INSIDER THREAT INCIDENTS REPORT

FOR

September 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

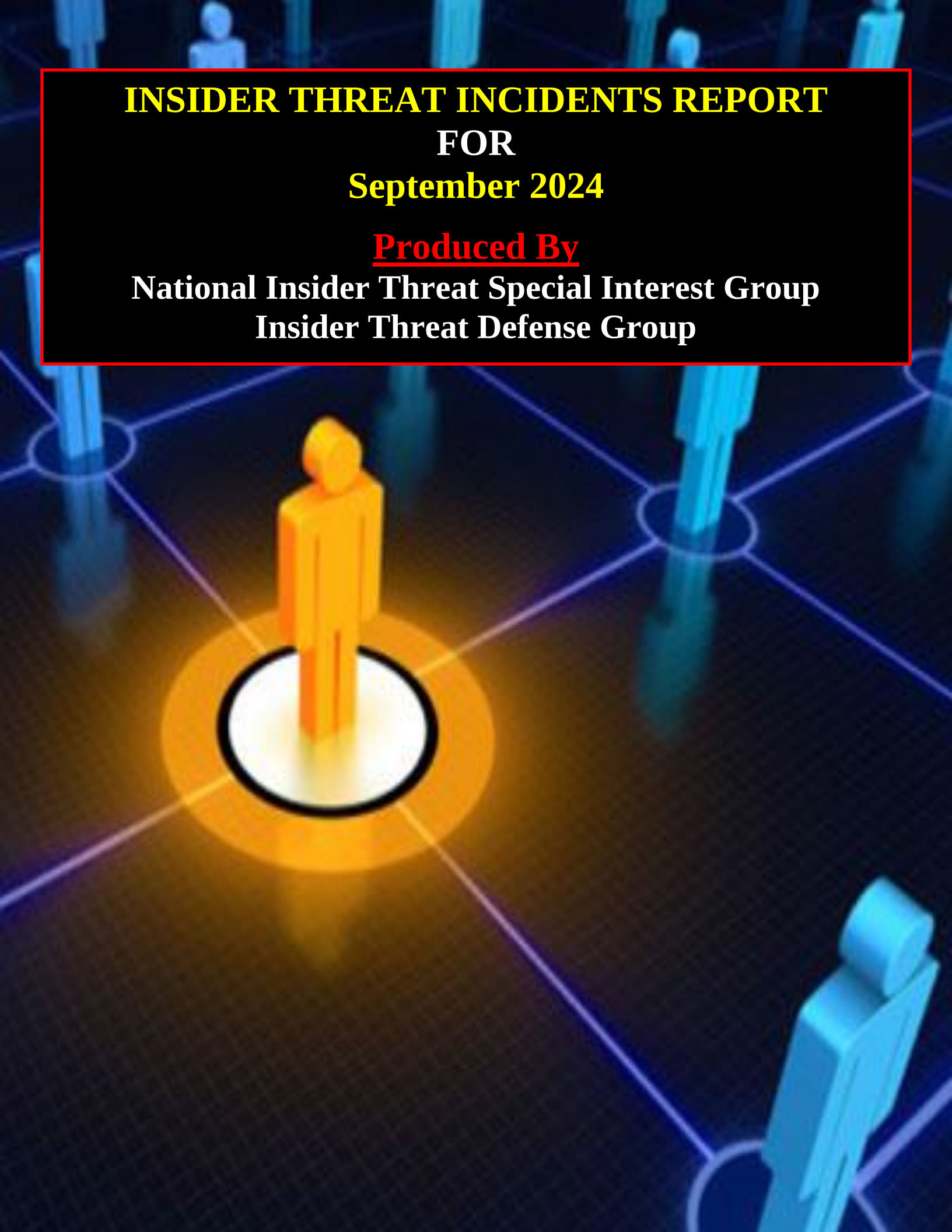


TABLE OF CONTENTS

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 15+ years. This research has evaluated and analyzed over **5,700+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

According to the Association of Certified Fraud Examiners 2024 Report To the Nations, the 1,921 fraud cases analyzed, caused losses of more than **$3.1 BILLION.**

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

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

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

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

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

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 23** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR SEPTEMBER 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

Former FAA Contractor Charged For Illegally Acting As An Agent Of The Iranian Government - September 27, 2024

From at least December 2017 through June 2024, Abouzar Rahmati conspired with Iranian government officials and intelligence operatives to act on their behalf in the United States, including by meeting with Iranian intelligence officers in Iran, communicating with coconspirators using a cover story to hide his conduct, obtaining employment with an FAA contractor with access to sensitive non-public information, and obtaining open-source and non-public materials about the U.S. solar energy industry and providing it to Iranian intelligence.

From June 2009 to May 2010, Rahmati served as a First Lieutenant in the Islamic Revolutionary Guard Corps (IRGC), an Iranian military and counterintelligence organization under the authority of the Supreme Leader of Iran. After being discharged from the IRGC, Rahmati lied to the United States government regarding his military service with the IRGC in order to, among other things, gain employment as a U.S. government contractor. (Source)

U.S Postal Service Worker Accused Of Stealing $1.5 Million+ Checks From Mail

Anthony Virdure worked at the Postal Service Processing and Distribution Center at 1720 Market Street in St. Louis, Missouri. He had access to all first-class mail routed through the center.

The indictment accuses Virdure of stealing checks with a face value of more than $1.5 million from the mail. (Source)

United States Geological Survey Employee Charged With Making $1.2 Million+ Of Un-Authorized Purchases For Personal Use - September 4, 2024

James Montoya worked as a federal employee at the United States Geological Survey (USGS) office in Lakewood, Colorado. USGS is part of the United States Department of the Interior (DOI).

During a routine initiative to identify misuse, DOI identified numerous questionable transactions on Montoya's government charge card. The indictment alleges that Montoya concealed these improper purchases by altering documents to indicate these purchases were for work-related items. The alleged actions defrauded the government of approximately $1,223,009.42 over approximately fifteen years beginning around December of 2008 and continuing through at least November 2023. (Source)

Small Business Administration Employee Convicted For Accepting $800,000+ In Bribes To Process Loan Applications - September 25, 2024

Angela Chew conspired with three others to submit applications for COVID-19 Economic Injury Disaster Loans (EIDLs) containing false and fraudulent information in exchange for bribe payments.

Chew used her position as a loan specialist for the Small Business Administration (SBA) to internally access those loan applications that she and a co-conspirator had submitted on behalf of others. Chew then took actions on the applications within the SBA's internal processing system that moved the loans towards approval. For example, Chew submitted a loan on behalf of a co-conspirator's business that she knew was not active or operating at the time she submitted the loan. The loan was flagged as a duplicate by the SBA's internal system, which stopped the application from progressing toward approval and funding. Chew then entered the SBA's loan processing system, accessed the loan application, reactivated it, and manipulated the loan's status multiple times in order to progress the application toward approval and funding in the amount of $150,000. In exchange, Chew received thousands of dollars in bribe payments from two of her co-conspirators. The evidence showed that Chew caused the funding of at least six EIDL applications, for a total loss of over $800,000. (Source)

IRS Information Technology Supervisor Pleads Guilty To Accepting $120,000+ In Bribes From Government Subcontractor Whom He Attempted to Extort - September 11, 2024

Satbir Thukral worked for the IRS as a computer engineer and supervised various information technology contracts.

In September 2018, Company 1 began working on a subcontract for the IRS that Thukral supervised. Starting in October 2018, Thukral sought cash payments from Company 1's owner, Individual 1, constituting a portion of the earnings from Company 1's work on the IRS subcontract. Between 2018 and 2020, Individual 1 made multiple cash payments to Thukral totaling more than $120,000. In February 2021, when Individual 1 told Thukral that Individual 1 would not pay any more money, Thukral attempted to extort Individual 1 by threatening that Individual 1 would suffer economic consequences if the payments did not continue. In early February 2023, Individual 1 recorded an in-person meeting with Thukral at the direction of law enforcement.

During the meeting, Individual 1 told Thukral that the FBI had asked about bank withdrawals that Individual 1 had made to pay Thukral, and Thukral instructed Individual 1 to lie to the FBI about the nature of the cash withdrawals. Later that same day, to assist and induce Individual 1 to lie to the FBI and to further the concealment of the payments, Thukral returned a portion of the proceeds that Thukral had received from Individual 1.

In a separate scheme, in July 2022, Thukral received approximately $2,800 in cash from a manager at a prime contractor with the IRS. The manager made the payment, in part, in return for Thukral's facilitating the continued employment of two underqualified individuals at two other IRS subcontractors with whom the manager had an affiliation. In addition, at the time of the payment, the manager believed that Thukral, who had been selected to serve on a three-person panel that would have evaluated the technical feasibility of bids of an upcoming IRS contract valued at approximately $200 million, could influence the valuations to the manager's benefit. (Source)

Social Security Administration Employee Sentenced To Prison For $49,000+ Fraudulent Telework Scheme While Working Another Job - September 26, 2024

Christopher Markham was employed by the Social Security Administration and assigned to an office in Anderson, Indiana.

Between February 13, 2019, and June 17, 2022, Markham engaged in a scheme by which he made it appear as though he was teleworking full-time for Social Security Administration (SSA) during workdays, when in reality he was earning income working as a home inspector for his personal business. Markham was paid his full federal salary and benefits, while concealing the fact that he was working for his personal business and not for SSA.

Markham routinely performed home inspections for his personal business during the workweek while purporting to "telework" on official SSA time. He concealed the fact that he was not performing SSA work during official work hours by having his wife and his mother access the SSA computer system and send emails to supervisors to make it appear as though he was online and working.

Markham nevertheless sought to be paid in full during this period and submitted 53 fraudulent time reports to SSA's online timekeeping portal, as well as falsified daily work logs to his supervisors.

