INSIDER THREAT INCIDENTS REPORT
FOR
April 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

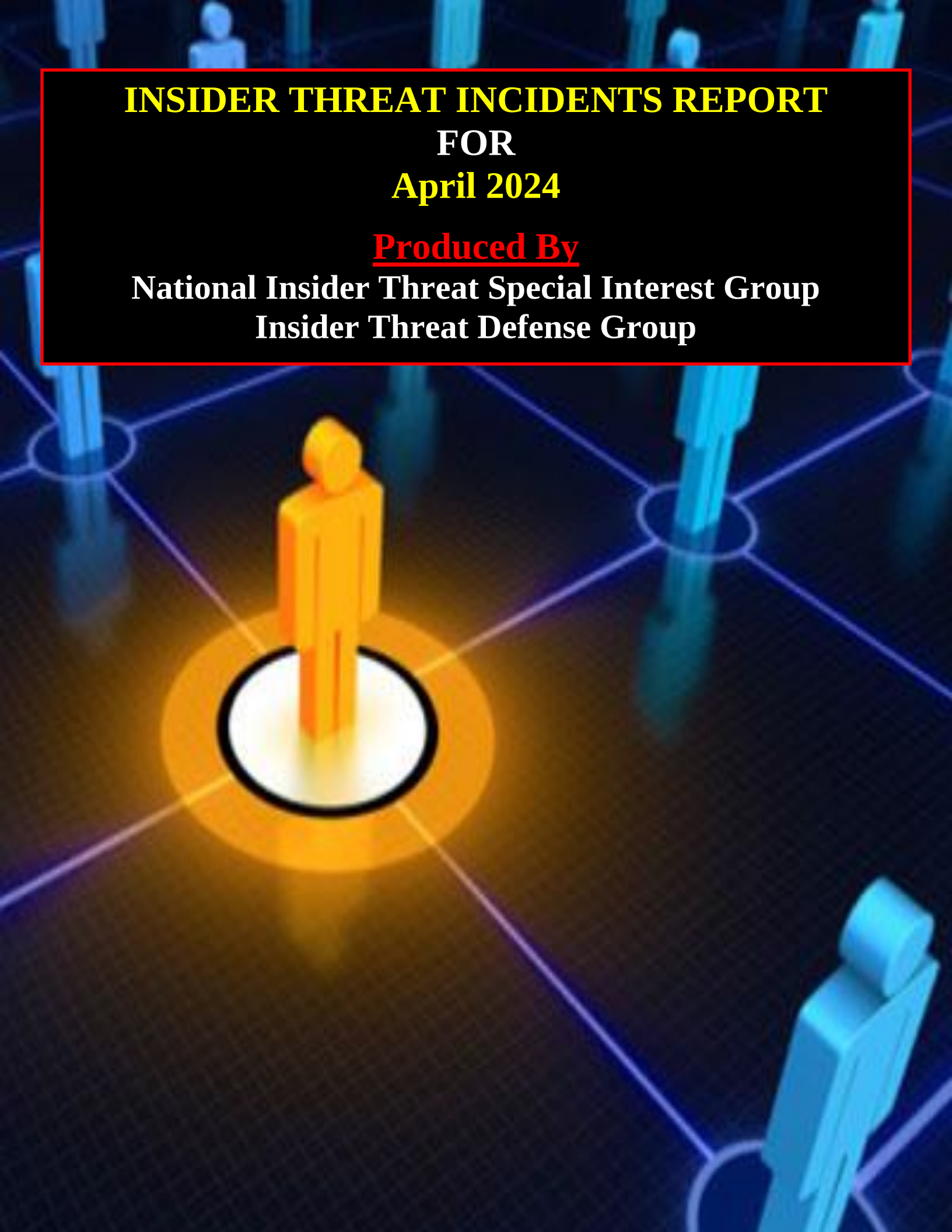


TABLE OF CONTENTS

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 **5,300+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

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

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 IRM. The incidents listed on pages **4 to 31** of this report provide the justification, return on investment and the funding that is needed for an Insider Risk Management Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR APRIL 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Former Comptroller General Of Ecuador Convicted For Role In $10 Million International Bribery & Money Laundering Scheme - April 24, 2024

Between 2010 to 2015, Carlos Faggioni solicited and received over $10 million in bribe payments from Odebrecht S.A., the Brazil-based construction conglomerate. Faggioni took bribes from Odebrecht in exchange for removing fines and not imposing fines on Odebrecht's projects in Ecuador. Additionally, in or around 2015, Polit received a bribe from an Ecuadorian businessman in exchange for assisting the businessman with obtaining certain contracts with the state-owned insurance company of Ecuador.

From in or around 2010 and continuing until at least 2017, at the direction of Polit, another member of the conspiracy caused proceeds of Polit's bribery scheme to "disappear" by using Florida companies registered in the names of friends and associates, often without the associates' knowledge. The conspirators also used funds from Polit's bribery scheme to purchase and renovate real estate in Florida.

Odebrecht S.A. pleaded guilty in December 2016 in the Eastern District of New York to conspiring to violate the anti-bribery provisions of the Foreign Corrupt Practices Act (FCPA) in connection with a broader scheme to pay nearly $800 million in bribes to public officials in 12 countries, including Ecuador. (Source)

Former Austria Intelligence Officer Arrested For Espionage With Russia – April 8, 2024

Austria faces its biggest espionage scandal in decades as the arrest of a former Intelligence Officer brings to light evidence of extensive Russian infiltration, lax official oversight and behavior worthy of a spy novel.

Egisto Ott was arrested March 29, 2024. The 86-page arrest warrant, obtained by The Associated Press, alleges among other things that he handed over cellphone data of former high-ranking Austrian officials to Russian intelligence, helped plot a burglary at a prominent journalist's apartment, and wrote up suggestions for improvement after a Russian-ordered killing in Germany.

Ott is suspected of having provided sensitive information to Jan Marsalek, a fugitive fellow Austrian wanted on suspicion of fraud since the collapse in 2020 of German payment company Wirecard, where he was the Chief Operating Officer. The warrant says chat messages provided by British authorities link Marsalek directly to the Russian intelligence agency FSB. German and Austrian media have reported that Marsalek is believed to have had connections to Russian intelligence since at least 2014. He is now thought to be in Russia. (Source)

U.S. GOVERNMENT

Former Social Security Employee Sentenced To Prison For $288,000+ COVID Pandemic Unemployment Assistance Fraud Scheme / Used Funds For Personal Expenses - April 3, 2024

Takiyah Austin pleaded guilty to one count wire fraud and one count of aggravated identify theft.

From May 2020 to May 2021, Austin, a Claims Specialist with the Social Security Administration (SSA), filed Pandemic Unemployment Assistance claims for ineligible recipients in exchange for payment from the individuals. Austin filed claims after accessing SSA databases to obtain the personal identifying information from unsuspecting individuals and then diverted the unemployment funds to addresses she controlled in order to use the funds for her own personal expenses. Through the scheme, Austin defrauded the government of over $288,000. (Source)

Former Social Security Administration Employee Facing Charges For $49,000+ Involving Multiple Fraud Schemes - April 26, 2024

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

Between February 13, 2019, and June 17, 2022, Markham allegedly engaged in a scheme by which he made it appear as though he was teleworking full-time for SSA during workdays, when in reality, he was earning income working as a home inspector for his personal business, Markham Inspection Services. 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.

Markham allegedly 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.

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. In total, Markham's fraudulent conduct caused a loss to the SSA of approximately $49,255.97. (Source)

Former U.S. Bolivia Ambassador / National Security Council Official Sentenced To Prison For Secretly Acting As An Agent Of The Cuban Government - April 12, 2024

Victor Rocha, is a former U.S. Department of State employee who served on the National Security Council from 1994 to 1995 and as U.S. Ambassador to Bolivia from 2000 to 2002.

