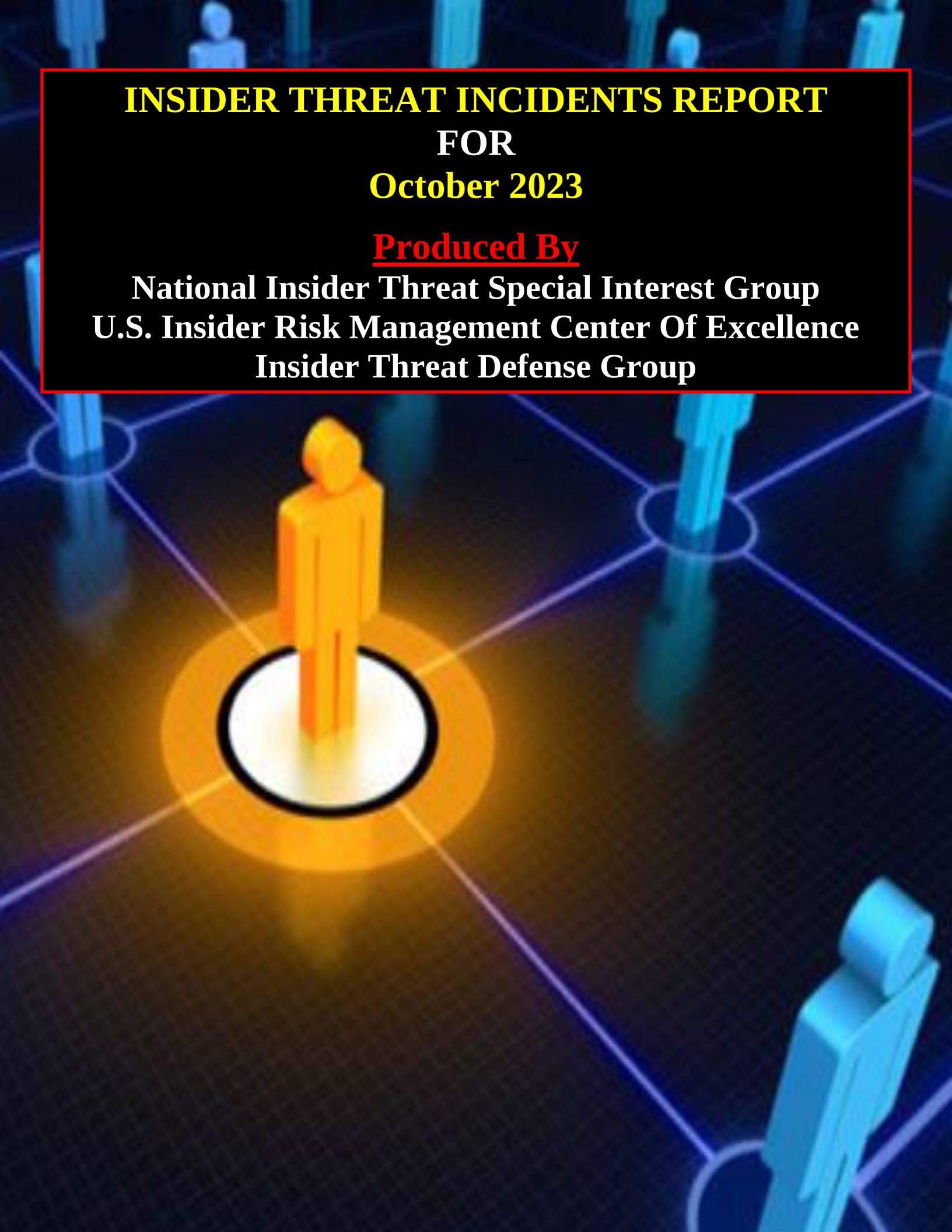
INSIDER THREAT INCIDENTS REPORT
FOR
October 2023

Produced By

National Insider Threat Special Interest Group
U.S. Insider Risk Management Center Of Excellence
Insider Threat Defense Group



INSIDER THREAT INCIDENTS

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 10+ years. This research has evaluated and analyzed over **4,900+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

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

According to the Association of Certified Fraud Examiners 2022 Report to the Nations, organizations with less than 100 employees' suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one must look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to **significant underreporting** on the Insider Threat problem.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the **Actual Malicious Actions** employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live a better lifestyle, etc.

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

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

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report shows.

These monthly reports are recognized and used by Insider Risk Program Managers working for major corporations, as a **TRUSTED SOURCE** for education to gain support from CEO's, C-Suite, Key Stakeholders and Supervisors for detecting and mitigating Insider Threats. The incident listed on pages **7 to 24** of this report provide the justification, return on investment and funding needed for developing, managing or optimizing an Insider Risk Management 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.

DEFINITIONS OF INSIDER THREATS

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 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

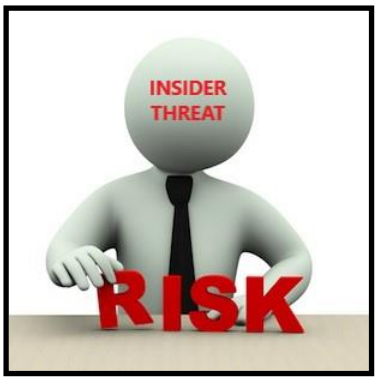
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

- ☐ 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
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction (Downtime
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead

Reputation Impact

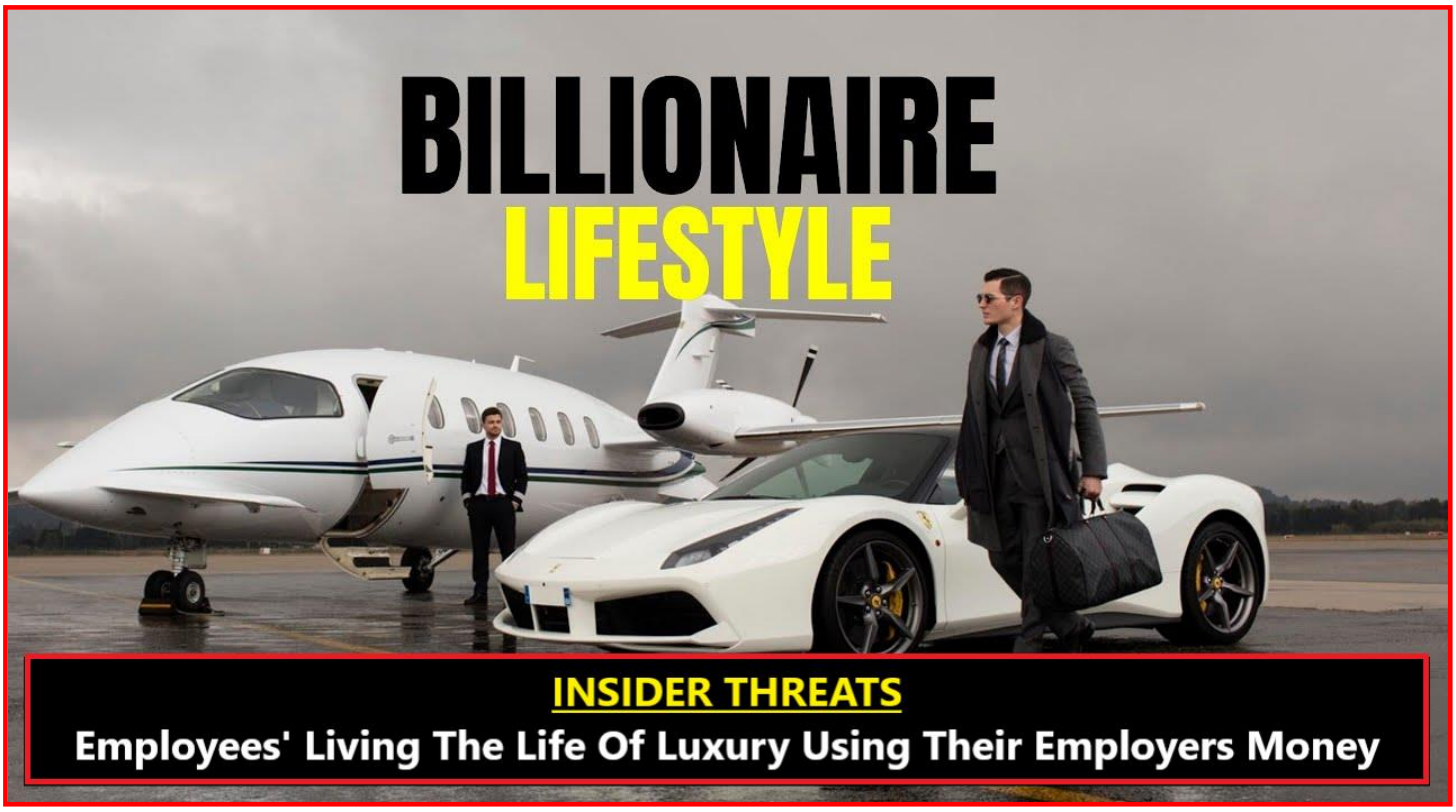
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees'