Additionally, Markham engaged in other fraud schemes to obtain Emergency Paid Leave by falsely claiming he was required to stay home to take care of his children.

In fact, his children were in daycare, and he was again performing work for and earning income from his personal business. He allegedly performed at least 70 home inspections for his personal business while claiming to be providing emergency care for his children.

Finally, on multiple occasions, Markham fraudulently claimed benefits under the Family and Medical Leave Act "FMLA) by falsely claiming he was unable to work due to illness—when he was actually doing home inspections for his personal business. Markham even attended an F.C. Tucker retreat promoting his business while claiming he was on FMLA leave.

On June 4 and 5, 2020, Markham was granted administrative leave after claiming that the internet wire to his home had been cut. Markham advised that his internet provider would not be able to send anyone to his home to repair the wire until Friday, June 5, 2020. In reality, his internet provider had no record of a damaged wire, and Markham used the administrative leave to take an unapproved, paid vacation to Gatlinburg, Tennessee.

In total, Markham's fraudulent conduct caused a loss to the SSA of approximately $49,255, which he has been court ordered to repay. Markham's failure to perform his duties caused needy members of the public to have their social security benefits delayed, including people with autism, blindness, and end stage cancer. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

CIA Officer Sentenced To Prison For Providing People's Republic Of China Classified Information - September 11, 2024

Alexander Ma of Honolulu, a former Central Intelligence Agency (CIA) officer, was sentenced to conspiring to gather and deliver national defense information to the People's Republic of China (PRC).

Ma was arrested in August 2020, after admitting to an undercover FBI employee that he had facilitated the provision of classified information to intelligence officers employed by the PRC's Shanghai State Security Bureau (SSSB).

Ma worked for the CIA from 1982 until 1989. His blood relative (Co-Conspirator CC #1), who is deceased, also worked for the CIA from 1967 until 1983. As CIA officers, both men held Top Secret security clearances that granted them access to sensitive and classified CIA information, and both signed nondisclosure agreements.

As Ma admitted in the plea agreement, in March 2001, over a decade after he resigned from the CIA, Ma was contacted by SSSB intelligence officers, who asked Ma to arrange a meeting between CC #1 and the SSSB. Ma convinced CC #1 to agree, and both Ma and CC #1 met with SSSB intelligence officers in a Hong Kong hotel room for three days. During the meetings, CC #1 provided the SSSB with a large volume of classified U.S. national defense information in return for $50,000 in cash. Ma and CC #1 also agreed to continue to assist the SSSB.

In March 2003, while living in Hawaii, Ma applied for a job as a contract linguist in the FBI's Honolulu Field Office. The FBI, aware of Ma's ties to PRC intelligence, hired Ma as part of a ruse to monitor and investigate his activities and contacts with the SSSB. Ma worked part time at an offsite location for the FBI from August 2004 until October 2012.

As detailed in the plea agreement, in February 2006, Ma was tasked by the SSSB with asking CC #1 to identify four individuals of interest to the SSSB from photographs. Ma convinced CC #1 to provide the identities of at least two of the individuals, whose identities were and remain classified U.S. national defense information.

Ma confessed that he knowingly and willfully conspired with CC #1 and SSSB intelligence officers to communicate and transmit information that he knew would be used to injure the United States or to advantage the PRC. (Source)

U.S. Army Recruiter Charged With $266,000 Bank Fraud And Identity Theft Scheme Using Army Recruits PII - September 11, 2024

Jane Crosby was a Sergeant First Class in the U.S. Army and U.S. Army recruiter. She has been charged for engaging in a fraudulent scheme to defraud a credit union by using her position to obtain the personally identifying information of U.S. Army recruits and recruit candidates and submit fraudulent bank account applications to the credit union on the recruits'.

From Sept. 12, 2023, to Dec. 27, 2023, Crosby submitted "Pre-Active Duty Membership" bank account applications to a credit union on behalf of seven U.S. Army recruits or purported recruits, without their knowledge or consent. Such accounts are intended to facilitate the direct deposit of soon-to-be service members' salaries once they join the military. These applications included the victims' names and Social Security numbers as well as copies of their passports, driver's licenses, and/or Social Security cards.

Once these credit union accounts were opened, Crosby, posing as the victims, applied for approximately $266,000 in loans and credit card accounts and used some of the accounts to deposit fraudulent checks and then withdraw funds. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 High Ranking New York Fire Department Officials Charged With Accepting $190,000 In Bribes For Fast Tracking Inspections - September 16, 2024

Anthony Saccavino and Brian Cordasco a 2 two former chiefs of the New York City Fire Department (FDNY) Bureau of Fire Prevention (BFP). They have been charged with bribery, corruption, and false statements offenses.

Saccavino and Cordasco were Fire Chiefs of the BFP, which is responsible for overseeing and approving the installation of fire safety and suppression systems in commercial and residential buildings in New York City

Saccavino and Cordasco repeatedly abused their positions of trust as high-ranking officials in the FDNY from at least in or about 2021 through in or about 2023 by soliciting and accepting tens of thousands of dollars in bribe payments in exchange for providing preferential treatment to certain individuals and companies with matters pending before the BFP.

Saccavino and Cordasco received more than $190,000 in payments in connection with this scheme. (Source)

Former Airport Customs Officer Sentenced To Prison For Stealing $18,000+ In Cash From Airline Passengers - September 26, 2024

Between mid-2023 and early-2024, while working asa U.S. Customs and Border Protection (CBP) Officer at the Naples Airport in Florida, William Timothy stole approximately $18,700 in cash from airline passengers during 17 incidents of theft uncovered by CBP's Office of Professional Responsibility investigators.

Evidence collected during the investigation showed that Timothy was surreptitiously stealing cash from arriving international passengers during border enforcement examinations and currency verifications performed as part of his official duties as an assigned CBP Officer at Naples Airport. (Source)

Drug Cartel Bribed 2 U.S. Customs & Border Protection (CBP) Agents To Let Drugs Into U.S. - September 6, 2024

2 CBP officers have been accused of working for a Mexican drug trafficking organization to allow vehicles loaded with fentanyl, heroin, cocaine, and methamphetamine to pass unchecked through their inspection lanes in southern California.

Prosecutors allege Jesse Garcia and Diego Bonillo "profited handsomely," earning tens of thousands of dollars for each drug-laden vehicle they ushered into the U.S. without scrutiny.

The indictment alleges that Garcia and Bonillo combined allowed more than 1,150 pounds of drugs into the U.S. on five occasions between April 2021 and February 2024. That total only accounts for the drugs that authorities later seized.

Their arrests came exactly a month before their former colleague, Leonard George, went on trial in a similar case. A federal jury convicted George in June of accepting hundreds of thousands of dollars in bribes in exchange for allowing smugglers to bring drugs and illegal immigrants through his inspection lane at the San Ysidro Port of Entry, just across the border from Tijuana. (Source)

Prison Employee Pleads Guilty To Accepting $53,000+ In Bribes Payment To Smuggle Contraband Into Prison - September 12, 2024

William Homan was a former facilities repair worker at Waupun Correctional Institution (WCI), in Wisconsin. He received approximately 125 bribe payments totaling approximately $53,579 from July 17, 2022, to September 30, 2023, from inmates, former inmates, and their associates in exchange for smuggling contraband into WCI. (Source)

California Firefighter Arrested For Starting 5 Fires While Off Duty - September 21, 2024

A 38 year old California firefighter was arrested, accused of igniting 5 fires in the North Bay in recent weeks when he was off duty.

"I'm still processing this but he doesn't live here, nor has he," said the suspect's estranged wife.

The estranged wife of the firefighter wants to stay anonymous, but says she's speechless about her husband's arrest for suspicion of felony arson. ABC7 News is not identifying the firefighter until he's been officially charged. "I don't think anyone will have any idea that this had been happening, I'm 100 percent in shock," she said.

The department suspects the firefighter of causing five brush fires in Sonoma County this summer while he was off duty, including, the Alexander Fire on Aug. 15, the Windsor River Road Fire on Sept. 8, the Geysers Fire on Sept. 12 and the Geyser and Kinley Fires on Sept. 14. All five brush fires burned less than an acre of wildland due to the quick action of residents and firefighters.

California Fire's Director, Chief Joe Tyler said in a statement, "I am appalled to learn one of our employees would violate the public's trust and attempt to tarnish the tireless work of the 12,000 women and men of Cal Fire." (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former High-Ranking New York State Government Employee Charged With Acting As An Undisclosed Agent For The People's Republic of China / Chinese Communist Party - September 3, 2024

While working for the New York State government, including in high-ranking posts in the Executive Chamber of the New York State government and in multiple state agencies, Linda Sun also acted as an undisclosed agent of the People's Republic of China (PRC) and the Chinese Communist Party (CCP).

Sun's husband and co-defendant Chris Hu was also charged with money laundering conspiracy, as well as conspiracy to commit bank fraud and misuse of means of identification.

Acting at the request of PRC government officials and the CCP representatives, Sun engaged in numerous political activities in the interests of the PRC and the CCP, including blocking representatives of the Taiwanese government from having access to high-level New York State officers; changing high-level New York State officers' messaging regarding issues of importance to the PRC and the CCP; obtaining official New York State proclamations for PRC government representatives without proper authorization; attempting to facilitate a trip to the PRC by a high-level New York State politician; and arranging meetings for visiting delegations from the PRC government with New York State government officials.

Sun also repeatedly violated internal rules and protocols within the New York State government to provide improper benefits to PRC and the CCP representatives, including by providing unauthorized invitation letters from the office of high-level New York State officers that were used to facilitate travel by PRC government

officials into the United States for meetings with New York State government officials. Sun's unauthorized invitation letters for the PRC government delegation constituted false statements made in connection with immigration documents and induced the foreign citizens into unlawfully entering the United States.