Rocha pleaded guilty to secretly acting for decades as an agent of the government of the Republic of Cuba. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Defense Contractor Pleads Guilty That Company Vice President Bribed A Navy Employee Involving Government Contracts Worth $100 Million+ - April 17, 2024

Cambridge International Systems, Inc., a defense contractor headquartered in Arlington, Virginia, pleaded guilty in federal court today, admitting that it participated in a bribery scheme with the company's former Executive Vice President Russell Thurston, and former Naval Information Warfare Center employee James Soriano, among others.

Thurston and an unnamed employee gave various things of value to Soriano, including jobs for Soriano's family and friends, meals, and a ticket to the 2018 MLB All Star Game held at Nationals Park in Washington D.C. One of the friends hired by Cambridge, Liberty Gutierrez, was giving Soriano $2,000 a month from her Cambridge salary.

In return, Soriano, acting in his position as a contracting officer's representative at Naval Information Warfare Center ensured that Cambridge was awarded two large task orders. Soriano further ensured Cambridge was able to capture a steady stream of government funds by approving various projects on the task orders after they were awarded the contract, including more than 70 projects on one of the task orders. As a result of the conspiracy, the government obligated more than $32 million on one of the task orders and over $100 million on the other.

Soriano also allowed Cambridge employees to draft various procurement documents for him, even where the company was competing for the contract against other bidders.

Thurston and Soriano worked together to remove document properties so other government employees would not know of Cambridge's involvement in drafting the documents.

Cambridge admitted that the company made a total profit of $7,429,995.23 as a result of the conspiracy. (Source)

Former U.S. Marine And U.S. Navy Sailor Sentenced To Prison For $65 Million+ Military Healthcare Program Fraud & Kickback Scheme - April 12, 2024

Former U.S. Marine Joshua Morgan and former U.S. Navy Sailor Kyle Adams were sentenced to 21 months and 15 months, respectively, and ordered to pay millions in restitution and forfeit the fruits of their criminal activity.

Morgan and Adams have admitted that they recruited fellow service members and their dependents to receive expensive prescription compounded drugs, while others in the conspiracy wrote bogus prescriptions and filled out duplicitous paperwork to process fraudulent insurance reimbursements, resulting in at least $65 million in losses to TRICARE.

According to plea agreements, the service members that Morgan and Adams recruited agreed to receive the pricey compounded medications in return for a monthly kickback of approximately $300. For young Sailors and Marines this money was equivalent to a significant portion of their monthly paycheck. Morgan noted that "it took very little work to sign people up to receive free money."

For recruiting bogus patients, defendants Morgan and Adams were paid an illegal kickback of between 3 and 7 percent of the total TRICARE reimbursement paid to the pharmacy for the drugs sent to their recruits. By the time this fraud scheme was in full swing, the average cost for these compounded drugs was over $13,000 for a 30-day supply, peaking at around $25,000 for individual drugs.

Over the course of the conspiracy, those illegal kickbacks amounted to at least $2,633,942.69 for Morgan, which, in recognition of his role as the top-level recruiter in this multi-level marketing scheme, was more than twice as much as the next nearest patient recruiter. Meanwhile, Adams earned more than $1 million for his efforts. (Source)

U.S. Army Financial Counselor Admits To Defrauding Families Through Investment Scheme Which Earned Him $1.4 Million In Commissions - April 16, 2024

From November 2017 to January 2023, Caz Craffy was a civilian employee of the U.S. Army, working as a financial counselor with the Casualty Assistance Office. He was also a Major in the U.S. Army Reserves, where he has been enlisted since 2003. Craffy was responsible for providing general financial education to the surviving beneficiaries. He was prohibited from offering any personal opinions regarding the surviving beneficiary's benefits decisions.

Craffy was not permitted to participate personally in any government matter in which he had an outside financial interest. However, without telling the Army, Craffy simultaneously maintained outside employment with two separate financial investment firms.

Craffy used his position as an Army financial counselor to identify and target Gold Star families and other military families. He encouraged the Gold Star families to invest their survivor benefits in investment accounts that he managed in his outside, private employment. Based upon Craffy's false representations and omissions, the vast majority of the Gold Star families mistakenly believed that Craffy's management of their money was done on behalf of and with the Army's authorization.

From May 2018 to November 2022, Craffy obtained more than $9.9 million from Gold Star families to invest in accounts managed by Craffy in his private capacity. Once in control of this money, Craffy repeatedly executed trades, often without the family's authorization. These unauthorized trades earned Craffy high commissions. During the timeframe of the alleged scheme, the Gold Star family accounts had lost more than $3.7 million, while Craffy personally earned more than $1.4 million in commissions, drawn from the family accounts. (Source)

U.S. Army Reservist Sentenced To Prison For Theft Of $11,000+ From Government - April 26, 2024

Leroy Daniels stole $11,693.87 from the U.S. Army by claiming reimbursement for the performance of military funeral honors ceremonies that never occurred. (Source)

Navy Chief Facing Found Guilty For Passing Classified Information To A Foreign Government - April 21, 2024

Chief Petty Officer Fire Controlman Bryce Pedicini, a sailor assigned to a guided-missile destroyer based in Japan, has been found guility of espionage for and passing classified information to a foreign government contact.

Prosecutors contended in a March 15 filing that an unnamed foreign government employee contacted Pedicini via Facebook Messenger and stated he or she was a defense researcher who offered him money in exchange for information about the U.S. military capabilities and strategies in the specific region.

Starting in November 2022 and continuing into May 2023 in the Hampton Roads, Va., area, the government alleged, Pedicini sent various documents through Facebook Messenger and other electronic means, including Signal and Telegram, and in May 2023 sent photographs he accessed via a classified SIPR terminal. At one point, that contact sent him a reportedly "secret" document "as an example" of documents they sought from him, a point his defense attorneys later argued was "inflammatory evidence" but not a wrongful act.

In a filing earlier this month, government prosecutors alleged the chief had received money paid via PayPal to his credit union account. "In exchange for national defense information, the accused sought and received monetary payment from Individual #1," the document stated

Pedicini had also been charged with failing to report foreign contacts to his chain of command, failing to report solicitation of classified information, taking a personal device into a secure room, and transporting classified information. (Source)

Former Marine Corps Reservist Sentenced To Prison For Stealing, Forging, Selling & Distributing Fraudulent COVID-19 Vaccination Cards - April 6, 2024

Jia Liu was sentenced to 21 months in prison for conspiring to steal, forge and distribute fraudulent COVID-19 Vaccination Cards.

On June 9, 2023, co-defendant Steven Rodriguez, a Long Island nurse, was sentenced to 30 months' imprisonment for his role in the same scheme. Liu and Rodriguez pleaded guilty in April 2023 to conspiracies to defraud and obstruct the United States' response to the COVID-19 pandemic.

In May 2021, Liu and Rodriguez conspired to steal, forge, sell and distribute COVID-19 Vaccination Cards to hundreds of unvaccinated persons. In addition to the cards, Liu and Rodriguez also offered buyers and co-conspirators false entry into government immunization databases.

Liu specifically targeted the armed forces and their attempts to contain the COVID-19 pandemic. From approximately August 2021 or earlier, the defendant created and distributed false COVID-19 Vaccination Cards to members of the U.S. Marine Corps Reserve to help them evade its vaccination requirements. Liu boasted to a co-conspirator on an encrypted messaging app: "you have no idea how many documents I have faked in my usmc (United States Marine Corps) career." (Source)

Former Veterans Affairs Procurement Supervisor Sentenced To Prison For Receiving Thousands In Kickbacks For 7 Years - April 15, 2024

While serving as a Procurement Supervisor at Veterans Affairs Medical Center in Chicago, Thomas Duncan received thousands of dollars in kickbacks paid in cash and checks from Daniel Dingle, the President of a medical supply company in Dolton, Illinois. The checks were made payable to Helping Hands Properties LLC, a third-party entity managed by Duncan, that contained false and misleading memo entries in order to conceal and disguise the existence and purpose of the kickbacks.