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ Employees' Loose Jobs / Company Goes Out Of Business



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

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

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

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

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

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

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

INSIDER THREAT INCIDENTS
FOR OCTOBER 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT
Senator Ted Cruz Issues Chilling Warning On Biden Appointed Iranian Spies Working In The U.S. Government - October 22, 2023

Senator Ted Cruz is pulling the curtain back on three "Iranian Spies" who were allegedly working at senior levels within the Biden administration, claiming that one of the Iran "sympathizers" is regularly accessing classified materials while working as a Chief Of Staff in the Department of Defense.

Cruz Stated:

"Rob Malley remains one of the greatest national security scandals in our nation's history. Rob Malley was Joe Biden's Chief Negotiator For Iran. He's an incredible Iran sympathizer. He is an advocate, a passionate advocate for the disastrous Obama-Iran nuclear deal. He's been fired. He's had his security clearances stripped, which I want you to pause and think, just how bad does his conduct have to be to have his security clearances pulled by the White House?

But we now know also that, among other things, three of Rob Malley's top advisers, his inner circle that he relied on, were Iranian operatives. They were recruited by the government of Iran. They were directed by the Iranian foreign minister. They reported to the Iranian foreign minister.

We have their emails now in which they discuss, one of them discusses with the foreign minister that his loyalties are with the government of Iran, and he is there to do whatever they direct, including making the message from within the federal government that there's nothing wrong with Iran having a nuclear stockpile. You literally had three Iranian spies working in senior positions directly around the U.S. government.

One of them, as far as we know, remains a chief of staff in the Department of Defense to this day with access to classified documents." (Source)

U.S. Postal Worker Charged For Role In Stealing Business Checks Worth Over $1.9 Million From Post Office For Personal Use - October 21, 2023

From November 2022 to April 2023, Dontavis Truesdale worked as a Processing Clerk at the Ballantyne Post Office in Charlotte Noth Carolina.

Truesdale used his position as mail processing clerk to steal hundreds of checks of businesses that maintained post office boxes at the post office. Truesdale sold the stolen checks to other co-conspirators who committed bank fraud, by depositing the stolen checks into bank accounts they controlled, and then quickly removed the funds before the banks detected the fraud. Truesdale stole more than 200 checks with a total face value of over $1.9 Million. (Source)

U.S. Postal Service Employee Admits To Defrauding The USPS Of $874,000+ For Personal Use - October 16, 2023

Ephrem Nguyen was employed by the U.S. Postal Service (USPS) as the Postmaster of the Danbury Post Office in Danbury, Connecticut .

His responsibilities that included supervising the maintenance and repair of all equipment, facilities, and vehicles assigned to the post office. In November 2020, Nguyen required that all Danbury Post Office vehicle maintenance and repair work be performed by a certain vendor, even though Nguyen knew that another vendor already had a contract for with the Danbury Post Office for those services. Nguyen demanded that the vendor provide free vehicle maintenance and repairs for himself, one of his children, a USPS employee, and employee of Nguyen's personal business. In 2022, Nguyen solicited and received $90,000 in cash bribes from the vendor. In exchange for these bribes, Nguyen caused the USPS to overpay the vendor for vehicle maintenance and repair, which Nguyen characterized as a "raise." Between approximately January 2022 and February 2023, Nguyen used USPS credit cards to pay the vendor more than $1 million, or approximately $760,000 more than necessary to pay for legitimate maintenance and repair work.

In addition, Nguyen embezzled more than $80,000 from the USPS by using his USPS credit cards to rent vehicles for the personal use of himself and others, and he approved more than $8,000 in fraudulent travel expense reimbursement claims for a co-worker.

Through these schemes, Nguyen defrauded the USPS of approximately $874,930.59. (Source)

Former Social Security Employee Admits To Creating Fake Children's Profiles To Steal $157,000+ Of Government Money For Personal Use - October 3, 2023

Lee Nichols is a former Claims Specialist with the Social Security Administration (SSA).

Nichols admitted to creating fictitious profiles for two children that did not exist. He linked the profiles to a recently deceased man and disabled woman living in Mexico in an attempt to create a survivor benefits application.

Nichols ensured that the debit cards for the children's benefits were sent to the address of someone with whom he was associated. He would then use the debit cards to make regular withdrawals at ATMs. When making those withdrawals, he attempted to disguise himself by using hats pulled down over his face, sunglasses, balaclavas and other clothing to conceal his appearance.

In addition, the IRS issued economic stimulus payments of $1,400 to each fictitious child.

As part of his plea, Nichols took responsibility for over $75,000 in loss to the federal government. He also agreed to pay $82,516 in restitution to the SSA and $2,800 in restitution to the IRS. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former NSA Employee Pleads Guilty To Attempted Espionage / To Release Top Secret Classified Information - October 23. 2023

From June 6, 2022, to July 1, 2022, Jareh Dalke was an employee of the National Security Agency (NSA) where he served as an Information Systems Security Designer.

Dalke admitted that between August and September 2022, in order to demonstrate both his "legitimate access and willingness to share," he used an encrypted email account to transmit excerpts of three classified documents to an individual he believed to be a Russian agent. In actuality, that person was an FBI online covert employee. All three documents from which the excerpts were taken contain NDI, are classified as Top Secret//Sensitive Compartmented Information (SCI) and were obtained by Dalke during his employment with the NSA.

On or about Aug. 26, 2022, Dalke requested $85,000 in return for all the information in his possession. Dalke claimed the information would be of value to Russia and told the FBI online covert employee that he would share more information in the future, once he returned to the Washington, D.C., area.

Dalke subsequently arranged to transfer additional classified information in his possession to the purported Russian agent at Union Station in downtown Denver. Using a laptop computer and the instructions provided by the FBI online covert employee, Dalke transferred five files, four of which contain Top Secret NDI. The other file was a letter, which begins (In Russian & Cyrillic Characters) "My friends!" and states, in part, "I am very happy to finally provide this information to you. . . . I look forward to our friendship and shared benefit. Please let me know if there are desired documents to find and I will try when I return to my main office." The FBI arrested Dalke on Sept. 28, moments after he transmitted the files. (Source)

Former U.S. Navy Service Member Sentenced To Prison For $2 Million Insurance Fraud Scheme - October 17, 2023

Christopher Toups, who at the time of his crimes was a Chief Petty Officer in the U.S. Navy, was sentenced in federal court to 30 months in prison after admitting that he and others defrauded an insurance program meant to compensate service members who suffer serious and debilitating injuries while on active duty.