Sun never registered as a foreign agent with the Attorney General, and in fact actively concealed that she took actions at the order, request, or direction of PRC government and the CCP representatives.

In return for these and other actions, Sun received substantial economic and other benefits from representatives of the PRC government and the CCP, including the facilitation of millions of dollars in transactions for the PRC-based business activities of Hu; travel benefits; tickets to events; promotion of a close family friend's business; employment for Sun's cousin in the PRC; and Nanjing-style salted ducks prepared by a PRC government official's personal chef that were delivered to the residence of Sun's parents. Sun and Hu laundered the monetary proceeds of this scheme to purchase, among other items, real estate property in Manhasset, New York currently valued at $4.1 million, a condominium in Honolulu, Hawaii currently valued at $2.1 million, and various luxury automobiles, including a 2024 Ferrari. Sun never disclosed any benefits she received from representatives of the PRC government and the CCP to the New York State government, as she was required to do as a New York State government employee.

Hu also laundered unlawful proceeds through bank accounts opened in the name of a close relative but that were actually for Hu's exclusive use. To open these accounts, Hu unlawfully used an image of the relative's driver's license. (Source)

County Department Of Public Works Supervisor Charged For $400,000+ Of Fraudulent Credit Card Charges By Creating Fake Company - September 9, 2024

William Richards was hired at the Glynn County Department of Public Works in 2010, progressing to a supervisory role that provided him with access to employee purchasing cards and the county's billing system.

In September 2023, the Glynn County Police Department and the FBI initiated an investigation after another Public Works employee noticed suspicious charges on his county purchasing card.

Investigators determined that Richards, who was responsible for coding and reconciling purchases made with the department's purchasing cards, had for more than two years made fraudulent purchases with his own county-issued card and with those of other employees, issuing payments to a fictitious company that he created and then transferring the funds to his own bank account.

Richards was ordered to pay $422,168 in restitution to the Glynn County government. (Source)

City Employee Sentenced For Embezzling $350,000+ / Used Funds For Gambling At Casino - September 18, 2024

Kelly Whitmore-Behling and her co-defendant were employed by the City of Milwaukee's Department of Public Works, where their responsibilities included disposing of vehicles and equipment the City no longer needed.

Between June and September of 2022, they executed an embezzlement scheme, selling City vehicles and equipment for cash and pocketing most of the proceeds for themselves.

The City lost over $350,000 in revenue and was forced to incur additional expenses to replace needed vehicles and equipment that had gone missing.

During the same time period, Whitmore-Behling gambled extensively at a local casino. The scheme ended when the co-defendants were suspended from work and the Department of Public Works conducted a thorough equipment audit that revealed the scope of their fraud. (Source)

State Department Of Human Services Supervisor & Daughter Charged For Obtaining $191,000 In A Fraudulent Manner - September 10, 2024

Nadine Baptiste repeatedly conducted telephonic balance inquiries on EBT benefit cards, frequently changing the PIN numbers associated with those cards. It is alleged that some of the individuals whose information was repeatedly accessed were either juveniles or individuals who were, at the time, homeless or incarcerated. It is further alleged that SNAP EBT benefit cards with a value of approximately $191,000 were improperly accessed.

The investigation into this matter was launched in September 2023, when the Rhode Island Office of Internal Audit received complaints from SNAP recipients via the Internal Audit Fraud Hotline alleging that they did not receive EBT benefit cards issued to them, which are commonly mailed to the address of the recipient or obtained in-person from a DHS office in the case of a homeless recipient. (Source)

City Mayor In Michigan Pleads Guilty To Accepting $100,000 In Bribes - September 25, 2024

Patrick Wimberly served as the Mayor of the City of Inkster, Michigan, from 2019 through 2023.

In the spring of 2022, Wimberly demanded $100,000 in cash payments to facilitate the sale of property owned by the City to an outside party (Person). Over several months, Person A provided Wimberly with monthly cash bribes to secure the purchase of this property.

The monthly payments started at $5,000 but the parties agreed to eventually increase that amount. After the initial bribes, Wimberly explained that he was ready to increase the payments. Person A agreed. But when Person A later did not provide the amount Wimberly expected, Wimberly complained that he was due "10$ a month." Person A then increased the monthly payments to $10,000. In total, Person A provided $50,000 in cash to Wimberly for the purpose of winning the bid for subject property. The Federal Bureau of Investigation intervened before the property could be transferred to Person A. (Source)

City Manager Charged With Accepting $2,0000 In Kickbacks From Vendor For City Business - September 12, 2024

From June to September 2019, Victor De La Cruz, a City Manager in Edcouch, Texas, solicited bribe payments from the owner of a Brownsville business that provides marketing services throughout the Rio Grande Valley. The business owner allegedly received two separate $3000 payments for marketing work he was allegedly performing for the city of Edcouch. In return, he made two $1000 kickback payments to Flores. (Source)

District Of Columbia Public School Employee & Government Contractor Charged In 5 Year Bribery Scheme - September 6, 2024

A federal grand jury yesterday returned an indictment charging Dana Garnett who is a former District of Columbia Public Schools (DCPS) employee, with conspiracy to commit bribery and wire fraud. The indictment also charges Yelake Meseretu, the owner of U.S. Office Solutions, a vendor of goods to DCPS, with bribery and wire fraud in exchange for Garnett steering business to Meseretu's business, and for accepting significantly fewer supplies than ordered in exchange for the bribe payments.

Over the course of at least five years, Garnett accepted payments from several vendors who supplied goods to DCPS. In exchange, Garnett steered business to the vendors. Some of the payments were generated from falsified orders awarded to the vendors that were paid in full by DCPS.

However, Garnett and co-conspirator Patricia Bailey, another former DCPS employee had coordinated with the vendors to deliver a lesser amount of goods than were listed on the orders. Based on false certifications made by or at the direction of Garnett, DCPS paid the full amount of the orders as if the orders had been fulfilled in full. The vendors paid cash to Garnett and Bailey in various locations in the D.C. and Maryland area. (Source)

Ohio City Prosecutor Charged With Bribery For Accepting Auto Repair Work For His Vehicle From Criminal Defendant - September 24, 2024

Nicholas Graham was a prosecutor who represented the City of Warren in Warren Municipal Court in Ohio.

Brian Votino had two criminal cases pending in the same court. The indictment alleges that in October 2019, Graham and Votino agreed that Graham would take action to benefit Votino with respect to Votino's criminal cases in return for Votino performing repairs to Graham's truck. To cover up the bribery arrangement, Graham instructed Votino through an intermediary to falsify a bill for the repair services and not to tell Votino's criminal defense lawyer. Graham and Votino ultimately carried out their agreement.

In exchange for the repair work by Votino, Graham took official action to reduce the charges against Votino and advocated for a lenient sentence. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Teacher Arrested For Making Online Threats To Kill School Officials And Students - September 4, 2024

Daniel Johnson made online threats over social media, including threats to kill named victims and commit other acts of violence using firearms and explosives. Additionally, law enforcement officers conducted a search of Johnson's home last week and discovered what are alleged to be components of explosive devices or materials used for the manufacturing of explosives. (Source)

School Employee Who Handled Payroll Sentenced To Prison For Stealing $766,000+ - September 4, 2024

Between January 11, 2016, and April 10, 2023, Janes Liles devised a scheme to defraud Silver River Mentoring and Instruction (SRMI), an alternative school for middle and high school students, in Florida.

During this time, Liles handled the school's payroll and had 137 unauthorized paychecks issued in her name by logging false information into SRMI's accounting software. Liles then received the fraudulent paychecks through wire transfers directly into her bank account.

During a financial review with the school's executive staff in April 2023, Liles admitted that she had been "paying [herself] extra money" and had become addicted to stealing the payroll funds.

In total, Liles's actions cost the school $766,553.54, a figure representing the fraudulent pay she received ($616,793.43) plus the associated benefits and taxes. (Source)

New York Department Of Education Employees Took Trips To Disney World Meant For Homeless Kids - September 17, 2024

New York City Department of Education workers snatched up city-paid trips to Disney World and other amusement locations, that were intended for homeless students.

The city's Special Commissioner of Investigation is accusing the workers of grabbing the trips for their own children.

One Queens borough supervisor for "Students In Temporary Housing" not only took her own children on the city-paid trips, but encouraged her co-workers to do the same thing. Linda Wilson allegedly tried to cover up the practice when investigators began asking questions about the trips.

“What happens here stays with us," Wilson allegedly told her co-workers of the practice. Wilson even went so far as to directly encourage her co-workers to lie about their use of the trips for their own children. “She said everyone should stick to the same story that we did not take our children on the trip. She told us to lie to the investigators.”

One educator was even forced to beg to secure spots on a Disney World trips for two of his students who were actually eligible for the program. City staffers even went so far as to forge documents using the names of homeless students who didn't actually go on the trips, to secure permission slips for their own children.

The program itself was funded by a $300,000 grant provided to New York City from the National Center for Homeless Education. The grant funded trips to Washington, D.C, New Orleans, Boston, Rocking Horse Ranch Resort, and the Frost Valley YMCA campground. The Disney World trip, which included roughly 50 adults and kids, clocked in at a whopping $66,000 in costs for the city.

The Department of Education confirmed that the staffers identified in the investigators' report have been separated from the Department. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Partner Of Investment Management Firm Sentenced To Prison Stealing $2.4 Million+ From Clients - September 23, 2024

From at least in or about March 2022 through at least in or about December 2022, Joshua Henner ran two schemes that defrauded victims out of at least $2.4 million. In the first scheme, Henner solicited and obtained funds from victims based on representations that he had been an angel investor in a start-up and that he needed funds to purchase additional shares in the company to maintain his investment position.