In exchange for the kickbacks, Duncan used his official position at the VA to fraudulently initiate and approve purchases of products from Dingle's company, knowing that many of the products would not actually be delivered to the VA.

The fraud scheme began in 2012 and continued until 2019. In late 2018, after Duncan became aware that the VA Inspector General's Office was investigating his conduct, Duncan created fake invoices from Helping Hands purporting to document work performed for Dingle's company. Duncan also told Dingle to falsely tell investigators that the payments Duncan received from Dingle's company were for work performed by Helping Hands. (Source)

U.S. Army Service Member Sentenced To Prison In Money Laundering Romance Scam - April 18, 2023

Sanda Frimpong, was an active duty service member stationed at Fort Bragg.

Frimpong was arrested after the unsealing of a 19-count indictment that included charges of Money Laundering,Fraud, Conspiracy, Aggravated Identity Theft, and Access Device Fraud in connection with multiple interstate and international fraud and money-laundering scams.

Frimpong and other conspirators, engaged in elaborate scams, impersonating romantic love interests, diplomats, customs personnel, military personnel, and other fictitious personas for the purpose of ensnaring their victims by earning their confidence, including promises of romance, sharing of an inheritance or other riches, or other scenarios intended to fraudulently induce the victims to provide money or property to the conspirators.

Frimpong allegedly laundered hundreds of thousands of dollars in proceeds of these frauds through his various bank accounts across state lines and through contacts in Ghana. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

DHS ICE Deportation Officer Charged For Money Laundering $700,000 - April 11, 2024

Christopher Toral is an employee of the Department of Homeland Security (DHS), working as a Deportation Ifficer for Immigration and Customs Enforcement.

On three occasions in 2023, Toral allegedly transported a total of approximately $700,000 in exchange for cash payments. In each instance, he believed the monies were proceeds from drug transactions..

Toral transported $200,000 between Feb. 9 and 28, 2023, from Dallas to Houston, according to the charges. In early March 2023, he allegedly travelled from Newark, New Jersey, to Houston with $300,000 in U.S. currency. (Source)

Prison Correctional Officer Supervisor Charged With Accepting $200,000+ In Bribes To Smuggle Contraband Into Prison - April, 15, 2024

Christine Livingston was a Correctional Officer / Supervisor at the South Carolina Department of Corrections (SCDC), where she worked as a law enforcement officer from 2005 through 2021.

Jerell Reaves is an inmate serving a sentence for voluntary manslaughter.

During her work at the Broad River Correctional Institute, Livingston accepted more than $200,000 in bribes from inmates and their families in exchange for smuggling contraband into the prison. She is alleged to have brought approximately 173 contraband cell phones into the facility, as well as headphones, sim cards, chargers, and other contraband.

Reaves is alleged to have caused more than $40,000 in bribes to be paid to Livingston in exchange for contraband. (Source)

Police Officer & Accountant Plead Guilty To $95,000+ COVID Emergency Loan Fraud Scheme - April 24, 2024

Owen Grigsby is a patrol officer with the Metropolitan Police Department (MPD) who is currently on administrative leave with pay.

Himmeh Kuawogai is an accountant and owner of HAK Accounting Services.

Kuawogai helped Grigsby establish Owen Grigsby Associates (OAG) in Maryland in July 2020. At the time, Grigsby was employed by the MPD. Although Grigsby was required to report any outside business venture to MPD pursuant to MPD policies, Grigsby failed to do so. OGA allegedly had no legitimate purpose and was created only to obtain Economic Injury Disaster Loans (EIDLs) and Paycheck Protection Program (PPP) loans.

In October 2020, Grigsby filed an EIDL application on behalf of OGA containing materially false statements to the Small Business Administration (SBA). Grigsby was approved for that loan and fraudulently obtained $53,600.00.

Grigsby also received an additional $40,000 in fraudulent loans. (Source)

DEA Task Force Officer Sentenced To Prison For Role In Distributing Narcotics - April 8, 2024

While employed as a Florida Highway Patrol Trooper and designated Task Force Officer with the Drug Enforcement Administration, Joshua Earrey and a co-conspirator engaged in widespread and extensive corrupt activity from 2017 - 2023. These corrupt acts included the theft of money and illegal drugs that were seized as evidence during criminal investigations; providing the illegal drugs to others to distribute on his behalf; and extorting or accepting cash payments from drug dealers in exchange for protecting them from arrest by law enforcement.

Earrey and his co-conspirator stole more than 1,000 pounds of marijuana from evidence and covered up the theft by submitting falsified paperwork showing that the drugs had been destroyed. Earrey, who had an addiction to prescription opiates, also used his corrupt activities to obtain illegal drugs for his own use. On one occasion, he traded cases of ammunition that he had diverted from the Florida Highway Patrol to a convicted murderer in exchange for oxycodone. Despite knowing that his drug addiction made it illegal for him to have firearms and ammunition, Earrey continued to possess these items in violation of federal law. (Source) (Source)

Former State Police Lieutenant Sentenced To Prison For Overtime Fraud Scheme While Running His On Business On The Side - April 26, 2024

From 2015 through 2018, Daniel Griffin and other troopers in the Traffic Programs Section at State Police Headquarters in Framingham, Massachusetts, conspired to steal thousands of dollars in federally funded overtime by regularly arriving late to, and leaving early from, overtime shifts funded by grants intended to improve traffic safety. During the course of the conspiracy, Griffin made and approved false entries on forms and other documentation to conceal and perpetuate the fraud.

When the Massachusetts State Police (MSP) overtime misconduct came to light in 2017 and 2018, Griffin, William Robertson and their co-conspirators took steps to avoid detection by shredding and burning records and forms. After an internal inquiry regarding missing forms, Griffin submitted a memo to his superiors that was designed to mislead them by claiming that missing forms were “inadvertently discarded or misplaced” during office moves.

Griffin spent significant time running his security business, Knight Protection Services, during hours that he was collecting regular MSP pay and overtime pay. From 2012 to 2019, Griffin collected almost $2 million in KnightPro revenue. Of that total, Griffin hid over $700,000 in revenue from the IRS and used hundreds of thousands of dollars in KnightPro income to fund personal expenses, such as golf club expenses, car payments, private school tuition and expenses related to his second home on Cape Cod. (Source)

U.S. Customs Border Patrol Agent Sentenced To Prison For Drug Smuggling And Bribery - April 12, 2023

On August 9, 2020, while working as a United States Border Patrol Agent, Carlos Passapera drove his Border Patrol vehicle into the Arizona desert, and retrieved two large duffel bags. Passapera then changed vehicles and transported the duffel bags to the Phoenix Sky Harbor International Airport, where he parked and loaded the bags into the vehicle of a co-conspirator.

The co-conspirator was stopped by law enforcement shortly after leaving the airport parking lot. A search of the two duffel bags revealed multiple packages of cocaine, fentanyl, and heroin. Approximately 21 kilograms of cocaine, one kilogram of fentanyl, and one kilogram of heroin were seized. An additional $311,100 in U.S. currency was seized from Passapera's safe deposit box. Passapera admitted to accepting large cash payments in exchange for using his position to smuggle drugs. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Atlanta's Former Chief Financial Officer Pleads Guilty To Theft Of Government Funds For Personal Use - April 8, 2024

From approximately November 2011 to May 2018, Jim Beard served as the CFO of the City of Atlanta. As CFO, Beard directed and managed the Department of Finance, with primary responsibility for oversight and management of the City's financial condition.