According to his plea agreement, participants in the scheme obtained approximately $2 Million in payments from fraudulent claims submitted to Traumatic Service Members Group Life Insurance Program, or TSGLI, and Toups personally obtained about $400,000. TSGLI was funded by service members and the Department of the Navy.

Toups admitted that from 2012 to at least December 2015, he conspired with his then-spouse Kelene McGrath, Navy Dr. Michael Villarroel, and others to obtain money from the United States by making claims for life insurance payments based on exaggerated or fake injuries and disabilities. (Source)

Former Navy IT Manager Sentenced To Prison For Hacking A Computer Database, Stealing 9,000 People's Identities & Selling Information For $160,000 In Bitcoin - October 16, 2023

Marquis Hooper is a former Navy IT Manager.

In August 2018, Hooper opened an online account with a company that runs a database containing the PII for millions of people. The company restricts access to the database to businesses and government agencies that have a demonstrated, lawful need for the PII. Hooper, however, opened his database account by falsely representing to the company that the Navy needed him to perform background checks.

After Hooper opened his database account, he added his wife and co-defendant, Natasha Chalk, to the account. They then stole over 9,000 people's PII and sold it to other individuals on the dark web for $160,000 in bitcoin. At least some of the individuals to whom Hooper and Chalk sold the PII used it to commit further crimes.

In December 2018, Hooper's database account was closed for suspected fraud. Thereafter, Hooper, Chalk, and a co-conspirator tried to regain access to the database. Hooper instructed the co-conspirator to open a new database account by representing that the Navy needed him to perform background checks just like Hooper had done. Hooper offered to pay the co-conspirator $2,500 for each month that the database account was opened. The co-conspirator submitted an application to open the database account and the company told him that a supply officer had to sign the contract.

Hooper then sent the co-conspirator multiple documents falsely identifying an identity theft victim as the supposed Naval supply officer.

These documents included a false contract, a fake driver's license for the identity theft victim, and a forged letter purporting to be from a commanding officer in the Navy. The co-conspirator submitted the fake documents to the company, but the company decided not to open the new database account. (Source)

Former Army Reservist Pleads Guilty For Role In Stealing $101,000+ Of Government Funds For Personal Use - October 13, 2023

Starting in January 2013, and continuing until in or about August 2016, Christopher O'Connor and co-conspirators conspired to obtain money from the Army States under false pretenses by submitting false applications to the Army for military funeral honors (MFH) payment requests for services that had not been performed. O'Connor proposed submitting false MFH pay requests in the co-conspirators' names in exchange for each sharing their proceeds with O'Connor. In addition to receiving a split of the fraudulent MFH payments from the co-conspirators, O'Connor also submitted and received approximately $18,825.83 in fraudulent MFH payment requests for himself. As a result of this conspiracy, the United States government was defrauded out of approximately $101,858.19.

The National Defense Authorization Act of 2000 authorizes MFH for active-duty soldiers, retirees, and veterans. At a family's request, eligible persons can receive military funeral honors, including the folding and presenting of the United States flag and the playing of Taps. (Source)

Former Army Sergeant Arrested / Charged For Efforts To Give Classified Information To China

A former U.S. Army sergeant was arrested Friday at the San Francisco airport and indicted on charges that he unlawfully retained classified information and attempted to deliver it to China's security services, the Justice Department announced.

Joseph Schmidt, 29, served as an active duty soldier between 2015 and 2020 with his primary assignment at Joint Base Lewis-McChord in Washington state, prosecutors said. In his role, Schmidt had access to SECRET and TOP SECRET information.

After his separation from the military, Schmidt allegedly reached out to the Chinese Consulate in Turkey and later, the Chinese security services via email offering information about national defense information.

In March 2020, Schmidt traveled to Hong Kong and allegedly continued his efforts to provide Chinese intelligence with classified information he obtained from his military service.

He allegedly retained a device that allows for access to secure military computer networks and offered the device to Chinese authorities to assist them in efforts to gain access to such networks. (Source)

U.S. Navy Sailor Pleads Guilty To Receiving $14,000+ In Bribes And Transmitting Sensitive U.S. Military Information To Chinese Intelligence Officer - October 10, 2023

Petty Officer Wenheng Zhao worked at Naval Base Ventura County in Port Hueneme and held a U.S. security clearance.

He admitted he engaged in a corrupt scheme to collect and transmit sensitive U.S. military information to the intelligence officer in violation of his official duties.

Between August 2021 and at least May 2023, Zhao admitted receiving at least $14,866 in at least 14 separate bribe payments from the intelligence officer.

In exchange for the illicit payments, Zhao surreptitiously collected and transmitted to the intelligence officer sensitive, non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao admitted he entered restricted military and naval installations to collect and record this information.

Zhao specifically admitted to transmitting plans for a large-scale maritime training exercise in the Pacific theatre, operational orders, and electrical diagrams and blueprints for a Ground/Air Task Oriented Radar system located in Okinawa, Japan.

Zhao further admitted to using sophisticated encrypted communication methods to transmit the information, destroying evidence, and concealing his relationship with the intelligence officer. (Source)

DoD Chief Information Officer Charged With Facilitating Dog Fighting Ring - October 2, 2023

Frederick Moorefield and Mario Flythe have been charged with promoting and furthering animal fighting venture.

Frederick Moorefield, a Deputy Chief Information Officer for Command, Control, and Communications, for Office of the Secretary of Defense, and Flythe used an encrypted messaging application to communicate with individuals throughout the United States to discuss dogfighting. Moorefield used the name "Geehad Kennels" and Flythe used the name "Razor Sharp Kennels" to identify their respective dogfighting operations.

For example, as detailed in the affidavit, Moorefield, Flythe and their associates used the encrypted messaging application to discuss how to train dogs for illegal dogfighting, exchanged videos about dogfighting, and arranged and coordinated dogfights. Moorefield and Flythe also discussed betting on dogfighting, discussed dogs that died as a result of dogfighting, and circulated media reports about dogfighters who had been caught by law enforcement. As further alleged in the affidavit, Moorefield and others also discussed how to conceal their conduct from law enforcement.

On September 6, 2023, law enforcement officers executed search warrants at Moorefield and Flythe's residences in Maryland. Following the execution of these warrants, twelve dogs were recovered and seized by the federal government. Law enforcement also recovered veterinary steroids, training schedules, a carpet that appeared to be stained with blood, and a weighted dog vest with a patch reading "Geehad Kennels." In addition, law enforcement officers seized a device consisting of an electrical plug and jumper cables, which the affidavit alleges is consistent with devices used to execute dogs that lose dogfights. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

17 Sheriff Office Employees Charged With $495,000+ Of COVID-19 Pandemic Relief Fraud For Personal Use - October 12, 2023

The charges were brought in 17 separate cases filed in the United States District Court for the Southern District of Florida. The charges allege that 17 defendants participated in independent schemes to defraud the U.S. Small Business Administration (SBA) and participating lenders by fraudulently applying for loans and other relief through the PPP and EIDL program. These programs were designed to provide emergency financial assistance to the millions of Americans who were suffering from the economic effects caused by the COVID-19 pandemic.

In total, the defendants allegedly received $495,171 in assistance unlawfully and used the proceeds to unjustly enrich themselves. (Source)

Former County Sheriff Sentenced To Prison For Stealing $89,000+ From Police Department For Personal Use - October 13, 2023

Keith Cooper was the a County Sheriff for approximately 20 years, until retiring in December 2018. Cooper's position gave him access to funds the Sheriff's Office seized from drug trafficking investigations, including a bank account designed to hold those proceeds.