To induce victims to give him funds, Henner routinely made materially false oral and written statements, including lies about his previous investment in the company and his ownership interest in the company. Without their knowledge or authorization, Henner misappropriated his victims’ funds by, among other things, transferring the funds to himself and other individuals.

Henner also used, without authorization, the name and email address of a lawyer purportedly involved in the investments to communicate via email with his victims and foster the illusion that he was using the funds that his victims lent him for their intended purposes.

In a second scheme, Henner also induced at least six victims to lend him money to renovate an apartment that he did not own. To carry out this fraud, Henner, among other things, informed victims that he had contracted with a renovations company and created a fraudulent email address with the real name of an employee of the renovation company. In truth and in fact, Henner rented and did not own the apartment, Henner was prohibited from renovating the apartment, and Henner did not use the funds that his victims gave him to renovate the apartment. (Source)

Bank Vice President Sentenced To Prison For Stealing $1.5 Million+ From Bank Over 22 Years - September 12, 2024

Stacia Wilson admitted that while she was employed as a Vice President of St. Clair County State Bank in Osceola, Missouri, that she defrauded the bank by creating false and fictitious loans utilizing the stolen identity information of bank customers. She deposited the loan proceeds into her personal bank accounts to use for her own benefit.

Wilson's fraud scheme, which lasted more than 20 years from 2000 until it was discovered in December 2022, resulted in numerous fraudulent loans and a $1,528,321 loss to the bank. (Source)

Credit Union Finance Officer Sentenced To Prison For Stealing $1.2 Million+ / Used Funds To Pay For Boat, Personal Expenses, Etc. - September 13. 2024

Teresa Paulo was the Southern Pine Credit Union's (SPCU) financial controller from Oct. 2011 to June 2020.

Leah Lehman served as President of SPCU from 1990 to 2020. The Credit Union's members are employees of the local paper mill and their families.

Lehman began her fraud in June 2003, when she created a share secured loan in a SPCU account using the name and social security number of a member without that individual's knowledge. From Feb. 2012 to May 31, 2020, Lehman paid off the loan and rebooked it multiple times with additional advances. She would take the proceeds and put them in a joint share draft account she had with the individual, using the proceeds to pay for a boat, a hunting club share, personal expenses and gifts to family members. This loan was repaid in full.

However, Lehman created another share secured loan in another individual's name without their knowledge and would also pay off the loan and rebook it multiple times for personal spending. To conceal these activities, Lehman created false credit transactions using the names and passwords of SPCU employees. These transactions would advance the due date on the loans, which prevented these loans from appearing on quarterly call reports to the NCUA and allowed Lehman to defer or not make payment on these loans. Following these transactions, Lehman created debit entries to put the loans back on the accounts, which would often include interest accrued on the outstanding loans. She made additional fraudulent loan advances simultaneously with those entries to advance the loan dates.

She reflected the loans as being paid off at the end of the quarter to prevent possible detection of artificial growth in the SPCU loan portfolio. In total, the drafts needed to pay off the loan balances at each quarter grew to $4,112,870.63, excluding payments and interest, as of May 31, 2020.

Lehman was ordered to pay $4,491,253.97 in restitution to Southern Pine Credit Union. Paulo was ordered to pay $1,238,638.29 in restitution to Southern Pine Credit Union. (Source)

Morgan Stanley Wealth Manager Charged With Theft Of $500,000+ Client Funds / Used Funds For Personal Benefit - September 26, 2024

Jason Head was a registered stockbroker who worked for Morgan Stanley Wealth Management throughout the relevant period.

Beginning in July 2020 and continuing through November 2023, Head withdrew approximately $500,114.81 from the accounts of two of his Morgan Stanley clients without their authorization. Head transferred the funds to accounts he controlled and used for his personal benefit. (Source)

Credit Union Employee Pleads Guilty To $406,000+ Fraud Scheme / Sold Customer Login Information - September 10, 2024

Brianna Johnson was previously employed by Alabama Credit Union as a Member Care Agent. In this role, Johnson was able to access credit union member account information including, among other things, the names and personal identifying information of accountholders and their account balances.

From August 2022 to January 2023, Johnson abused this access, misappropriating customer account information and then providing that account information to the administrator of a Telegram channel called "The Lucky Shop."

The administrator of "The Lucky Shop" channel sold the information that Johnson provided, including bank logins and digital checks, to customers of his channel. The administrator also worked with others to withdraw funds from certain accounts.

This part of the scheme, which the conspirators called "Operation ACU," included depositing fraudulent checks, submitting fraudulent loan applications, and initiating fraudulent Automated Clearing House transfers. It also included using stolen passcodes to withdraw funds from Automated Teller Machines.

Johnson has agreed to pay at least $406,809.96 in restitution to her former employer as part of her plea agreement. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Contract Employee Pleads Guilty To Stealing Data From Employer, Then Extorts Employer For $2.5 Million Threatening To Publish Data Unless Paid - September 27, 2024

Cameron Curry pleaded guilty to stealing sensitive data from his prior employer, a D.C.-based company, and extorting the company by threatening to publish this data unless the company paid him $2.5 million.

Curry admitted that he had been working as a contract employee with the victim company but was told on December 5, 2023, that his last day of employment would be December 15, 2023. On December 11, 2023, posing under the pseudonym of "Loot," Curry began sending a series of emails to the victim company and its employees threatening to publish certain sensitive financial records and personally identifiable information of the victim company's employees. In one email, Curry wrote, "If you wish to reclaim your data, we recommend doing so promptly at 2.5 million USD in order to save your company and stocks, as each subsequent month will incur a $100,000 USD increase." Between December 11 and January 23, Curry allegedly sent over 60 similarly threatening emails to the company.

On January 24, 2024, when the FBI sought to execute a search warrant at Curry's residence, Curry was arrested after he refused to leave the residence and then sent a series of messages to the victim company threatening to publish its data if he were to be arrested. (Source)

Revlon Sues 4 Ex-Employees For Stealing Trade Secrets For Britney Spears Fragrance - September 3, 2024

Revlon has sued four former employees who allegedly sabotaged the beauty giant's long standing relationship with Britney Spears.

Lawyers for Revlon and its subsidiary Elizabeth Arden said the ex-workers stole trade secrets linked to its licensing deal to market the pop star's perfumes.

The four are accused of breaching their contract when they moved to rival Give Back Beauty, taking the Britney account with them.

Fragrances under Britney Spears' branding include Curious, Prerogative and Circus.

According to the complaint filed on August 26 to the New York Southern District Court, Britney Brands refused to sign a new extension the companies had negotiated earlier this year. Revlon's relationship with Britney Brands began in 2004 and was renewed every five years.

This followed the move of ex-Revlon employees Vanessa Kidd and Dominick Romeo, who focused on the Britney Brands account, along with Ashley Fass and Reid Mulvihill to Give Back Beauty, said Revlon.

The lawsuit alleged that Kidd accessed more than 250 files about Elizabeth Arden's fragrance business before she left. Fass, meanwhile, is accused of downloading trade secret information on the subsidiary's fragrance licenses. (Source)

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

No Incidents To Report

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

Pharmacy Chief Financial Officer And Pharmacy President Admit Roles In $33 Million Pharmacy Compounded Medication Fraud Scheme - September 25, 2024

From 2014 through 2016, Jeffrey Andrews, Adam Brosius and others used Main Avenue Pharmacy, a mail-order pharmacy with a storefront in Clifton, New Jersey, to run an illegal kickback scheme involving compounded drugs including scar creams, pain creams, migraine mediation, and vitamins. Andrews worked as the Chief Financial Officer for Main Avenue. Brosius worked as Main Avenue's director of business development, and later as its president.

After filling prescriptions, Main Avenue submitted claims to health care benefit programs for reimbursement, including Medicare, Tricare, and commercial payers in New Jersey and elsewhere. After Main Avenue obtained reimbursement, it paid kickbacks to marketers who had generated the prescriptions. Main Avenue signed contracts with many of the marketers, which detailed the illicit kickback arrangement, which called for Main Avenue to pay each marketer money based on the volume of referrals of compounded prescriptions and the reimbursement amount that Main Avenue received. Main Avenue received approximately $33 million in reimbursements for compounded medications alone from health care benefit programs. Over $5.8 million of that amount was paid by TRICARE, a federal payer. (Source)

Hospital, Laboratory, Referring Physician & 3 Lab Employees Pay $7.2 Million+ To Resolve Allegations Of Fraudulent Laboratory Testing - September 27, 2024

A hospital, a laboratory, three lab employees, and a referring physician and his office manager have agreed to collectively pay the United States more than $7.2 million dollars to resolve civil allegations that they defrauded federal healthcare programs in connection with laboratory tests that were not medically necessary or were tainted by violations of the federal Anti-Kickback Statute. (Source)

Former Medical Practice Administrator Sentenced To Prison for Stealing Nearly $600,000 From Employer / Used Funds For Credit Card Debit, College Tuition, Etc. - September 23, 2024

Tianna Keller is the former Office Manager and Bookkeeper for a Pawtucket, Rhode Island medical practice.

Keller was sentenced to more than two years in federal prison for misappropriating nearly $570,000 in medical practice funds and more than $11,000 in TDI benefits she fraudulently applied for and received,

Keller was ordered to pay restitution totaling $579,857 to the medical practice, an insurance company that covered some of the loss to the medical practice, and the Rhode Island Department of Labor and Training Temporary Disability (TDI) Benefits program.

Keller managed all aspects of the medical practice's finances, developed and executed schemes to add family members and friends as unauthorized paid employees; collected and converted patient co-payments and other business funds to pay her own personal expenses; pay tens of thousands of dollars in personal credit card debt; pay wireless phone bills; and pay college tuition payments for a family member.