During his tenure, Beard devised and executed a scheme to obtain money and property from the City of Atlanta for private use, including using City of Atlanta funds to: **(1)** pay for personal travel expenses for himself, his family, and his travel companions; **(2)** buy items for personal use, including two machine guns; **(3)** pay for travel to conferences or meetings for which the conference or meeting host reimbursed Beard, but Beard kept the money and did not give the reimbursement funds to the City of Atlanta; and **(4)** pay for travel that Beard falsely claimed to the IRS was related to his personal consulting business. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Principal Racist Comments Were Actually A Fake AI Recording Created By Disgruntled Employee - April 25, 2024

A Maryland high school principal didn't go on a racist rant about "ungrateful Black kids" and Jewish individuals as suggested by a voice recording that surfaced online in January, according to police.

Pikesville High School Principal Eric Eiswert denied making the disparaging comments heard in the recording, and suspected his technologically savvy athletic director was somehow behind it, police wrote in charging documents.

Eiswert told police he had discussions with the athletic director about not renewing his contract, and this fueled a grievance between them ahead of the audio clip's release.

The now former athletic director, Dazhon Darien was arrested or disrupting school activities. "We have now conclusive evidence that the recording was not authentic," Baltimore County Police Chief McCullough said at a news conference. Darien is accused of using AI to create the recording of Eiswert. The fake recording "not only led to (Eiswert's) temporary removal from the school but also triggered a wave of hate-filled messages on social media and numerous calls to the school.

Darien is accused of making the clip in retaliation against Eiswert, "who had launched an investigation into the potential mishandling of school funds. Darien is charged with stealing school district funds valued between $1,500 and $25,000, according to police. (Source)

School District Employee Accused Of Embezzling $100,000+ - April 17, 2024
Linda Johnson is facing multiple federal charges after being accused of embezzling money from 2020-2022 as an employee at Dupo Community Unit School District #196.

Johnson worked an administrative role in the superintendent's office. In this role, Johnson oversaw the district's activities account with funds for student athletics, clubs, and extracurriculars.

The indictment charges that Johnson received control over cash and checks intended to be deposited into the district's activities account. She would prepare bank deposit slips reflecting the correct amount of cash and checks received, but later she prepared a second set of fraudulent deposit slips that only accounted for the checks, while she kept the cash. The loss to the school district is estimated to be more than $100,000.
(Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Labor Union Official Sentenced To Prison For Embezzling $12,000+ - April 12, 2024
Jason Weaver used his position as Secretary / Treasurer of the American Postal Workers Union, Local 1509 to write out a check for $352.62 to himself. The check was written from the unions bank account. Weaver signed his name as an authorized account signatory and forged the name of another union officer who was also an authorized account signatory.

Weaver admitted that he knew he was not entitled to the money, and that he deposited the check into his personal bank account.

Weaver further admitted that he used his position with Local 1509 to embezzle a total of $12,396.78 union funds, including issuing 17 union checks to himself and misusing the union's credit card 59 times, from at least April 25, 2016, through November 13, 2021. Weaver repaid $9,500 of that total before pleading guilty to the embezzlement offense. (Source)

BANKING / FINANCIAL INSTITUTIONS

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)

Former Bank Manager Charged For Embezzling $250,000+ From Customers Accounts / Used Funds To Make Payments For House & Car - April 16, 2024

Eric Schouest was employed at Regions Bank from 2010 to 2021 as a Branch Banager overseeing business transactions and practices at the Regions Bank Plank Road branch in Louisiana.

Beginning in or about 2020, and continuing through in or about April 2021, Schouest embezzled funds from customer accounts and deposited the money into his personal bank accounts. Schouest would also send false and fraudulent emails and forged documents to other Regions Bank employees to conceal his scheme. Schouest used some of the traceable fraudulent funds to make loan payments on personal items such as a house and a car. Through his scheme, Schouest caused a loss to Regions Bank of more than $250,000. (Source)

Armored Truck Company Employee Pleads Guilty To Stealing $220,000+ Of Cash For ATMs - April 26, 2024

Justin Eskridge admitted he took more than $220,000 from PNC ATMs. Eskridge was employed as an Armed Service Technician for Loomis LLC and delivered cash for and to federally insured financial institutions. Loomis contracted with PNC Bank to transport money to various ATMs and bank branches.

Eskridge was employed with Loomis beginning in July 2021 and transported bags of money by armored vehicle to various PNC branches and ATMs. The thefts began around Dec. 14, 2022, and continued through Jan. 9, 2023.

PNC bank tellers reported shortages totaling approximately $226,000 cash when they balanced the residual amounts on certain ATMs. An investigation by Loomis identified Eskridge as the technician servicing that route. Eskridge eventually admitted to Loomis that he had taken the money and led Loomis to recover approximately $144,000 cash hidden in his car. As part of his plea, he will pay the remaining balance to Loomis. (Source)

Credit Union Manager Pleads Guilty To Embezzling $200,000+ Causing Credit Union To Fail - April 23, 2024

Gloria Hall was employed at Prairie View Federal Credit Union (PVFCU) in Texas.

From 2017 through 2019, while acting as manager, Hall purposefully maintained an antiquated business practice which would not allow customers to access their accounts online. Hall admitted she was able to and did access at least two elderly customer accounts and misappropriated $211,563.12 of their funds for her own personal gain.

PVFCU was one of the oldest continually operational federal credit unions a historically black college or university had established in the United States.

It did not survive Hall's embezzlement. PVFCU existed for approximately 85 years prior to its failure and merger with the Cy-Fair Federal Credit Union in early 2022. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

AIG Insurance Sues Former Senior Executives Who Launched Rival Insurance Company For Stealing Trade Secrets - April 3, 2024

Global insurance company American International Group (AIG.N), opens new tab sued three of its former senior executives on Tuesday in U.S. court, accusing them and their newly formed rival Dellwood of unlawfully using confidential AIG information to conduct business.

AIG's lawsuit, filed in federal court in New Jersey, alleges unfair competition and claims Dellwood is benefiting from unlawful misappropriation of trade secrets and confidential information.

The lawsuit said Dellwood's management team was using AIG information to solicit its current and prospective customers.

The other defendants are Dellwood CEO Michael Price, who previously served as chief executive of AIG's North America general insurance business; Kean Driscoll, now serving as Dellwood's president and chief underwriting officer; and Thomas Connolly, who is Dellwood's chief financial officer.

Price left AIG in June 2023, and Driscoll departed the company in March, according to AIG's lawsuit. AIG's lawsuit said Price and Driscoll were parties to agreements with AIG that impose upon them post-employment contractual obligations. (Source)

Hedge Fund Firm Accuses Former Employees Of Stealing Trade Secrets - April 12, 2024

Millennium Management, one of the world's largest hedge fund firms, was sued by rival Jane Street Group, which accused it of stealing a valuable in-house trading strategy after two traders defected.

Jane Street said the traders Douglas Schadewald and Daniel Spottiswood had been intimately involved in developing the strategy before resigning separately to join Millennium in February 2024.

It said the theft became apparent when its profit from the strategy plunged more than 50% almost immediately after Schadewald left. Jane Street said it built the trading strategy to take advantage of inefficient markets.

The lawsuit seeks compensatory and punitive damages for causing severe and irreparable harm through the egregious misappropriation of closely guarded trade secrets, which allegedly violated the traders' confidentiality agreements. (Source)

True Velocity Sues Sig Sauer Guns Alleging Employee Stole Trade Secrets - April 17, 2024

True Velocity Ammunition and sister company Lone Star Future Weapons sued gunmaker Sig Sauer, alleging the company stole trade secrets to obtain an unfair competitive advantage.

The companies are competing against each other to produce the U.S. Army's Next-Generation Squad Weapon (NGSW) worth an estimated $4.5 Billion. Sig Sauer won that competition in April 2022. Those first weapons from Sig Sauer were delivered to soldiers from the 101st Airborne Division at Fort Campbell, Kentucky in March of 2024

Lone Star originally teamed with General Dynamics Ordnance & Tactical Systems (GDOTS) in 2021 for the NGSW competition, where GDOTS transferred its technical data and marketing materials to Lone Star. Lone Star then took over as the prime contractor in the NGSW competition and further design activities of the program.