Over a four-year period, Cooper made numerous unauthorized cash withdrawals and unlawfully retained proceeds from drug trafficking investigations instead of depositing them into the account. Cooper wrongfully took $58,230 in proceeds, which included $46,100 in unexplained cash withdrawals from the bank account and $12,130 in forfeited proceeds that should have been deposited. Cooper also wrongfully took $29,458.87 in ammunition paid for with Sheriff's Office funding and wrongfully used county funds to pay for $1,837.26 in fuel used during his personal trips in 2018. (Source)

Special Agent For Homeland Security Investigations Sentenced To Prison For Accepting $50,000 In Kickbacks From Informant - October 23, 2023

Anthony Sabaini was assigned to the Oakbrook Terrace, Illinois field office of Homeland Security Investigations (HSI), a criminal investigative unit within DHS.

Evidence at trial revealed that Sabaini maintained a corrupt relationship with an HSI confidential informant and tipped off the informant to sensitive investigations conducted by other law enforcement agencies, including the FBI and DEA. In exchange for Sabaini's protection, the informant paid Sabaini at least $50,000. Sabaini also stole cash from drug dealers and pocketed money from HSI that had been earmarked for investigative activity.

Sabaini deposited more than $250,000 into a bank account for which he was the sole signatory. He made the deposits in more than 160 transactions, with the amount of each deposit being less than $10,000. The deposits were structured in an effort to evade federal reporting rules, which require financial institutions to notify the U.S. Department of the Treasury about transactions of more than $10,000. (Source)

The evidence also showed that Sabaini lied on official HSI memoranda in 2017 and 2018 to protect his corrupt relationship with the informant. (Source)

Police Detective Pleads Guilty To Accepting Illicit Benefits From Colombian Art Dealer In Exchange For Immigration Help - October 13, 2023

Paul Gollogly began working for the Murrieta Police Department (MPD) in California, in March 2013, to lead its purported anti-money laundering program. In this role, he handled and directed confidential informants (CI) registered with the department, including non-U.S. citizens who needed authorization from the U.S. government to enter and work in the United States.

In April 2013, Gollogly registered an individual – identified in court documents as "Person A" – as a CI with MPD. Person A was a Colombian national and a wealthy art dealer who had significant business interests in Colombia, the United States, Mexico, Panama, and Spain. Person A owned art galleries in New York and Spain, as well as a hotel in Mexico.

From April 2013 to February 2020, Gollogly helped Person A obtain various immigration benefits, including authorization from the U.S. Department of Homeland Security (DHS) to allow Person A to enter and work in the United States for one year at a time and facilitation of Person A's physical entry into the United States. Gollogly also attempted to assist with Person A's permanent residency application.

Gollogly wrote letters of support to DHS for Person A's approvals to enter the United States, falsely stating that Person A's work as a CI resulted in arrests, seizures of large amounts of money and drugs, and additional investigations. In fact, the information Person A provided MPD resulted in none of these things.

Also, on at least 25 occasions, Person A texted Gollogly to inform him of Person A's arrival in the United States, including Person A's arrival date and location, and flight information in case Person A got held up at a port of entry by immigration authorities. On at least five occasions, after receiving notice of Person A's arrival at the San Ysidro Port of Entry at the U.S.-Mexico border, Gollogly personally drove to San Ysidro to meet Person A and facilitate Person A's incident-free reentry into the United States.

In exchange for this help with immigration authorities, Gollogly solicited and received benefits from Person A, including:

- Receiving tickets to art shows in New York and Miami.
- The hiring of a Gollogly family friend to work at one of Person A's businesses and making efforts to help a Gollogly relative secure a job with a major philanthropist, whom Person A knew personally.
- Arranging for hotel stays for two close Gollogly relatives and another Gollogly friend at Person A's hotel in Mexico.
- Paying four months' rent in 2018 and 2019 for a Gollogly relative who was living in New York City.
- Paying for dinner at an upscale New York restaurant for Gollogly and four of his relatives in December 2019. (Source)

State Penitentiary Corrections Officer Sentenced To Prison For Drug Trafficking - October 23, 2023

Leticia Rodriguez a Corrections Officer at a state penitentiary in Washington state.

Rodriguez was part of a large drug trafficking organization that involved a legitimate landscaping business to cover up the organizations drug trafficking activities. Investigators developed information that Rodriguez would act a courier for cocaine, fentanyl, and methamphetamine as well large amounts of money between Eastern Washington, Arizona and California. She was arrested at the Walla Walla State Penitentiary, where she worked as a corrections officer. (Source)

Former Customs & Border Protection Officer Sentenced To 5 Years' Probation For Violating Airport Security Requirements - October 30, 2023

From 2018 through 2022 Supreme Jones was an armed CBP officer assigned as a uniformed officer at the Baltimore Washington International / Thurgood Marshall Airport (BWI). As a result of his duties, Jones was issued credentials authorizing him to go into any area of BWI, including the areas beyond the Transportation Security Administration (TSA) security checkpoints, for the performance of his official duties.

In June 2021, the FBI began an investigation into complaints that Jones was abusing his authority by using his credential to enter secure areas when not performing official duties, specifically when flying for personal travel. During a 14 month period Jones made more than 60 flights, either going from or returning to BWI. Upon review of surveillance imagery corresponding to the entry point hits, the FBI discovered that Jones was often entering the sterile area of BWI via the controlled exit portals when in civilian clothing by displaying his badge to the TSA Officer or TSO on duty at the exit portal.

On February 21, 2022, Jones flew from BWI to Atlanta, GA. He did not declare himself to be armed on this flight. Nonetheless, while in civilian clothes, he used his badge to access the security area to proceed to his departure gate within. When he arrived at the gate, he engaged in a conversation with the airline personnel, appeared to display a previously unseen limp and obtained a special needs boarding pass from the airline, thus enabling him priority boarding of the aircraft.

On April 5, 2022, FBI agents conducted surveillance of Jones in BWI. They saw Jones, while still on duty and in his uniform, jump a long line of passengers in line at an airline ticket counter to check-in for a flight he was taking later that day in his personal capacity.

As a result of his federal conviction, at least during his five year term of probation, Jones will not be able to be employed in law enforcement. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Manager Of Sweepstakes Gaming Company Sentenced To Prison For Paying State Lawmaker $10,000 In Bribes - October 12, 2023

James Weiss owned Collage LLC, a gaming compnay.

In 2019, Weiss paid thousands of dollars in bribes to then-Illinois State Representative Luis Arroyo. The bribes were paid from Weiss's gaming company, Collage LLC, in the form of checks made payable to Spartacus 3 LLC, Arroyo's private lobbying firm in Chicago. In exchange for those bribes, Arroyo promoted legislation in the Illinois General Assembly related to the sweepstakes industry and advised other state lawmakers to support the legislation.

Weiss caused two checks totaling $5,000 to be delivered to the Senator. Each check was made payable to a fictitious third party and labeled as a consulting payment. Weiss later falsely told law enforcement that he had personally spoken to the fictitious third party. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former County Education Official Arrested For Embezzling $14 Million+ From School District / Used Funds To Buy House, SUV Etc. - October 21, 2023

Jorge Contreras is a former Senior Director of Fiscal Services working for a county public school district . He was arrested today on a federal criminal complaint alleging he embezzled more than $14 million from the district over a 7 year period and used the illicitly obtained funds to finance a house, buy luxury items, and obtain cosmetic treatment from a dermatologist.