Once her fraud was discovered, Keller left the practice on medical leave. Upon expiration of her medical leave, she was terminated from the practice and applied for and was granted TDI benefits. Shortly thereafter, Keller gained new employment but continued to report to the Department of Labor and Training that she was unable to work, and she continued to collect TDI benefit payments she was not entitled to receive. (Source)

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

Company Credit Analyst Pleads Guilty To Embezzling $1.4 Million+ By Directing Payments To His Personal Banking Account - September 10, 2024

Adil Rahman worked in Ontario, Canada as a credit analyst for Company A. that was a subsidiary of a large electrical distribution and services company based in Pittsburgh. As part of his job, Rahman interacted with clients of Company A concerning invoices for the company's services.

Between November 2022 and December 2023, Rahman directed certain customers of Company A to pay their invoices via ACH transfers to his personal bank account, rather than to the account of Company A.

For example, in or about November 2022, Rahman sent an email to the accounts payable department of Company B – a nonprofit municipal corporation based in Hartford, Conn. asking if the company would be interested in paying future invoices to Company A by ACH transfer rather than by check. When Company B agreed to do so, Rahman provided his personal account information to Company B.

Thereafter, under the false impression that it was sending the money to Company A to pay the invoices it owed, Company B sent at least 15 ACH transfers to Rahman's personal account between December 2022 and June 2023.

In May 2023, Rahman emailed the accounts payable department at Company C, a privately held provider of corporate security systems based in Andover, Massachusetts, asking if Company C wished to pay future invoices by ACH transfer. Once again, when Company C agreed to do so, Rahman provided his personal bank account information and Company C thereafter made 11 ACH transfers to Rahman's personal account between May 2023 and July 2023.

In total, through this scheme, Rahman defrauded Company A and its clients of more than $1.4 million. (Source)

Bookkeeper For Funeral Home Sentenced To Prison For Embezzling $500,000+ Over 7 Years - September 12, 2024

LaSaundra Simmons worked as the bookkeeper for Farwell Funeral Service, Inc. for several years.

Starting in 2015, and continuing until it was discovered in January 2023, Simmons employed a scheme to embezzle funds from the company. On more than 100 occasions, she either made unauthorized wire transfers of funds from the funeral home's bank account to her own account, or drafted unauthorized checks which she deposited by electronic wire transfer into her own account. She would often describe these checks as "commissions" or "consulting fees." She embezzled $541,381 over the course of the scheme. (Source)

Pharmaceutical Executive Charged With Insider Trading That Earned Him $250,000+ - September 10, 2024

Dishant Gupta worked as the Director of Strategy and Operations in the Boston office of a global pharmaceutical company (Company A).

In the spring of 2022, during the course of his employment at Company A, Gupta allegedly obtained material non-public information about the fact that Company A was negotiating to acquire certain assets of a smaller pharmaceutical company based in Boston (Company B), including its leading cancer drug, and that Company A later agreed to acquire Company B outright.

While in possession of this material non-public information, and in violation of his fiduciary duties to Company A, Gupta allegedly acquired shares of Company B in his own and his wife's brokerage accounts – in an effort to profit from the eventual public announcement of the transaction. Gupta allegedly purchased more than 300,000 shares of Company B across several different brokerage accounts over approximately two and a half months.

It is further alleged that Gupta then sold all the shares he had acquired after Company A announced the acquisition of Company B.

Gupta allegedly earned more than $250,000 trading in securities of Company B while in possession of material non-public information. (Source)

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

Williams-Sonoma Warehouse Manager Charged With $10 Million+ Fraud Scheme / Used Funds For Purchasing Home, Yacht, Automobiles, Sporting Tickets, Etc. - September 19, 2024

Ben Thomas is a former employee of San Francisco based Williams-Sonoma. He was charged on with defrauding the company more than $10 million.

Thomas is alleged to have registered a fake company called Empire Logistics Services (Empire) billing Williams Sonoma, Inc. millions of dollars for work that Empire never performed, according to the indictment.

Thomas allegedly spent the money on a yacht, automobiles, sporting events tickets, pet cloning, a 12,000-square-foot home, and professional landscaping services for the home.

Thomas worked as a General Manager at a Williams-Sonoma hub and distribution facility in Braselton, Georgia from 2016-2023.

From 2017-2023, he allegedly submitted hundreds of Empire invoices to Williams-Sonoma, each one under his $50,000 approval limit, and approving them.

During that time, Thomas made 335 payments totaling $10 million to a bank account he managed. (Source)

Employee Stole $2.2 Million+ From Employer Over 9 Years / Used Funds For Gambling - September 17, 2024

Between January 2013 and October 2022, Angela Courington stole more than $2.2 million from her employer and his companies in her role as the companies' accounting manager.

Courington made at least 84 company checks payable to herself without authorization by fraudulently forging the signature of the owner of the companies. To conceal her fraud, Courington documented the forged checks in the companies' accounting systems as legitimate expenses. Additionally, as part of her fraudulent scheme, she used the companies' credit cards and funds from her employer's personal bank account for her own benefit, including, in large part, to fund her gambling habit. (Source)

Finance Director For Aviation Company Charged With Stealing $1.2 Million / Used Funds To Pay Credit Cards - September 6, 2024

Elizabeth Batten was the Director of Financing at McCreery Aviation in the Rio Grande Valley in Texas from 2019 to 2023.

While serving in that role, she allegedly diverted company funds to pay for her personal expenses. She used signed blank company checks, intended for legitimate business purposes, to settle her personal credit card accounts. She allegedly concealed her actions by sending the fraudulent payments through the U.S. Postal Service.

In late 2023, a McCreery Aviation employee noticed irregularities in the handling of company checks.

A subsequent investigation allegedly uncovered the full extent of the financial damage Batten's actions caused. (Source)

Employee Embezzles $440,000+ From 2 Different Employers / Used Funds To Pay Credit Cards - September 11, 2024

Between September 2017 and April 2020, Jasmyne Botelho stole at least $280,000 from her employer. Specifically, Botelho directed payments purportedly intended for the company's vendors to bank accounts she controlled and used company funds to make payments on personal credit cards and an auto loan.

To hide her scheme, Botelho falsified her employer's books and records to make it appear as though the payments had in fact been sent to legitimate vendors rather than to Botelho.

Between May 2022 and December 2023, Botelho improperly inflated her payroll from another employer by more than $160,000. She concealed her scheme by manipulating her employer's payroll and accounting software to hide her inflated payroll as well as phony "reimbursements" she paid herself. (Source)

Accounting Firm Employee Stole $405,000+ Of Clients Money To Pay her Personal Credit Card - September 4, 2024

From 2016 to 2021, Irene Fike was employed by an accounting firm in Winchester, where she had access to financial information belonging to the victim and performed bookkeeping tasks for the victim. According to her plea agreement, in the fall of 2021, Fike left her employment at the accounting firm and the victim hired her as an independent contractor to assist with paying bills, creating and updating financial records, general bookkeeping, and other matters. She also had access to the victim's bank accounts.

As part of Fike's scheme, from April 2018 until September 2022, she defrauded the victim through the unauthorized use of the victim's credit cards and bank accounts to benefit herself.

In total, Fike used $224,349.93 in the victim's funds to pay her personal credit card. Additionally, she used the victim's credit cards to make various online purchases totaling $139,307.74.

To conceal her fraud, Fike misrepresented the expenditures and debits on financial reports to avoid raising the suspicions of the victim and family.

Fike was ordered to pay $405,867.08 in restitution to the victim. (Source)

Liquor Store Manager Pleads Guilty To Embezzling $374,000 / Used Funds For Gambling - September 10, 2024

From December 2021 to October 2023, Russel Hester embezzled at least $374,807.10 from the Alcohol Beverage Control Board of Rutherfordton (the Board) which manages the ABC Store where Hester worked as a manager for nearly 10 years.

As store manager, Hester had access to, and control over, the Board's financial accounts and records, wrote checks to pay bills, and was responsible for creating the budget each year. Hester was also responsible for providing all information needed for the annual independent third-party audit of the ABC Store.

Beginning as early as December 19, 2021, Hester used the Board's debit card to withdraw funds at Two Kings Casino. Continuing until October 22, 2023, Hester used this debit card at the casino 192 times to withdraw funds totaling $374,807.10, and used the money to gamble, primarily playing slot machines.

On days where Hester used the Board's debit card, he won jackpots totaling $1,469,368.31, and deposited the winnings into his personal bank accounts.

For example, on July 4, 2023, Hester used the Board's debit card to withdraw $3,000 at Two Kings Casino. Hester then placed these funds into a slot machine and won a jackpot of $18,350. Hester elected to have this jackpot issued in the form of a check, which he deposited into a bank account under his control.

Plea documents also show that Hester took steps to cover up the embezzlement. For example, during the Board's 2023 annual independent audit, Hester provided multiple altered and falsified bank statements to the auditor. In furtherance of the fraud, Hester removed transactions from the casino, added fabricated transactions, and falsified bank account balances on the statements before providing them to the auditor. (Source)

Employee For 2 Non-Profit Organizations (YMCA) Sentenced To Prison For Embezzling $400,000+ - September 12, 2024

Deborah Wilczek was charged in 2023 with devising and carrying out a scheme to defraud the YWCA in Enid (YWCA) and the Cimarron Montessori School (Cimarron).

From November 2012 through April 2019, Wilczek served in leadership positions for the YWCA. She also served on Cimarron's School Board in various capacities from August 2016 to April 2021. The Superseding Indictment alleges Wilczek routinely accessed both the YWCA and Cimarron's business bank accounts, wrote herself checks, and made several unauthorized bank transfers to pay for her personal expenses, including her personal credit card. She concealed her theft by misclassifying these expenses in each nonprofits' bookkeeping system.