True Velocity and Lone Star are claiming that Sig Sauer misappropriated trade secrets by aggressively recruiting GDOTS employees who had spent years designing and developing these technologies and obtaining crucial and highly confidential design data. (Source)

Former Vice President Of Company Accused Of Disclosing Trade Secrets To Competitor - April 19, 2024

CesiumAstro alleges in a newly filed lawsuit that a former executive disclosed trade secrets and confidential information about sensitive tech, investors and customers to a competing startup company called Any Signal.

Cesium develops active-phased array and software-defined radio systems for spacecraft, missiles and drones. While phased-array antenna systems have been used on satellites for decades, Cesium has considerably advanced and productized the tech over its seven years in operation. The startup has landed more than $100 million in venture and government funding, which it has used to develop a suite of products for commercial and defense customers.,

According to the suit, filed by Cesium, the former Vice President (Erik Luther) misappropriated trade secrets and confidential information on investors and customers, and subsequently disclosed to AnySignal. Notably, Luther did not leave Cesium to work for AnySignal, instead taking a role as head of marketing at a company that operates in a different sector entirely. But the suit says that Luther maintained "personal connections" with AnySignal's co-founders, having worked with AnySignal CEO John Malsbury previously at a different company. (Source)

CHINESE ESPIONAGE / THEFT OF TRADE SECRETS INVLOVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

Anesthesiologist Working At Surgical Center Convicted Of Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - April 12, 2024

Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

Between May and August 2022, numerous patients at Surgicare North Dallas suffered cardiac emergencies during routine medical procedures performed by various doctors. About one month after the unexplained emergencies began, an anesthesiologist who had worked at the facility earlier that day died while treating herself for dehydration using an IV bag.

In August 2022, doctors at the surgical care center began to suspect tainted IV bags had caused the repeated crises after an 18-year-old patient had to be rushed to the intensive care unit in critical condition during a routine sinus surgery.

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

Ortiz surreptitiously injected IV bags of saline with epinephrine, bupivacaine and other drugs, placed them into a warming bin at the facility, and waited for them to be used in colleagues' surgeries, knowing their patients would experience dangerous complications.

Surveillance video introduced into evidence showed Ortiz repeatedly retrieving IV bags from the warming bin and replacing them shortly thereafter, not long before the bags were carried into operating rooms where patients experienced complications. Video also showed Ortiz mixing vials of medication and watching as victims were wheeled out by emergency responders.

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

Oncology Practice, Physicians & To Pay $4 Million+ To Settle False Claims / Kickback Allegations - April 3, 2024

Oncology San Antonio, PA and its affiliated physicians have agreed to pay $1.3 million, and CorePath Laboratories, PA has agreed to pay $2,746,275.22 plus accrued interest, in civil settlements with the United States and the State of Texas to resolve alleged violations of the False Claims Act.

The United States alleged that Oncology San Antonio, a hematology and oncology practice, entered an unlawful kickback arrangement with CorePath Laboratories, a San Antonio-based diagnostic reference laboratory, in August 2016.

CorePath Laboratories provided in-office bone marrow biopsy services at Oncology San Antonio practice locations and performed subsequent diagnostic testing on the biopsies. According to the United States, CorePath Laboratories agreed to pay $115 for each biopsy referred by Oncology San Antonio and its physicians. The payments for each referred biopsy were paid to the private practice entities of three Oncology San Antonio physicians.

The civil settlement with Oncology San Antonio and its physicians also resolves allegations that Dr. Jayasree Rao, through Oncology San Antonio and her own oncology and hematology practice entity, provided medically unnecessary tests, services, and treatments to Medicare, TRICARE, and Texas Medicaid beneficiaries in the

San Antonio Metro Area, and billed the federal healthcare programs for the medically unnecessary tests, services and treatments. (Source)

Former Health Insurance Coverage Supervisor Sentenced To Prison For Embezzling $920,000+ / Used Funds For Shopping, Casino Gambling & Vacations - April 3, 2024

Yolanda Brooks was employed by a company as a Medicaid Supervisor from December 16, 2005, until July 2, 2020. She processed medical insurance claims on behalf of Medicare, Medicaid, and commercial insurance companies.

In March and July of 2018, Brooks opened two personal bank accounts at Key Bank in her maiden name, Yolanda Mohid. The address listed for both accounts was Brook's personal residence in Indianapolis. Other than the introductory title of Yolanda Mohid on each account, the account names were similar to the names of clients of the compay she worked at.

Between March 22, 2018, and July 23, 2021, Brooks took approximately 486 checks mailed to her company in the total amount of $920,148.51 and deposited them into her two personal bank accounts.

Brooks falsely represented to the bank that she was authorized to negotiate said checks and deposit them into her personal accounts.

Brooks used the stolen money for her own personal purposes, including shopping at Victoria's Secret, casino gambling, and luxury vacations. (Source)

Former Hospital Manager Sentenced To Prison For Stealing $607,000+ / Used Funds For Personal Purchases & Casinos - April 3, 2024

While employed as a Rehab Manager for a local hospital and medical group, Timothy Gilbert used a corporate credit card to make unauthorized purchases of prepaid credit cards and gift cards. He would then convert funds from the fraudulently obtained cards using his personal PayPal, Stripe, and bank accounts to conceal his scheme, make personal purchases, and withdraw large amounts of cash to gamble at casinos.

Gilbert concealed the credit card payments from his employer by circumventing company policies. Between 2019 and 2022, Gilbert stole and laundered over $607,000. (Source)

Former Hospital Administrator Pleads Guilty In $200,000+ Identity Theft Scheme / Used Fake Identity For 30 Years - April 1, 2024

Matthew Keirans, a former Iowa hospital administrator. who lived under a false identity for more than 30 years and caused the false imprisonment of his victim pled guilty in federal court.d identity theft.

Evidence presented at hearings in the case established that Keirans and his identity theft victim worked together at a hotdog cart in Albuquerque, New Mexico, in the late 1980s. Keirans assumed the victim's identity and, for the next three decades, used that identity in every aspect of his life. Keirans obtained several false documents in the victim's name, including a Kentucky birth certificate.

In 2013, Keirans obtained employment as a high-level administrator in an Iowa City hospital.

Keirans provided the hospital with false identification documents during the hiring process, including a fictitious I-9 form, social security number, date of birth, and other identification documents in his victim's name.

After getting hired, Keirans worked for the hospital remotely from his residence in Wisconsin. Keirans' access to, and roles in, the system architecture of the hospital's computer infrastructure were the highest it could be, and Keirans was the key administrator of critical systems.

Between August 2016 and May 2022, Keirans repeatedly obtained vehicle and personal loans from two credit unions in the Northern District of Iowa using the victim's name, social security number, and date of birth. Keirans obtained eight loans with a total value of over $200,000 from the credit unions.

Keirans also maintained deposits at a national bank. In 2019, the victim, who was homeless at the time, entered the branch of the national bank in Los Angeles, California, and told a branch manager that he had recently discovered that someone was using his credit and had accumulated large amounts of debt. The victim stated that he did not want to pay the debt and wished to close his accounts at the bank. The victim presented the bank with his true social security card, as well as an authentic State of California identification card. Due to the large amount of currency in the accounts, the branch manager asked the victim a series of security questions, which the victim was unable to answer. The national bank then called the Los Angeles Police Department (LAPD).

LAPD officers spoke with Keirans on the telephone, who stated he lived in Wisconsin and did not give anyone in California permission to access his bank accounts. After faxing the LAPD a series of phony identification documents, the LAPD arrested Keirans' victim on two felony charges. The victim was charged in Keirans' name and held without bail at the Los Angeles County Jail.

In the ensuing months, Keirans contacted the LAPD and Los Angeles District Attorney (LADA) numerous times requesting updates on the victim's prosecution. Meanwhile, Keirans' victim continued to assert throughout the California criminal proceedings that he was not Keirans.