From August 2016 to July 2023, Contreras embezzled more than $14 Million from the school fistrict by making unauthorized payments to himself from district funds, payments that came from more than 250 checks from the district that were deposited into Contreras' personal bank account. The checks ranged from approximately $11,000 to approximately $95,000 and listed fictitious persons as the payee, the affidavit alleges.

From August 2022 to July 2023 alone, Contreras allegedly embezzled more than $4.1 Million from the school district. Contreras used the embezzled funds to pay more than $1.9 Million to American Express, withdraw $325,000 in cash from ATMs, and transfer more than $130,000 to his partner, whom he married in August 2023. Contreras allegedly also used the illicitly obtained funds to purchase his residence in Yorba Linda for approximately $1.5 Million as well as a BMW SUV for approximately $127,000, which he used to deposit embezzled funds into his personal bank account via drive-thru ATMs.

Contreras purchased the Yorba Linda residence in 2020 and paid for more than $1 million of it via a wire transfer from his personal bank account. Contreras also allegedly altered bank statements submitted as part of the loan application for this property to hide funds he embezzled from the school district. (Source)

Public Schools' Employee Pleads Guilty To Creating $603,000+ Of Fraudulent Invoices / Purchase Orders - October 20, 2023

Devin Fletcher is the former Chief Learning and Talent Officer for Tulsa Public Schools (TPS).

Fletcher was hired in August of 2016 to be the District's Chief Academic Officer. He was promoted to be the District's Chief Learning and Talent Officer prior to his resignation in June 2022. Fletcher was responsible for human resources and educational performance issues throughout TPS. Fletcher was entrusted with limited hiring and firing authority for certain personnel, including consultants where he had limited expenditure approval authority.

While working for TPS, Fletcher, admitted to working with another person to create, alter, and fabricate fraudulent invoices, purchase orders and supporting documents to defraud TPS and the Foundation for Tulsa Schools (Foundation). The Foundation is a public charity recognized as a 501(c)(3) organization with a mission to build a better community through the support of TPS by providing education resources via donated funds. In total, Fletcher's fraudulent actions caused a loss of at least $603,992.32 to TPS and the Foundation. (Source)

Former University Professor Charged For Theft Of Grant Funds / Used Funds For Personal Use - October 20, 2023

Xinjian Kevin He, is a former West Virginia University Professor, who was working in the engineering department.

He allegedly embezzled federal grant funding, using the money to purchase clothing, furniture, home goods, and electronics for his personal use.

The indictment was returned in November of 2020 but remained sealed because the defendant fled the country and wasn't arrested until September 26, 2023, when he entered the United States from Canada and was apprehended in New York. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Loan Officer Sentenced To Prison For $2.6 Million+ Bank Fraud / $270,000 Kickback Scheme - October 20, 2023

Two operators of a loan brokerage business and a loan officer at a Massachusetts-based bank were sentenced today for conspiring to defraud a bank and the U.S. Small Business Administration (SBA).

Ted Capodilupo, Joseph Masci and Brian Ferris were each sentenced to one year and one day in prison and two years of supervised release. Additionally, Capodilupo and Masci were each ordered to pay restitution of $1,424,087 and Ferris was ordered to pay restitution of $1,236,251.

Between 2015 and 2018, Capodilupo, Masci and Ferris agreed to defraud a bank and the SBA by submitting fraudulent loan applications to the bank, which administered the SBA's small business express loan program, to secure bank loans guaranteed by the SBA. Capodilupo and Masci submitted dozens of fraudulent loan applications on behalf of borrowers who were ineligible for traditional business loans. These loan applications misrepresented, among other things, the identity of the real loan recipients and the businesses for which the loans were sought.

Capodilupo and Masci also falsified applicant signatures and falsely indicated that no broker had assisted in preparing or referring the loan applications, when they in fact charged borrowers excessive fees for obtaining these fraudulent loans.

Ferris, who worked as a loan officer at the bank, processed the fraudulent loan applications and in some cases fabricated federal tax forms in support of the applications. Ferris caused the bank to issue loans for which Capodilupo and Masci submitted applications and received a kickback from Capodilupo and Masci of approximately $500 per loan. The scheme generated approximately $270,000 in fees for Capodilupo and Masci.

Many of the loans that the bank issued as a result of the fraudulent applications ultimately defaulted, resulting in substantial losses to the bank. (Source)

Wells Fargo Former Bank Manager Pleads Guilty To Stealing $1.2 Million+ From Bank Customers - October 12, 2023

Brian Davie worked for Wells Fargo from March of 2014 until he was fired in June 2019.

Davie used his position as a Manager at the branch to conduct unauthorized transactions. Davie had access to customer files containing information about bank account balances.

Davie hid his criminal activity by repeatedly exchanging cashier's checks until they were small enough to cash without triggering banking reporting requirements.

Davie continued undetected because he stole from elderly customers who might be less likely to closely monitor their account balances. Some of Davie's victims had dementia or had limited English skills and did not understand banking transactions.

In at least one case, Davie failed to file the paperwork to install a victim's relative as a co-signer on the victim's accounts. That failure prevented the relative from being able to monitor the account and detect the fraudulent transactions.

Davie deposited some of the stolen money in an account he created in the name of a relative's business. He made some of the cashier's checks payable to that relative or to the business account he created. Much of the money was withdrawn as cash.

In all Davie embezzled S1,279,840 from victim accounts. Wells Fargo reimbursed victims for their losses. Judge Settle will determine the amount of restitution at sentencing. (Source)

Bank Employee Charged With Accepting Bribes To Facilitate Millions Of Dollars of Money Laundering - October 30, 2023

Oscar Flores worked for an international financial institution, at a branch located in Scotch Plains, New Jersey.

Starting in early 2022, Nunez exploited his position as a bank employee to facilitate money laundering activities in exchange for bribes. Nunez used his position and inside access to open bank accounts in the names of shell companies with nominee owners. Those accounts were then used to launder narcotics proceeds, including to Colombia. Nunez assisted the money laundering efforts by giving those who bribed him online access to the accounts, along with dozens of debit cards for the accounts that were later used to withdraw cash from ATMs in Colombia. Nunez received thousands of dollars in bribes for each account he opened. The investigation has revealed that millions of dollars were laundered to Colombia through accounts opened by Nunez since early 2022. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

CHINESE ESPIONAGE TARGETING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

No Incidents To Report

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

Secretary - Treasurer Sentenced To Prison For Embezzling $1.7 Million+ - October 13, 2023

Catherine Skidmore was employed as the Secretary - Treasurer of the Black Canyon Irrigation District (BCID), a state water supply organization, from approximately January 2014 through July 2022. As the Secretary - Treasurer of the BCID, Skidmore, among other things, handled fee collecting, bill payments, management of the investment accounts, and maintained the BCID's QuickBooks database and ledgers.

Beginning in May 2019 and continuing to July 2022, Skidmore knowingly devised a scheme to defraud the BCID by embezzling more than $1.7 million through the use of an elaborate series of transfers between the BCID's various financial accounts. To implement the scheme, in May 2019, using a falsified form containing the forged signature of a member of the board of directors. (Source)

Former Company Marketing Employee Sentenced To Prison For $1 Million+ Bank Fraud & Identity Theft Scheme - October 27, 2023

Between 2013 and 2019, Karen Crutchfield was employed as an Account Manager at Good Advertising in Memphis, Tennessee. Crutchfield handled the company payroll, accounts receivable, and accounts payable.