In total, Wilczek embezzled $414,951.35 from the two nonprofits, with $139,308.35 coming from YWCA and $275,643 coming from Cimarron. It is also alleged that Wilczek forged Cimarron board members' signatures on checks written to herself and her consulting firm.

The court ordered Wilczek to pay $439,749.80 in restitution, with $139,308.35 going to the YWCA, $221,622.45 going to Cimarron. (Source)

Non-Profit Organization Finance Director Charged With Embezzling $320,000+ / Used Funds For To Pay For Travel For Family & Friends - September 6, 2024

Jarrett Lewis was arrested and charged with embezzling over $320,000 from a District Of Columbia non-profit advocacy organization.

Between October 2021 and October 2022, while serving as Director of Finance for the non-profit, Lewis perpetrated a scheme to defraud his employer. On at least 35 occasions, Lewis used his position to misdirect hundreds of thousands in payments to bank accounts he controlled, while falsely designating the payments to a vendor for "digital" services and creating other false documentation to hide the embezzlement. Lewis also allegedly misused the organization's credit card on at least eleven occasions to purchase airfare for travel by Lewis and his friends and family. (Source)

Employee Extradited From Scotland Sentenced To Prison For Embezzling $165,000 From Employer / Used Funds For Luxury Lifestyle - September 5, 2024

Sarah Tweedie previously worked as a controller of a St. Louis area publishing company. She was responsible for payroll processing, expense reimbursements and paying all company bills, including company credit cards.

From July through January of 2018, Tweedie stole from her employer in multiple ways.

She used her company credit card and a card belonging to a former employee to make $138,137 in purchases, a Scottish kilt and a $1,239 premium seat upgrade on her flight from Chicago to Glasgow. She used the corporate account to purchase $6,400 in Amazon gift cards.

Tweedie also fraudulently increased her annual salary from $80,000 to $110,000 and triggered $16,086 in expense reimbursements to which she was not entitled.

Tweedie began a long-distance relationship with a Scottish man in 2015, according to extradition documents, and they became engaged in March of 2017, the month before she began working for the publishing company.

Tweedie told her employer in December of 2017 that her fiancée had been injured in a car accident and that she needed to leave to be with him. In reality, Tweedie had applied for and received a visa to live in Scotland and did not plan to return. She was arrested on July 9, 2019, but fought extradition until her final appeal was denied in March of 2024. (Source)

Executive Director For Virginia Southwest Regional Recreation Authority Admits To Embezzling $16,000 To Purchase Property - September 27, 2024

Melissa Rose is the former Executive Director of the Southwest Regional Recreation Authority (SRRA) in Vitginia. She pled guilty to bank fraud and embezzlement associated with her scheme to steal money intended for the Spearhead Trail System within the counties of Buchanan, Dickinson, Lee, Russell, Scott, Tazwell, Wise and the City of Norton.

Rose was hired on July 23, 2019, as the Sales and Finance Manager for SRRA. The SRRA Board of Directors promoted Rose to Executive Director in October 2021. As Executive Director, Rose was responsible for the day-to-day operations of the SRRA and the Spearhead Trail System. She resigned from her position on February 3, 2023, following an investigation concerning embezzlement of SRRA funds.

On January 23, 2023, the SRRA learned that Rose had used SRRA funds for her personal use. Specifically, Rose wrote $16,614 in checks drawn on the SRRA's bank account that were purportedly signed by another SRRA board member. The checks were drawn on the SRRA First Bank and Trust Company account and were for the purchase of a residential property priced at $69,5000 with a $15,000 down payment. The property was for Rose's personal use. In an attempt to hide her fraud, Rose logged her payments for the residential property into the SRRA's QuickBooks account management system as purchases for "Tools" with "Land Lease for 5 Years on Mountainview Trail for Conex & SXS Storage" written in the description. She also prepared a fraudulent purchase order and a fraudulent lease for the property, again forging a signature of another SRRA employee. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Office Manager (Mom) & Son Who Worked For The Same Company Sentenced To Prison For Stealing $3.4 Million+ From Employer - September 25, 2024

Eva Wells was the Office Manager for Mid-Georgia Sales and was responsible for its finances, including issuing weekly payroll and making other payments on behalf of the business.

Her son, Billy Lee Wells, Jr., was also employed at Mid-Georgia Sales, working in IT and sales.

In Dec. 2008, Eva Wells began writing unauthorized checks to herself and her son from the company's general operating fund, as opposed to the account used for payroll. When the theft was discovered, a full accounting was conducted. Between Dec. 31, 2008, and May 10, 2019, Eva Wells wrote a total of $3,404,772.22 in unauthorized checks to Billy Lee Wells, Jr. which were either cashed or deposited in his bank account. In addition to the checks made to Billy Lee Wells, Jr., Eva Wells also wrote unauthorized checks to herself which she cashed or deposited into her bank account. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

American Airlines Mechanic Sentenced To Prison For Role In Conspiring To Import $250,000+ Worth Of Cocaine Bricks In Compartment Under Cockpit Of Jet - September 5, 2024

Paul Belloisi was a former American Airlines mechanic at John F. Kennedy International Airport (JFK Airport). He was sentenced to prison for his role in a conspiracy to import and possess cocaine.

On February 4, 2020, American Airlines flight 1349 arrived at JFK Airport's Terminal 8 from Montego Bay, Jamaica. The aircraft was selected for a routine search by CBP officers from the JFK Airport Anti-Terrorism Contraband Enforcement Team. The officers found 10 bricks of cocaine weighing 25.56 pounds hidden inside an electronics compartment on the underside of the cockpit. The cocaine was replaced with fake bricks and sprayed with a substance that glows when illuminated with a special black light.

CBP officers and HSI special agents placed the aircraft under surveillance from a distance and shortly before it was scheduled to take off for its next flight, they observed Belloisi drive up and pull himself inside the electronics compartment. Belloisi was confronted by law enforcement who observed his gloves glowing under the black light indicating he had handled the fake bricks.

Belloisi was also carrying an empty tool bag and the lining of his jacket had cutouts sufficiently large enough to hold the bricks. The cocaine found in the aircraft had a street value of more than $250,000. (Source)

Nurse Working At Rehabilitation Center Sentenced To 3 Years Of Probation For Taking Oxycodone Intended For Patients And Using For Herself - September 18, 2024

From February through May 2020, Jaclyn McQueen worked as a registered nurse at a rehabilitation center in Dedham, Massachusetts. The center provides long-term chronic and post-acute care to patients.

In her capacity as a nurse, McQueen had access to oxycodone, a Schedule II narcotic, prescribed to patients at the rehabilitation center.

During her work shifts, McQueen removed liquid oxycodone from syringes intended for use by patients, consumed the oxycodone herself and refilled the syringes with water to avoid detection. McQueen returned the diluted syringes to the medication carts where they could have been administered to patients. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

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

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

No Incidents To Report

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

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.

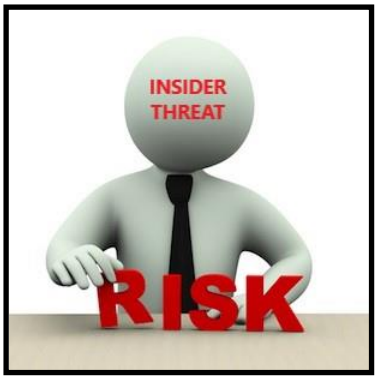
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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 / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

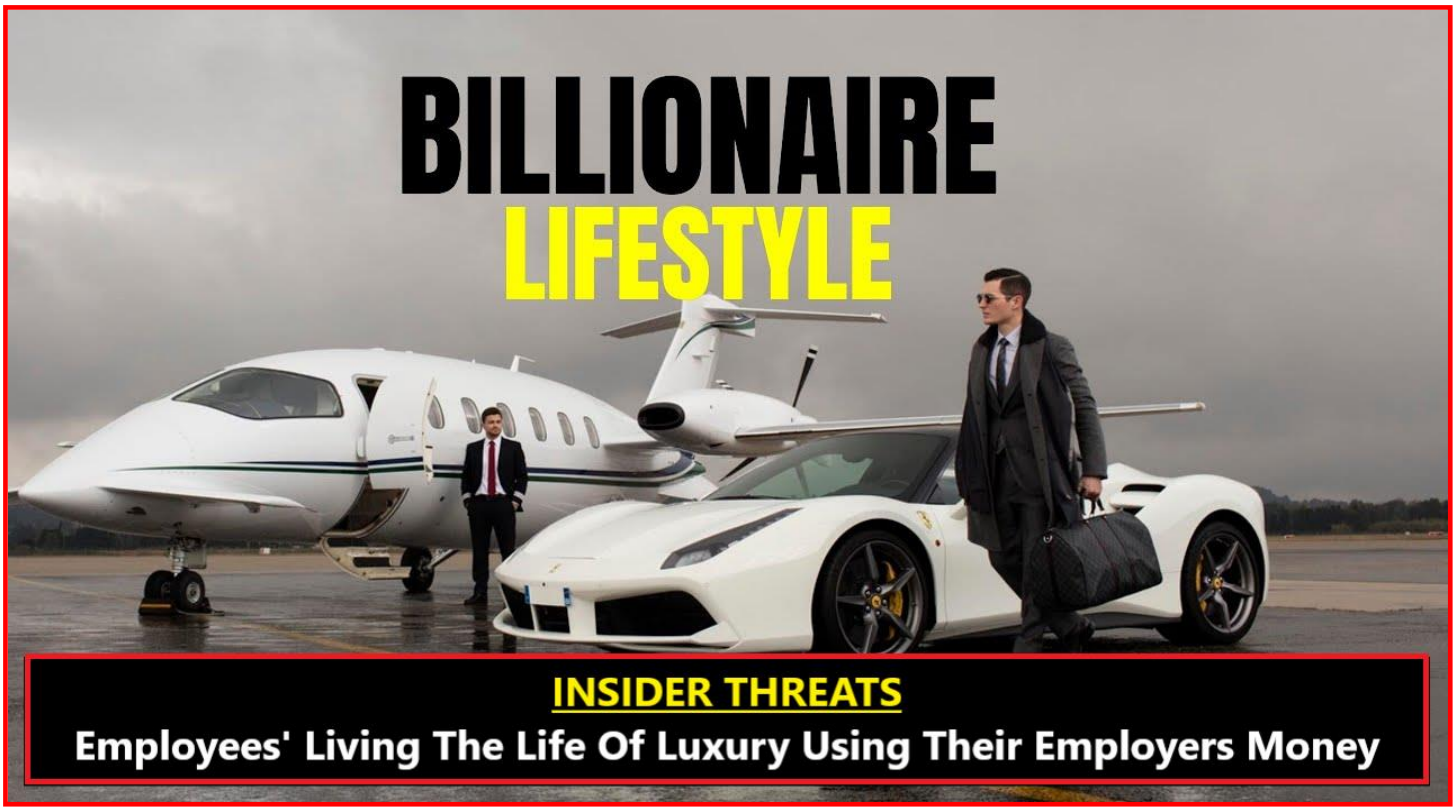
- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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