A California state court judge ultimately found Keirans' victim was not mentally competent to stand trial and ordered Keirans' victim to a California mental hospital. The California state court also ordered Keirans' victim to receive psychotropic medication.

After his release from jail and hospital, Keirans' victim made numerous attempts to regain his identity. For his part, Keirans continued to make false reports and statements to law enforcement officials in Wisconsin and California.

In January 2023, after learning where Keirans was employed, the victim contacted the Iowa City hospital's security department about Keirans.

The hospital referred Keirans' complaint to a local law enforcement agency, which assigned an experienced detective to investigate the victim's complaint. The detective conducted an investigation and, over the course of the ensuing months, unraveled Keirans' identity theft scheme.

Among other things, the detective obtained DNA evidence that conclusively proved that Keirans was not the son of an elderly man in Kentucky, as Keirans had claimed, but that Keirans' victim was the man's son. (Source)

Hospital Nurse Sentenced To Prison For Stealing Pain Medication From 50 New Mothers For Her Drug Use Problem - April 1, 2024

Christina Hovey, is an Iowa nurse who stole pain medication from at least 50 new mothers at a hospital.

From January 2022, to March, 2022, Hovey used her nursing license to gain access to controlled substances in the hospital's labor and delivery unit. Instead of administering the controlled substances to the women in pain, Hovey diverted the controlled substances to herself for her own illicit drug use. Hovey admitted she stole narcotics from no less than 50 victims.

In order to cover up her crimes, Hovey used a variety of fraudulent means, including falsely documenting that she had administered pain medication to new mothers when she had not done so.

Hovey also admitted to tampering with pain medication, replacing fentanyl inside a vial with saline and diverting the narcotic for her own use.

Hovey admitted that she routinely drank alcohol and used marijuana while working at the hospital. In order to pass a drug test at the hospital, Hovey injected another person's urine into her bladder. In September 2021, after receiving reports that Hovey was disappearing from her shift for extended periods of time, the hospital's director referred Hovey to an employee assistance program. On September 9, 2021, however, Hovey took a leave of absence from the hospital for about three months after she was arrested for drunk driving. Her blood alcohol level at the time of her arrest was no less than .274.

In July 2022, Hovey entered into a settlement agreement with the Iowa Board of Nursing under which she agreed to voluntarily surrender her nursing license for one year. As a part of her plea agreement, Hovey has now forfeited her nursing license to the United States. (Source)

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

Former Law Firm Paralegal Sentenced To Prison For Embezzling $600,000+ From Bankruptcy Estate Funds Over 9 Years - April 3, 2024

Becky Sutton fraudulently embezzled $600,000+ from 2009 to 2018 while working on bankruptcy matters at the law firm.

Sutton embezzled money from more than 40 bankruptcy estate accounts and several liquidating trust accounts in Chapter 7 and Chapter 11 matters on which she worked.

Sutton orchestrated fraudulent transfers of bankruptcy funds from fiduciary bank accounts intended for creditors to accounts she controlled, including her personal bank account, credit card account, student loan account, and mortgage account. In one instance, Sutton listed a company with a name similar to a true creditor to disguise her fraudulent diversion of the funds. Sutton's conduct victimized not only the creditors, but also her law firm, a partner at the firm for whom she worked, and the U.S. Trustee Program, among others. (Source)

Company Account Charged With Stealing $64,000+ - April 26, 2024

From June 2020 through October 2021, Jason Pick worked as an accountant for his company. His company manages residential and commercial real estate in the New Orleans area.

During his employment, Pick stole approximately $64,137.00 from his company by altering the face of money orders intended to be rent payments from tenants and deposited the altered money orders into his own bank account. While awaiting sentencing for a scheme to defraud his previous employer, Pick submitted a fraudulent letter from his company to a federal judge. The letter was intended to delay his prison report date so he would have more time to make fraudulent changes in hsi company's accounting system, thereby concealing his scheme to defraud his company. (Source)

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

Former Office Manager Sentenced To Prison For Embezzling $8.5 Million+ / Used Funds For Lavish Lifestyle - April 8, 2024

Between 2015 and 2020, Sonya Hesenius was employed as an Office Manager and Executive Assistant at a company in Alpharetta, Georgia. The company provides third-party yard management services.

During her employment, Hesenius made fraudulent charges on corporate credit cards and caused the company to reimburse her personal credit card for personal expenses. To conceal her scheme, she coded and approved all the charges herself, withheld supporting documentation from the company, and disguised the unauthorized expenditures in the company's accounting system as legitimate expenses such as newspaper advertisements. Hesenius further spread the expenditures among different job sites to further conceal the fraud.

Hesenius used the fraudulently obtained funds to live a lavish lifestyle, resulting in staggering losses to her employer.

Her fraudulent activities included company expenditures for: **(1)** more than $172,000 on her daughter's wedding; **(2)** more than $600,000 at Saks Fifth Avenue on items such as designer handbags; **(3)** over $460,000 for herself, family members, and friends to travel all over the world; **(4)** flying herself and her family on private jets to vacations in France, Greece, Hawaii, and Turks and Caicos, totaling more than $145,000; **(5)** tickets to attend University of Tennessee sporting events, the Kentucky Derby, the Masters, the Stanley Cup Finals, and various concerts, totaling more than $238,000; **(6)** a recreational vehicle costing more than $100,000, using $40,000 of company money as a down payment; **(7)** hundreds of thousands of dollars on high-end furniture; **(8)** plastic surgery and dental expenses; and **(9)** conversions of company funds into cash through over $1 million in PayPal, Venmo, and Square transfers to herself and family members. In total, Hesenius embezzled $8,614,729.37 over the course of the fraud scheme. (Source)

Company Financial Controller Pleads Guilty To Embezzling $1.5 Million+ / Used Funds For Gambling - April 23, 2024

Lawrence Malachefski oversaw a staff of other financial professionals as the financial controller and was trusted to independently initiate money transfers between the HVAC company's bank accounts.

From March 21, 2023, to May 18, 2023, investigators say Malachefski embezzled $1,586,557.45 from the HVAC company's accounts to his personal account.

Once in his personal account, officials say Malachefski gambled the money on various gambling sites such as FanDuel, Barstool Sports, DraftKings, and Unibet. (Source)

General Manager For A/C, Appliance, Plumbing & Repair Business Sentenced To Prison For Role In Embezzling $400,000+ From Senior Citizens / Used Money For Personal Expenses, Vacations - April 24, 2024

Victoria Zerillo was sentenced to prison for wire fraud, for her embezzlement of funds from a senior citizen residential community.

Zerillo was employed as a General Manager of a non-profit organization that provided HVAC, appliance, and plumbing repair services to members of a senior citizen residential community. From December 2015 through November 2022, Zerillo and others conspired to commit wire fraud and embezzled more than $400,000 from the non-profit by creating false and fraudulent bank statements and destroying records. Zerillo spent the money on personal expenses, including luxury vacations. At sentencing, members of the senior citizen community testified that Zerillo's embezzlement significantly harmed them financially. (Source)

Company Bookkeeper Sentenced To Prison For Role In Embezzling $400,000 / Used Funds To Pay Morgtgage, Vacations, Etc. - April 26, 2024

Jodi Hamrick conspired with David Gluth, the co-owner of Gluth Contract Flooring, to steal from the company and defraud the silent partner who had put up the money for the business. Hamrick and Gluth carried out the scheme by embezzling more than $400,000 from the commercial flooring business. Between 2011 and 2016, Gluth and Hamrick raided the company accounts to pay for everything from a home mortgage, to luxury vacations, to Nordstrom bills.

The two not only raided company funds, they also defrauded financial institutions by taking out loans without the knowledge or permission of the company's co-owner. The two used the company funds for a variety of personal expenses.