Crutchfield used her access to create false invoices, duplicate or fictitious vendors, and more than 620 fraudulent checks, totaling approximately $662,000. In addition, she stole more than $168,740 from the owners' profit-sharing account and used company credit cards to pay nearly $59,000 in personal expenses and withdraw $82,000 in cash advances. She inflated her wages, telling the company's payroll processer that her annual salary was $95,000 – more than double the $45,000 she legitimately earned. Crutchfield used her access to the company owners' personal identifying information to apply for a business loan without permission, in an apparent effort to cover the shortfall caused by her theft. (Source)

Salesman For IT Company Admits To Embezzling $750,000+ From Employer - October 16, 2023

Thomas Syddall worked as Salesman for an Information Technology Corporation, which was owned by Anderson ZurMuehlen & Co.

From about March 2020 to about August 2021 Syddall embezzled money through multiple means, including creating bogus purchase orders and invoices, stealing inventory and directing payments to fictitious companies and unauthorized vendors. Syddall then sold the inventory, none of which was authorized, on eBay and KSL Classifieds. When questioned by other employees about the discrepancies in orders and payments, Syddall sent lulling emails attempting to cover up and prolong the fraud.

In addition, Syddall concealed financial transactions by laundering proceeds from the wire fraud into third-party accounts. Syddall then directed the transfer of the money into accounts over which he had control. The government alleged the investigation has identified approximately $759,100 in restitution. (Source)

Biotech Company Employee Provides Husband With Insider Trading Information / Husband Made $90,000 In Illegal Profits - October 18, 2023

In the spring of 2019, Brian Rubin made $90,450 in illegal profits from the purchase and sale of stock options in the a biotech company that employed Rubin's spouse.

Rubin used material, non-public information obtained from her about the biotech company's successful development of certain products and its expected acquisition by the New York-based pharmaceutical company to purchase the options ahead of a public announcement of the acquisition in June 2019.

After the announcement, the biotech company's stock price increased and Rubin exercised the options for the profit, the charge alleges. Rubin's spouse had learned the information through her position as an account director for the biotech company's operations. (Source)

Supervisor At Food Services Company Charged With Accepting Hundreds Of Thousands Of Dollars In Kickbacks To Hire Temporary Employees - October 5, 2023

The indictment returned against Jason Bonnewell alleges that during his tenure as a supervisor at a Pennsylvania food services company from 2014 to 2019, he and his coconspirators accepted cash bribes and other things of value from other coconspirators who owned and operated Global Staffing Services, Inc. and Penns Independent Staffing.

Global Staffing Services, Inc. and Penns Independent Staffing were two companies that leased temporary employees to Bonnewell's company.

In exchange for the kickbacks, Bonnewell and his co-conspirators entered contracts with and hired the temporary employees of the two staffing companies. Allegedly, over $13,000,000 were paid to the two staffing companies, in exchange for hundreds of thousands of dollars in kickbacks. (Source)

Cincinnati City Council Member Sentenced To Prison For Accepting $40,000 In Bribes - October 10, 2023

Alexander Sittenfeld is a former Cincinnati City Council Member.

Sittenfeld accepted $20,000 in bribe payments to his political action committee (PAC) from undercover FBI agents posing as corrupt businessmen working with a real estate developer.

Sittenfeld knowingly received the $20,000 in bribe payments in return for guaranteeing votes for a development project. Sittenfeld told the undercover agents he could "deliver the votes."

Sittenfeld solicited the real estate developer to collect $10,000 in contributions to the former council member for Sittenfeld's support of the developer's efforts.

In total, Sittenfeld accepted eight $5,000 checks in 2018 and 2019 from the undercover FBI agents. The latter $20,000 was received from the undercover agents for help with their sports book.

Sittenfeld's received a total of $40,000, and also failed to list expensive gifts and dinners he received from the undercover agents. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

Former CEO Of Commercial Lending Business And 4 Co-Conspirators Plead Guilty To Running $250 Million Securities Fraud Scheme - October 13, 2023

Carl Ruderman is the former Chairman of 1 Global Capital LLC). He pled guilty to a $250 million securities fraud scheme. Four of Ruderman's co-conspirators have already pleaded guilty for their role in this fraud, including two lawyers who provided him with false legal cover to skirt federal securities laws.

Ruderman admitted that he and others made false and misleading representations to investors and potential investors as to the profitability of 1 Global's business in marketing materials and periodic account statements. According to plea documents, investors were falsely told that 1 Global had audited financials by a public accounting firm, that the investor's money would be spent on the MCAs, and that they could expect double-digit returns on their investments, among other things.

Ruderman admitted that he spent 1 Global's investor's money on credit card payments, vacation travel, insurance payments for his art collection and valuable jewelry, drivers, nannies, housekeepers, mortgage payments for his house, tuition, and payments for a luxury car. Ruderman also admitted that he diverted 1 Global investor money to businesses benefiting him and his family, without the investors' knowledge. (Source)

Former Senior Fiscal Officer For Non-Profit Organization Charged With Embezzling $2.3 Million+ Over 16 Years / Used Funds For Mortgage, Credit Card, Car Payments, Etc. - October 11, 2023

Marcia Joseph was the Senior Fiscal Officer of a 501(c)(3) non-profit organization (Company 1) located in Brooklyn, New York that provides comprehensive services to support employment opportunities for persons with emotional, developmental, and/or physical disabilities, and those who are economically disadvantaged.

Joseph set up a company called Prestige Business Services (Prestige), which purported to provide specialized services to other companies on behalf of Company 1. In truth, Prestige performed no work, and instead was used by Joseph for the exclusive purpose of embezzling more than $2.3 million from Company1 over a 16-year period.

Joseph used the money paid by Company 1 to Prestige to pay for numerous personal expenses, including approximately $235,000 in mortgage payments; 207,000 in credit card payments; $98,000 in car payments; $45,000 in Amazon expenses; and various other personal items, such as home remodeling, spa treatment, landscaping expenses, and luxury goods.

Joseph also withdrew nearly $100,000 in cash, disbursed approximately $16,000 to friends and family, and issued approximately $50,000 in Prestige checks to herself. (Source)

Employee Pleads Guilty To Embezzling $900,000+ From Employer Over 4 Years For Personal Use - October 5, 2023

From February 2007 through November 2016, Tamara Mannisto worked for a company that was in the business of mechanical food processing and farming. In her role at the company, Mannisto's duties included preparing checks for the owners to sign.

Beginning in at least January 2012, and continuing through October 2016, Mannisto carried out a fraudulent scheme to steal over $900,000 from her employer. As part of the scheme, Mannisto created company checks and made them payable to herself, without authorization and for amounts not due her.

To make the checks appear legitimate, Mannisto forged the owners' signatures on the checks or stamped them with one of the owners' signatures. Falsely posing as the checks' lawful payee, Mannisto deposited the checks in bank accounts she controlled. (Source)

Company Employee Charged With Using Corporate Credit Card For $525,000 Of Un-Authorized Charges Over 10 Years For Personal Use - October 27, 2023

Scott Richard was a Systems Engineer his company. His responsibilities included the specification, purchase, installation, and support of equipment and systems used by the company's technology infrastructure.

Richard is alleged to have used the corporate credit card issued to him for his own personal benefit. From January 1, 2012 through September 27, 2021, Richard fraudulently diverted $526,569.42 from his company to himself. (Source)

Former Church Employee Sentenced To Prison For Stealing $450,000 To Pay For Credit Card Payments, Utilities, Living Expenses - October 18, 2023

Beginning in early 2014 and continuing through at least January 2020, Darla Bralley devised a scheme to defraud and obtain money from St. Paul. Bralley was employed as payroll administrator for St. Paul during this period and had the authority to issue checks for authorized expenses on behalf of the church.

Bralley issued approximately 198 unauthorized checks, drawn from St. Paul's checking account, to pay for various personal items including personal credit card payments, utilities, and living expenses.