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

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

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

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

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

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

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

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

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

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

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

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

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

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

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

Fraud In Government Organization's / Infographic

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

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

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

Former Wells Fargo Executive Pleads Guilty To Opening Millions Of Accounts Without Customer Authorization - Wells Fargo Agrees To Pay $3 BILLION Penalty - March 15, 2023

The former head of Wells Fargo Bank's retail banking division (Carrie Tolstedt) has agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 BILLION penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding." (Source)

Former Company Chief Investment Officer Pleads Guilty To Role In $3 BILLION Of Securities Fraud / Company Pays $2.4 BILLION Fine - June 7, 2024

Gregorie Tournant is the former Chief Investment Officer and Co-Lead Portfolio Manager for a series of private investment funds managed by Allianz Global Investors (AGI).

Between 2014 and 2020, Tournant the Chief Investment Officer of a set of private funds at AGI known as the Structured Alpha Funds.

These funds were marketed largely to institutional investors, including pension funds for workers all across America. Tournant and his co-defendants misled these investors about the risk associated with their investments. To conceal the risk associated with how the Structured Alpha Funds were being managed, Tournant and his co-defendants provided investors with altered documents to hide the true riskiness of the funds' investments, including that investments were not sufficiently hedged against risks associated with a market crash.

In March 2020, following the onset of market declines brought on by the COVID-19 pandemic, the Structured Alpha Funds lost in excess of $7 Billion in market value, including over $3.2 billion in principal, faced margin calls and redemption requests, and ultimately were shut down.

On May 17, 2022, AGI pled guilty to securities fraud in connection with this fraudulent scheme and later was sentenced to a pay a criminal fine of approximately $2.3 billion, forfeit approximately $463 million, and pay more than $3 billion in restitution to the investor victims. (Source)

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Paying $1.6 BILLION In Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

Ng Chong Hwa, also known as "Roger Ng," a citizen of Malaysia and a former Managing Director of The Goldman Sachs Group, Inc., was was sentenced to 10 years in prisont for conspiring to launder BILLIONS of dollars embezzled from 1Malaysia Development Berhad (1MDB), conspiring to violate the Foreign Corrupt Practices Act (FCPA) by paying more than $1.6 BILLION in bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

1MDB is a Malaysian state-owned and controlled fund created to pursue investment and development projects for the economic benefit of Malaysia and its people.

Between approximately 2009 and 2014, Ng conspired with others to launder billions of dollars misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions it executed with Goldman Sachs, known as "Project Magnolia," "Project Maximus," and "Project Catalyze." As part of the scheme, Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite also known as "Jho Low," conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

They also conspired to launder the proceeds of their criminal conduct through the U.S. financial system by funding major Hollywood films such as "The Wolf of Wall Street," and purchasing, among other things, artwork from New York-based Christie's auction house including a $51 million Jean-Michael Basquiat painting, a $23 million diamond necklace, millions of dollars in Hermes handbags from a dealer based on Long Island, and luxury real estate in Manhattan.

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

Boeing Charged With 737 Max Fraud Conspiracy Agrees To Pay Over $2.5 BILLION In Penalties Because Of Employees Fraudulent And Deceptive Conduct - January 11, 2021

Aircraft manufacturer Boeing has agreed to pay over $2.5 billion in penalties as a result of "fraudulent and deceptive conduct by employees" in connection with the firm's B737 Max aircraft crashes.

"The misleading statements, half-truths, and omissions communicated by Boeing employees to the FAA impeded the government's ability to ensure the safety of the flying public," said U.S. Attorney Erin Nealy Cox for the Northern District of Texas.

As Boeing admitted in court documents, Boeing through two of its 737 MAX Flight Technical Pilots deceived the FAA about an important aircraft part called the Maneuvering Characteristics Augmentation System (MCAS) that impacted the flight control system of the Boeing 737 MAX. Because of their deception, a key document published by the FAA lacked information about MCAS, and in turn, airplane manuals and pilot-training materials for U.S.-based airlines lacked information about MCAS.

On Oct. 29, 2018, Lion Air Flight 610, a Boeing 737 MAX, crashed shortly after takeoff into the Java Sea near Indonesia. All 189 passengers and crew on board died.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 MAX, crashed shortly after takeoff near Ejere, Ethiopia. All 157 passengers and crew on board died. (Source)

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than $1.4 billion in loans. (Source)

Member Of Supervisory Board Of State Employees Federal Credit Union Pleads Guilty To $1 BILLION Scheme Involving High Risk Cash Transactions - January 31, 2024

A New York man pleaded guilty today to failure to maintain an anti-money laundering program in violation of the Bank Secrecy Act as part of a scheme to bring lucrative and high-risk international financial business to a small, unsophisticated credit union.

From 2014 to 2016, Gyanendra Asre of New York, was a member of the supervisory board of the New York State Employees Federal Credit Union (NYSEFCU), a financial institution that was required to have an anti-money laundering program. Through the NYSEFCU and other entities, Asre participated in a scheme that brought over $1 billion in high-risk transactions, including millions of dollars of bulk cash transactions from a foreign bank, to the NYSEFCU.

In addition, Asre was a certified anti-money laundering specialist who was experienced in international banking and trained in anti-money laundering compliance and procedures, and represented to the NYSEFCU that he and his businesses would conduct appropriate anti-money laundering oversight as required by the Bank Secrecy Act. Based on Asre's representations, the NYSEFCU, a small credit union with a volunteer board that primarily served New York state public employees, allowed Asre and his entities to conduct high-risk transactions through the NYSEFCU. Contrary to his representations, Asre willfully failed to implement and maintain an anti-money laundering program at the NYSEFCU. This failure caused the NYSEFCU to process the high-risk transactions without appropriate oversight and without ever filing a single Suspicious Activity Report, as required by law. (Source)

Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024

3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the world. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Pearce concealed the fraud scheme for many years by using these privileges to alter information about the accounts, which helped hide his creation of unauthorized license keys. Dusti Pearce handled accounting for the illegal business.

Hines operated Direct Business Services International (DBSI), a New Jersey-based business communications systems provider and a de-authorized Avaya reseller. He bought ADI software license keys from Brad and Dusti Pearce and then sold them to resellers and end users around the world for significantly below the wholesale price. Hines was by far the Pearces' largest customer and significantly influenced how the scheme operated. Hines was one of the biggest users of the ADI license system in the world.

To hide the nature and source of the money, the Pearces funneled their illegal gains through a PayPal account created under a false name to multiple bank accounts, and then transferred the money to investment and bank accounts. They also purchased large quantities of gold bullion and other valuable items. (Source)

COLLUSION – HOW MANY EMPLOYEES' OR INDIVIDUALS CAN BE INVLOVED?

193 Individuals Charged (Doctors, Nurses, Medical Professionals) For Participation In $2.75 BILLION Health Care Fraud Schemes - June 27, 2024

The Justice Department today announced the 2024 National Health Care Fraud Enforcement Action, which resulted in criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

In connection with the coordinated nationwide law enforcement action, and together with federal and state law enforcement partners, the government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication; over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

2 Executives Who Worked For a Geneva Oil Production Firm Involved In Misappropriating $1.8 BILLION - April 25, 2023

The former Petrosaudi employees are suspected of having worked with Jho Low, the alleged mastermind behind the scheme, to set up a fraudulent deal purported between the governments of Saudi Arabia and Malaysia, according to a statement from the Swiss Attorney General.

1MDB was the Malaysian sovereign wealth fund designed to finance economic development projects across the southeastern Asian nation but become a byword for scandal and corruption that triggered investigations in the US, UK, Singapore, Malaysia, Switzerland and Canada.

Low, currently a fugitive whose whereabouts are unknown, has previously denied wrongdoing. His playboy lifestyle was financed with money stolen from 1MDB, according to US prosecutors.

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 billion in financing from 1MDB, according to Swiss prosecutors. The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

The allegations cover a period at least from 2009 to 2015 and the duo have been indicted for commercial fraud, aggravated criminal mismanagement and aggravated money laundering. (Source)

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION in Health Care Fraud Scheme - June 28, 2023

The Justice Department, together with federal and state law enforcement partners, announced today a strategically coordinated, two-week nationwide law enforcement action that resulted in criminal charges against 78 defendants for their alleged participation in health care fraud and opioid abuse schemes that included over $2.5 Billion in alleged fraud. The enforcement action included charges against 11 defendants in connection with the submission of over $2 Billion in fraudulent claims resulting from telemedicine schemes.