The lies and deceit in this scheme involved forged signatures, forged documents, altered records, secret bank accounts, secret credit cards, false bookkeeping entries, and false statements in declarations and court filings. The evidence in the case included years of Skype instant messages between Hamrick and Gluth, showing the planning and execution of the fraud in minute detail. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Trucking Company Service Manager Pleads Guilty To Embezzling $1.3 Million+ From Employer Using Fake Company - Invoice Scheme - April 4, 2024

Leon Keener was employed as a Service Manager at an interstate trucking company from 2011 to 2022. In his role, Keener had managerial oversight for the financial operations at his companys location.

Beginning in 2015 through 2022, Keener knowingly devised and participated in a scheme to embezzle $1,314,633 from his employer.

Keener was responsible for providing vehicle owners and insurance companies with estimates on repair work costs on damaged vehicles. He also provided insurance companies with supplemental repair estimates discovered during the repair process, after the original estimate had already been provided.

If the insurance company denied reimbursement of some portion of the claim, his company would write off the repair cost as a loss. As manager, Keener had the authority to write off repairs and create purchase orders in his companys accounts payable system.

Keener used his managerial authority to embezzle funds from the company by misappropriating more than $562,000 in reimbursement checks from insurance companies to cover supplemental vehicle repair costs.

Keener then deposited the insurance check into a personal bank account under his control. He concealed the embezzlement by directing his employees to provide him directly with any checks received from insurance companies, cutting out the administrative and accounting employees staff at his company.

Keener also embezzled $751,000 from the company by generating and submitting false vendor payment requests, which he diverted for his own use and benefit. Many of these bogus requests for vendor payments were for a shell company he created and controlled called CR Services, which he added to his companys accounts payable system in 2012, before the system required verified vendor identification. (Source)

Former Employee Charged For Embezzling $1 Million+ From Employer For 11 Years Using Fake Company Scheme - April 11, 2024

From October 2009 and continuing until May 2020, Kennith Moore committed wire fraud by engaging in a scheme to embezzle $1,145,800 from his employer. Moore caused his employer to issue checks to him and to KBM Solutions, a company Moore created whose primary purpose was to receive the embezzled funds.Moore laundered money by transferring the embezzled funds to his personal checking, personal savings, and credit card accounts. (Source)

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

Former Public School Information Technology Manager Sentenced To Prison Damaging School's Computer Network / Phone Systems After Being Terminated - April 2, 2024

Conor LaHiff was employed as a desktop and network manager at a public high school until he was terminated in June 2023.

After he was fired, LaHiff used his administrative privileges to deactivate and delete thousands of Apple IDs from the school's Apple School Manager account, the software that used to manage student, faculty and staff information technology resources. LaHiff also deactivated more than 1,400 other Apple accounts and other IT administrative accounts and disabled the school's private branch phone system, which left the school's phone service unavailable for approximately18 hours.After his termination for the charged conduct, LaHiff had obtained a similar position at another public high school. (Source)

2 Former Employees Fof Non-Profit Mental Health Treatment Provider Sentenced To Prison For Sabotaging Network After Leaving Organization - April 10, 2024

Nathan Howe and co-conspirator Patrick Edmonds-Morin were employed by the non-profit until April 2021 and October 2020.

Between September and December of 2021, Howe conspired with Edmonds-Morin to access records of the non-profit's employees, listen to and view conversations between the employees, and create and deploy a computer program designed to impede the non-profit's use of the network.

In November 2021, Howe accessed the computer network and transmitted a command that shut down the network for the non-profit's Westborough campus where individuals were receiving in-patient treatment.

By shutting down the network, Howe made the non-profit's electronic medical records system inaccessible at its sites across Massachusetts, impairing or potentially impairing the medical examination, diagnosis, treatment and care of patients.

Additionally, between July 2018 and November 2020, Howe and Edmonds-Morin conspired to commit wire fraud by obtaining cell phones from a cell phone provider which were intended for the non-profit's staff and, instead, selling the cell phones to third parties for personal profit, typically in the amounts of hundreds of dollars per phone. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Airline Employee Among 6 Arrested In $22 Million+ Airport Gold Robbery- April 17, 2024

6 people have been arrested in last year's multimillion-dollar gold heist at Toronto's Pearson International Airport according to police in Canada.

On April 17, 2023, an air cargo container carrying more than $22 Million Canadian dollars' worth of gold bars and foreign currency, was stolen from a secure storage facility using fake paperwork, police say. The gold and currency had just arrived on an Air Canada flight from Zurich, Switzerland.

At least 2 former Air Canada employees allegedly helped in the audacious theft, police say. One is now in custody and an arrest warrant has been issued for the other.

Canadian and U.S. officials say the investigation is ongoing and only a fraction of the stolen gold bars and cash has been recovered.

Police say after executing a search warrant in Ontario, they found five crudely melted gold bangles worth about $90,000. "This was the largest gold heist in Canadian history, reportedly, it's the sixth largest in world crime history," said Deputy Police Chief Nick Milinovich. (Source)

Former Augusta National Golf Club Employee Charged With Stealing Millions In Gold Tournament Memorabilia For 13 Years - April 18, 2024

A former employee of Augusta National Golf Club in Georgia is set to plead guilty in federal court to charges of stealing and transporting millions of dollars worth of merchandise and memorabilia from the Masters tournament. Richard Globensky is accused of transporting stolen goods across state lines to Tampa, Florida, between 2009 and 2022.

Globensky is a former warehouse coordinator at Augusta National who was in charge of overseeing the vast array of Masters merchandise and memorabilia sold annually.

Real estate records show Globensky and his wife sold their lavish home in nearby Evans, Georgia, for just over $2 Million last year, a year after the alleged scheme ended. The six-bedroom, 7,300-square-foot home featured an in-ground pool and outdoor putting green. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

City Employee Working As Mail Clerk Pleads Guilty To Role In Stealing $600,000 - April 22, 2024

Beginning in 2017, Brandon Santanoo worked as a clerk in the mail room at the Law Department's office in Brooklyn. By virtue of his position, Santanoo had access to mail that was sent to the Law Department.

From at least in or about June 2021 through at least in or about May 2023, Santanoo stole checks that had been mailed to the Law Department, including checks made payable to the Law Department's Worker's Compensation Division, which is responsible for administering claims of city employees who are injured on the job.

Santanoo then passed those checks onto other people, who deposited or attempted to deposit forged, altered, and fraudulently endorsed versions of those checks into third parties' bank accounts. Approximately 40 checks, totaling approximately $600,000, were stolen and deposited or attempted to be deposited as part of the scheme. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Assistant Director Of Nursing At Medical Rehabilitation Center Sentenced To Prison For Removing / Tampering With Patients Morphine Medications - April 4, 2024

Sarah Diamond was employed as the Assistant Director of Nursing at a Chicago-area medical rehabilitation center, where she was responsible for dispensing medications to patients, including those in hospice care.

In the summer of 2021, Diamond removed morphine from bottles that had been prescribed to at least five patients to manage their pain and replaced it with another liquid, knowing the diluted substance would be dispensed.

Diamond removed the morphine for her own personal use and with reckless disregard and extreme indifference for the risk that the patients would be placed in danger of bodily injury.

In at least one instance, a patient's family members observed the patient suffering during what would end up being some of the final moments before dying. (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

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)

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.