Bralley also made approximately 1,068 fraudulent, unauthorized transfers from the St. Paul checking account to pay her personal expenses. In all, Bralley defrauded St. Paul out of approximately $451,177.54. (Source)

Bookkeeper Sentenced To Prison For $213,000 Of Identity Theft By Forging Checks / Used Funds For Personal Use - October 20, 2023

Alexandria Fisk was hired to be a Bookkeeper for 3 businesses owned by the same person. On November 17, 2020, the business owner alerted authorities that checks had been issued without his consent to a company owned by Fisk.

Fisk pleaded guilty to using the identity of the victim, her former employer, to forge checks for her own personal use. The judge ordered Fisk to pay $213,581.12 in restitution to her employer. (Source)

Former Union President Pleads Guilty To Stealing $42,000+ Of Union Funds / Used Funds For Casino's, Personal Insurance, Etc. - October 6. 2023

Tamlyn Ulin-Gilson pleaded guilty to wire fraud for stealing from the American Federation of Government Employees (AFGE) Local Union 1273.

Ulin-Gilson served as President of Union 1273 from January 2019 to April 24, 2021. Union 273 is a federal labor organization that represents approximately 1,1000 medical support staff employed at the U.S. Department of Veteran Affairs Healthcare System in Boise and affiliated clinics. Prior to serving as president, Ulin-Gilson served as the vice president and secretary-treasurer for Union 1273.

With the resignation of the other executive board members, Ulin-Gilson had exclusive and unchecked control of Union 1273's bank account beginning in February 2020. She abused her authority by fraudulently misusing at least $42,674.45 of Union 1273's funds on unauthorized, personal expenses.

Ulin-Gilson spent at least $34,632.60 at casinos in Idaho and Nevada during this time, and also spent $7,037.35 on personal insurance premiums, and caused $1,004.50 in bank fees from the transactions. (Source)

Director Of Day Care Center Sentenced To Prison For Stealing $45,000 / Used Funds For Personal Expenses - October 27, 2023

Bridget Hansen was employed as the director of Our Redeemer Day Care in Jacksonville, Illinois,

Hansen devised a scheme to defraud the day care by transferring money from the business's bank accounts to her own bank accounts. Hansen would also write checks on the day care's bank accounts to herself or to cash and use the money for personal expenses. Hansen stole over $45,000, which caused the day care to cut back on the services it offered and contemplate closing the facility. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Health Care Executive Convicted Of $4 Million+ Fake Vendor Scheme Over 8 Years / Used Funds For Personal Use - October 23, 2023

Shawn Rains was an executive at OrthoNet, a healthcare claims processing company based in White Plains, New York.

Between approximately 2009 and 2017, Rains and Joseph Maharaj, another OrthoNet executive, designed and executed a scheme to defraud OrthoNet of over $4 million and to launder the fraud proceeds.

Rains conspired with Maharaj and others to create fake vendors that purported to do work on behalf of OrthoNet. Rains, Maharaj and their co-conspirators then signed invoices approving payment for the fake work, and OrthoNet sent payments to the fake vendors. Rains, Maharaj and their co-conspirators then converted the money to cash to hide the source of the fraud proceeds and split it up amongst themselves. (Source)

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Former Information Technology Manager Sentenced To Prison For Stealing / Selling $1.4 Million+ Of IT Equipment From Employer - October 17, 2023

Todd Erickson served as the Information Technology Manager at a telecommunications company. Erikson was responsible for submitting requests to purchase equipment, such as computers and hard drives.

From at least January 2012 through February 2019, Erickson fraudulently submitted purchase requests for computer equipment that the company did not need. Thereafter, without the knowledge or approval of his employer, Erickson sold the items to third parties. He was also ordered to pay restitution of $1,596,328. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Surgical Center Nurse Pleads Guilty To Tampering With Medication After Being Fired / Admitted To Drug Addiction - October 3, 2023

Katherine Rankin was a registered nurse and employed by a surgical center in Jacksonville, Florida.

On October 13, 2022, after discovering that Rankin had forged an anesthesia record, a supervisor confronted Rankin and told her that she was being fired. After being terminated, but while still in the building, Rankin was seen by another employee, and captured on a surveillance camera, removing some vials from a controlled substances cabinet.

While still at the surgical center, Rankin had a discussion with three other employees telling them that she had an addiction and that she had been taking drugs from the facility. She also said that the center's drug count was going to be off.

Rankin eventually turned over four vials of injectable hydromorphone, stating that the vials did not contain hydromorphone, but saline. Rankin explained that she had removed the hydromorphone, replaced it with saline, glued the caps back on, and then put vials back in the inventory so that surgical center's drug count would be correct.

Laboratory testing later showed that all four vials contained evidence of physical tampering (caps being removed and glued back on) and chemical tampering (each vial contained very diluted amounts of hydromorphone). (Source)

Hospital Nurse Pleads Guilty To Diverting Fentanyl At Hospital For His Own Use - October 11, 2023

In August 2022, before Luis Ramirez-Cajas began working at a Cajas and the Iowa Board of Nursing's Iowa Nurse Assistance Program (INAP) entered into an agreement under which Cajas promised to abstain from drugs and alcohol and to refrain from working with narcotics.

Cajas previously had admitted to diverting and using narcotics in the emergency room of an Iowa City hospital in late 2021 and early 2022. In September and October 2022, while working at the Waterloo hospital, Cajas diverted fentanyl, hydromorphone, and morphine to his own use. (Source)

OTHER FORMS OF INSIDER THREATS

Off-Duty Commercial Airline Pilot Sitting In Cockpit Charged For Attempting To Shut Down Engines - October 24, 2023

Joseph Emerson has been charged by criminal complaint with one count of interfering with flight crew members and attendants.

On October 22, 2023, Port of Portland police officers responded to a report of inbound aircraft that had diverted from its route between Everett, Washington, and San Francisco to Portland International Airport due to an inflight disturbance. Police dispatch reported that Emerson, an off-duty Alaska Airlines pilot seated in a cockpit jump seat, had attempted to shut down the plane's engines during flight.

After landing, responding officers interviewed the two pilots. The pilots recounted that, approximately halfway between Astoria, Oregon, and Portland, after engaging with them in casual conversation, Emerson attempted to grab and pull two red fire handles that would have activated the plane's emergency fire suppression system and cut off fuel to its engines. After a brief physical struggle with the pilots, Emerson exited the cockpit.

Flight attendants placed Emerson in wrist restraints and seated him in the rear of the aircraft. During the flight's descent, Emerson tried to grab the handle of an emergency exit. A flight attendant stopped him by placing her hands on top of his. (Source)

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

2 Former Bank Officers Sentenced To Prison For $1 BILLION Bank Fraud Scheme Causing Bank To Collapse / 500 Employees' Lost Jobs - October 2, 2023

William Burnell, Robert Calloway and Frank Adolph were sentenced to prison for their roles in a bank fraud conspiracy that led to the collapse and failure of First NBC Bank (Bank), in April 2017.

Burnell was the bank's Chief Credit Officer. Burnell conspired with the bank President, Ashton Ryan and others, to conceal material information and defraud the bank. Burnell fraudulently risk rated loans to past due borrowers so new loans could be issued to them to conceal the borrowers' past due status from the Board.

Calloway was the bank's Executive Vice President. Calloway and other bank officers, including Ryan and Burnell conspired to conceal the financial condition of a bank borrower, Gary Gibbs, from bank's Board of Directors, auditors, and examiners.

They falsely stated in loan documents that Gibbs was able to pay his loans with cash generated by his businesses. They concealed from the bank's Board of Directors, auditors, and examiners that Gibbs was only making his existing loan payments by getting new loans from the Bank. (Source)

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

U.S. Postal Service Employee Charged With Stabbing A Supervisor At Postal Facility - September 1, 2023

Edwin Cuadrado is a U.S. Postal Service (USPS) employee.