In a case involving the alleged organizers of one of the largest health care fraud schemes ever prosecuted, an indictment in the Southern District of Florida alleges that the Chief Executive Officer (CEO), former CEO, and Vice President of Business Development of purported software and services companies conspired to generate and sell templated doctors' orders for orthotic braces and pain creams in exchange for kickbacks and bribes. The conspiracy allegedly resulted in the submission of $1.9 Billion in false and fraudulent claims to Medicare and other government insurers for orthotic braces, prescription skin creams, and other items that were medically unnecessary and ineligible for Medicare reimbursement. (Source)

10 Individuals (Hospital Managers And Others) Charged In $1.4 BILLION Hospital Pass - Through Billing Scheme - June 29, 2020

10 individuals, including hospital managers, laboratory owners, billers and recruiters, were charged for their participation in an elaborate pass-through billing scheme using rural hospitals in several states as billing shells to submit fraudulent claims for laboratory testing.

The indictment alleges that from approximately November 2015 through February 2018, the conspirators billed private insurance companies approximately $1.4 billion for laboratory testing claims as part of this fraudulent scheme, and were paid approximately $400 million. (Source)

Former University Financial Advisor Sentenced To Prison For $5.6 Million+ Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee. As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied.

Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

3 Bank Board Members Of Failed Bank Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman. Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

TRADE SECRET THEFT

Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION - May 2, 2022

Gongda Xue worked as a scientist at the Friedrich Miescher Institute for Biomedical Research (FMI) in Switzerland, which is affiliated with Novartis. His sister, Yu Xue, worked as a scientist at GlaxoSmithKline (GSK) in Pennsylvania. Both Gongda Xue and Yu Xue conducted cancer research as part of their employment at these companies.

While working for their respective entities, Gongda Xue and Yu Xue shared confidential information for their own personal benefit.

Gongda Xue created Abba Therapeutics AG in Switzerland, and Yu Xue and her associates formed Renopharma, Ltd., in China. Both companies intended to develop their own biopharmaceutical anti-cancer products.

Gongda Xue stole FMI research into anti-cancer products and sent that research to Yu Xue. Yu Xue, in turn, stole GSK research into anti-cancer products and sent that to Gongda Xue. Yu Xue also provided hundreds of GSK documents to her associates at Renopharma. Renopharma then attempted to re-brand GSK products under development as Renopharma products and attempted to sell them for billions of dollars. Renopharma's own internal projections showed that the company could be worth as much as $10 billion based upon the stolen GSK data. (Source)

U.S. Brokerage Firm Accuses Rival Firm Of Stealing Trade Secrets Valued At Over $1 BILLION - November 14, 2023

U.S. brokerage firm BTIG sued rival StoneX Group, accusing it of stealing trade secrets and seeking at least $200 million in damages.

StoneX recruited a team of BTIG traders and software engineers to exfiltrate BTIG software code and proprietary information and take it to StoneX, according to lawyers for BTIG.

StoneX used the software code and proprietary information to build competing products and business lines that generate tens of millions of dollars annually, they alleged in the lawsuit.

BTIG said in the lawsuit that StoneX had committed one of the greatest financial industry trade secret frauds in recent history, and that the scope of its misconduct is not presently known, and may easily exceed a billion dollars."

The complaint said StoneX hired several BTIG employees to steal confidential information that it used to develop its competing trading platform.

The complaint said that StoneX's stock price has increased 60% since it started misusing BTIG's trade secrets. (Source)

U.S. Petroleum Company Scientist Sentenced To Prison For $1 BILLION Theft Of Trade Secrets - Was Starting New Job In China - May 27, 2020

When scientist Hongjin Tan resigned from the petroleum company he had worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.

But Tan told a colleague a different story over dinner. He revealed to his colleague that he actually did have a job waiting for him in China. Tan's dinner companion reported the conversation to his supervisor. That conversation prompted Tan's employer to ask him to leave the firm immediately, and his employer made a call to the FBI tip line to report a possible crime.

Tan called his supervisor to tell them he had a thumb drive with company documents on it. The company told him to return the thumb drive. When he brought back the thumb drive, the company looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about. (Source)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners. As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

CEO Of Bank Sentenced To Prison For $47 Million Fraud Scheme That Caused Bank To Collapse - August 19, 2024

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering." The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (Source)

3 Bank Board Members Of Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged / Bank Collapsed - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (Source)

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

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

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly.

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

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

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

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

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

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

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

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis.

From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

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

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

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

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

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

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

Former Controller Of Oil & Gas Company Sentenced To Prison For Role in $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999.

In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

EMPLOYEE EXTORTION

Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / He Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - February 2, 2023

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through April 1, 2021. Sharp was a Senior Developer who had administrative to credentials for company's Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from his technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guilty To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE

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

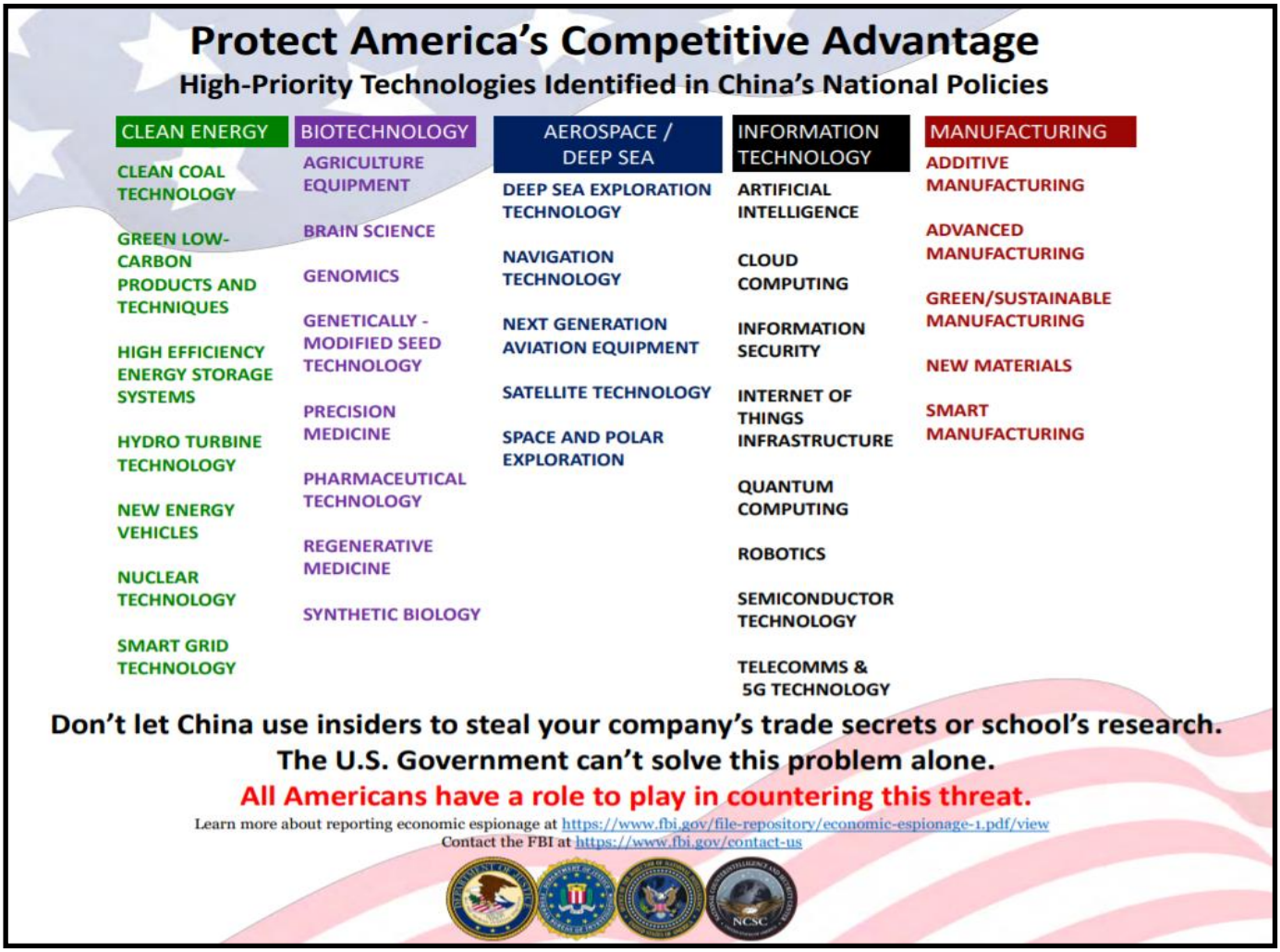
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 (**5,700+ 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 SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

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 / X

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)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Insider Threat Symposium & Expo

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 Insider Threat Program Managers / Insider Risk Program Managers with ***Hands On Experience***.

At the expo are many vendors that showcase their training, services and products. This link provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.

ITS&E events were not held in 2020 to 2023 because of COVID. The next ITS&E is scheduled for March 4, 2025 at the John Hopkins University Applied Physics Lab in Laurel, Maryland

The ITS&E provides attendees with access to a large network of security professionals for collaborating with on all aspects of IRM.

NITSIG Advisory Board

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

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and Insider Risk Management Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive Insider Risk Management. We will provide the training, guidance and resources to ensure that the Insider Risk Program Manager and key stakeholders are universally aligned from an enterprise / holistic perspective to detect and mitigate Insider Risks and Threats.

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training & Workshops For C-Suite, Insider Risk Program Manager / Working Group, Insider Threat Analysts & Investigators
- ✓ IRM Program Development, Management & Optimization Training & Related Courses
- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx 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 **675+** organizations. (Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

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

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