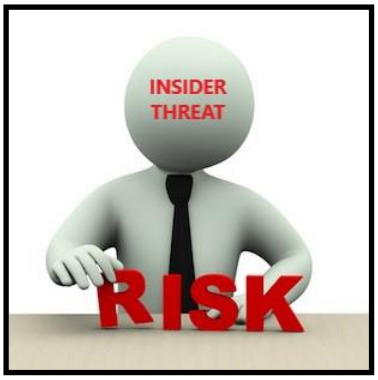
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

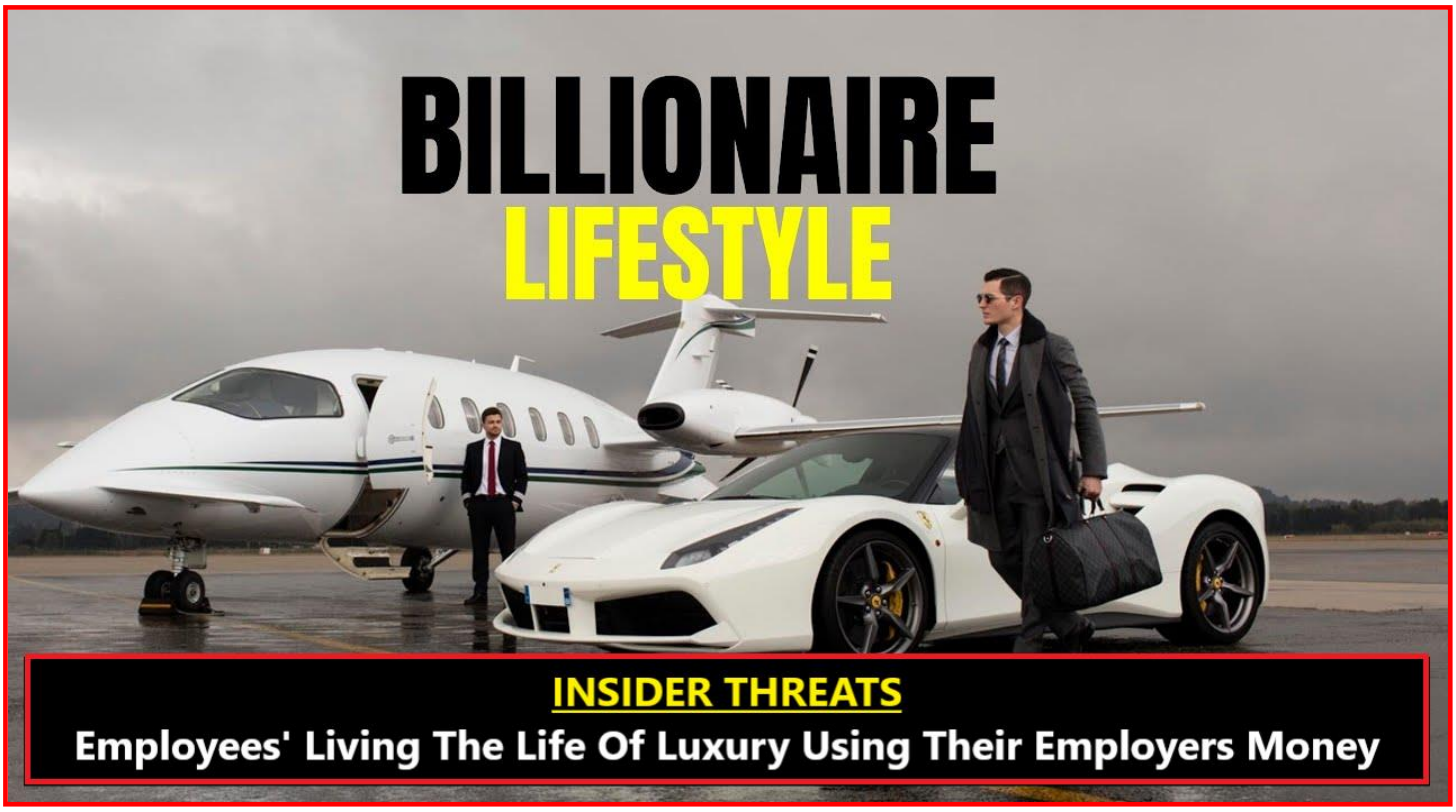
- ☐ Bribery, Extortion, Blackmail

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 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)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

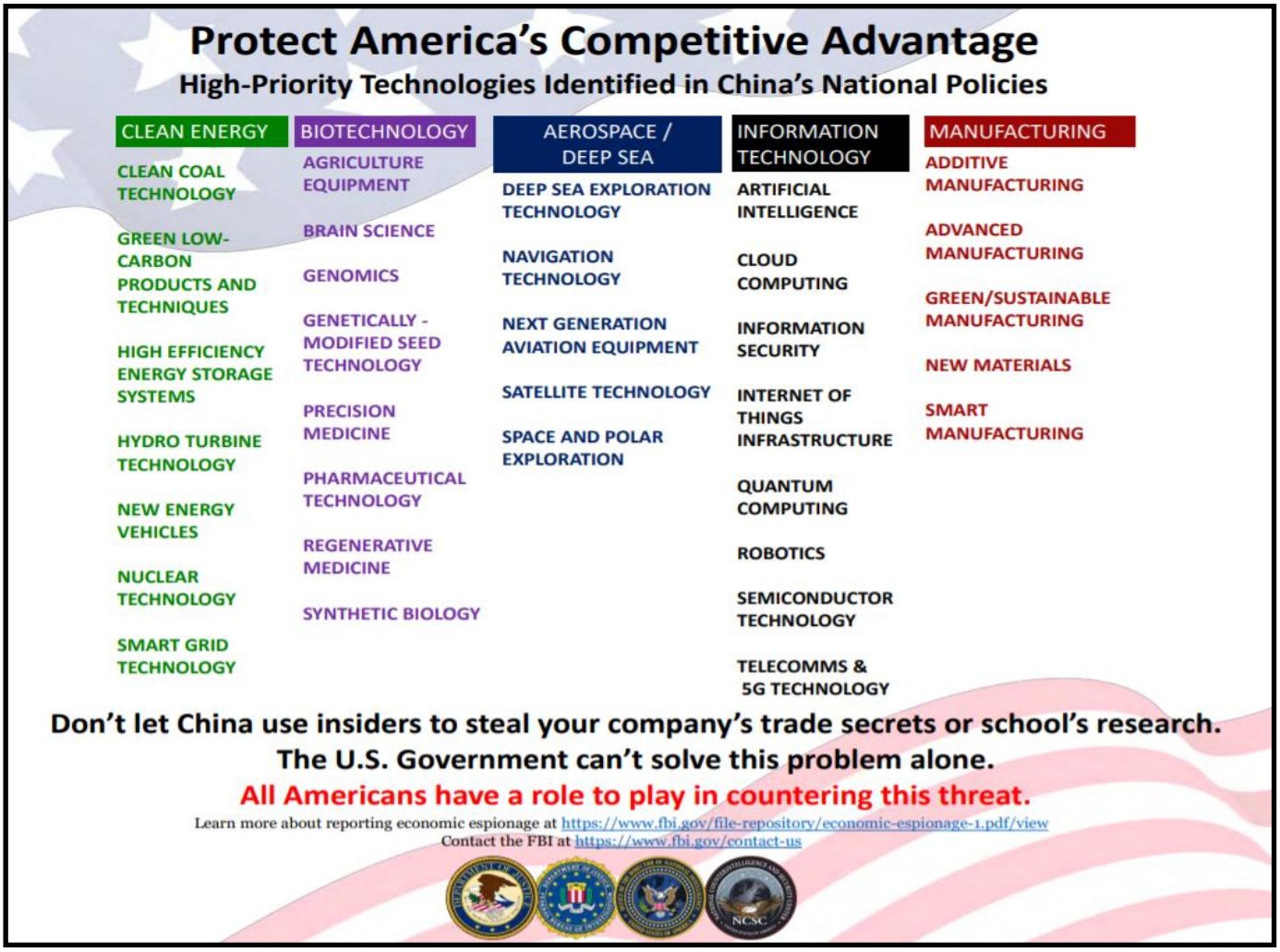
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

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



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,000+ 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

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The NITSIG has been successful in bringing together Insider Risk Management (IRM) professionals and other security professionals from the U.S. Government, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM.

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

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

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

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

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

The NITSIG had to cancel ITS&E events for a few years due to COVID. We are in the process of planning our next ITS&E.

NITSIG Insider Threat Mitigation Resources

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

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Is Our Business

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 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. (Training Brochure)

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 Specialist
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
LinkedIn NITSIG Group

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