According to the criminal complaint, Cuadrado first engaged in a verbal and physical altercation with one of his USPS supervisors at a nearby gas station late in the afternoon on August 25. Shortly thereafter, Cuadrado drove his USPS vehicle into the main employee parking lot of the USPS mail processing and distribution facility. While in the parking lot of that facility, three different supervisory USPS employees attempted to speak with Cuadrado regarding the recent altercation. Cuadrado responded by brandishing a knife and stabbing one of the supervisors before leaving the scene. Responding paramedics treated the wound to the back of the supervisor's head before that supervisor was taken to a hospital for further treatment. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

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 Guility To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day. The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

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

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

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

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

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)

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)

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

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

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

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

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

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

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

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

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

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

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

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

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

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

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

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

Former Controller Of Oil & Gas Company Sentenced To Prison For $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)

WORKPLACE VIOLENCE

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)

Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022

Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

On or around June 21, 2022 a 55 year old female coworker of Ortiz, experienced a medical emergency and died immediately after treating herself for dehydration using an IV bag of saline taken from the surgical center. An autopsy report revealed that she died from a lethal dose of bupivacaine, a nerve blocking agent.

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU. Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupicavaine, and lidocaine.

Surgical center personnel concluded that the incidents listed above suggested a pattern of intentional adulteration of IV bags used at the surgical center. They identified about 10 additional unexpected cardiac emergencies that occurred during otherwise unremarkable surgeries between May and August 2022 .

The complaint alleges that none of the cardiac incidents occurred during Dr. Ortiz's surgeries, and that they began just two days after Dr. Oritz was notified of a disciplinary inquiry stemming from an incident during which he allegedly "deviated from the standard of care" during an anesthesia procedure when a patient experienced a medical emergency. The complaint alleges that all of the incidents occurred around the time Dr. Ortiz performed services at the facility, and no incidents occurred while Dr. Ortiz was on vacation.

The complaint further alleges that Dr. Ortiz had a history of disciplinary actions against him, and he had expressed his concern to other physicians over disciplinary action at the facility, and complained the center was trying to "crucify" him.

A nurse who worked on one of Dr. Ortiz's surgeries told law enforcement that Dr. Ortiz refused to use an IV bag she retrieved from the warmer, physically waving the bag off. A surveillance video from the center's operating room hallway showed Dr. Ortiz placing IV bags into the stainless-steel bag warmer shortly before other doctors' patients experienced cardiac emergencies.

The complaint alleges that in one instance captured in the surveillance video, Dr. Ortiz was observed walking quickly from an operating room to the bag warmer, placing a single IV bag inside, visually scanning the empty hallway, and quickly walking away. Just over an hour later, according to the complaint, a 56-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. The complaint alleges that in another instance, agents observed Dr. Ortiz exit his operating room carrying an IV bag concealed in what appeared to be a paper folder, swap the bag with another bag from the warmer, and walk away. Roughly half an hour later, a 54-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours.

Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

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

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

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

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

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

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

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

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

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house. Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check. Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

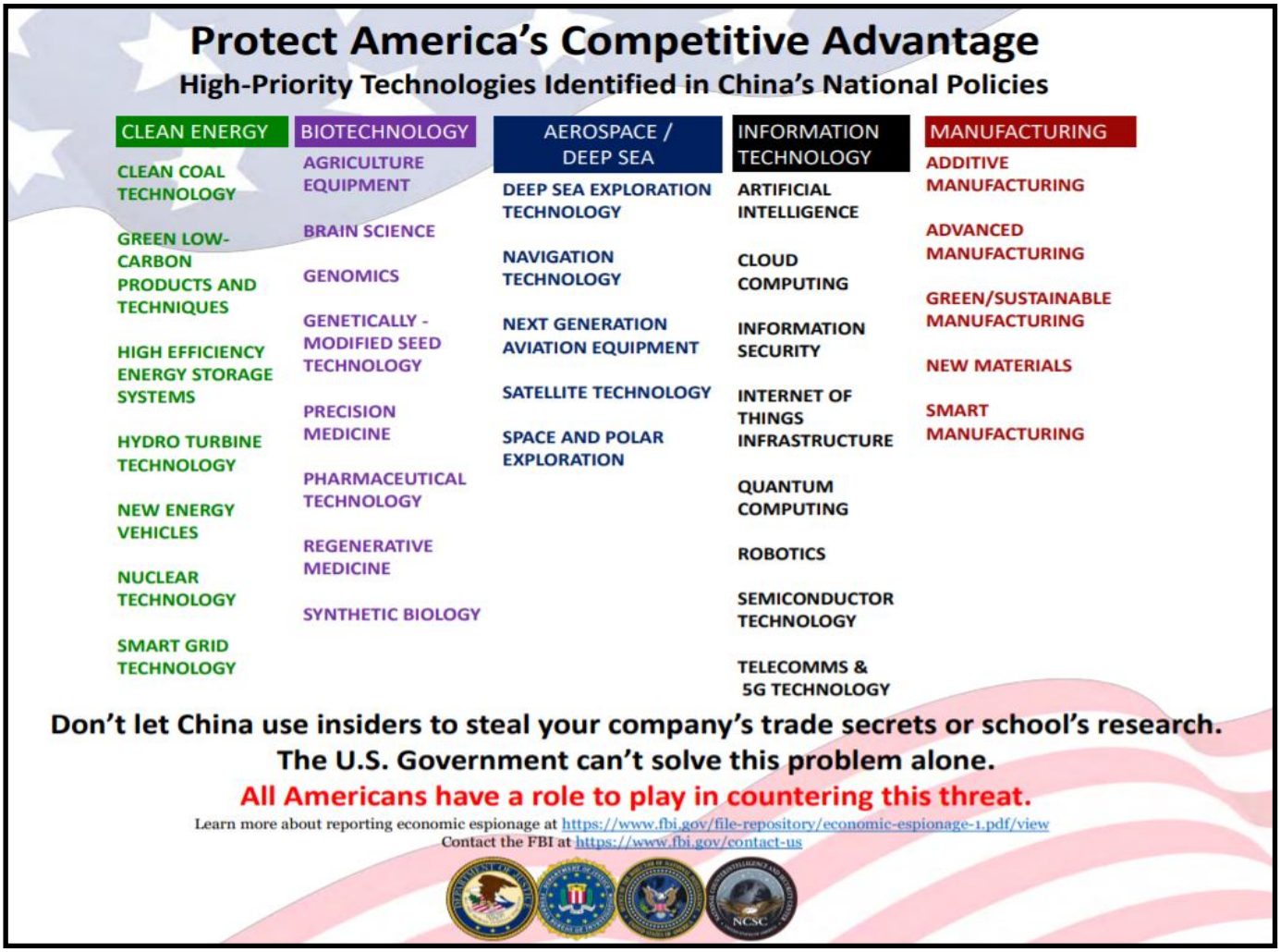
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,900+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

https://www.insiderthreatdefense.us/category/insider-threat-incidents/

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.
https://www.insiderthreatdefense.us/news/

INSIDER THREAT INCIDENTS COSTING $1 MILLION TO $1 BILLION +

https://www.linkedin.com/post/edit/6696456113925230592/

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

The NITSIG has created a LinkedIn Group for individuals that interested in sharing and gaining in-depth knowledge regarding ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in ITM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E in 2020 to 2022 due to the COVID outbreak. We are working on resuming meetings in the later part of 2023, and looking at holding the ITS&E in 2024.

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

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the: White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines,) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **900+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over **10+** years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

Our training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefensegroup.com / jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org