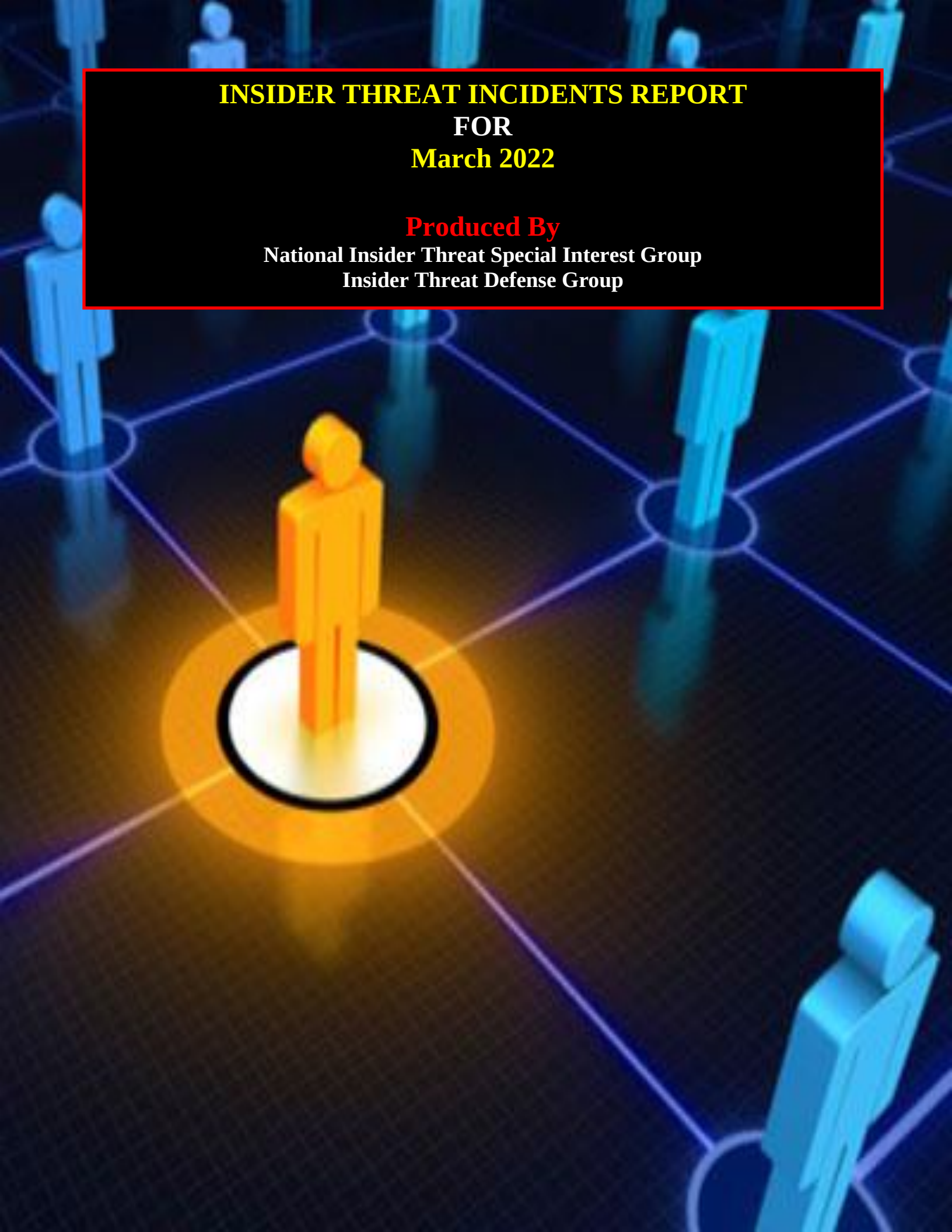

INSIDER THREAT INCIDENTS REPORT
FOR
March 2022

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **3,500+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

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

According to the Association of Certified Fraud Examiners 2020 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most 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.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 21 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

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 CC2 & 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
- ☐ Theft Of Organizations Assets
- ☐ 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 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

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 / Airline Industry (Pilots, Flight Attendants)
  - 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)
- ☐ And Others

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR MARCH 2022

U.S. GOVERNMENT

Former Post Office Manager & 2 Co-Conspirators Charged In Conspiracy Involving Theft Of $1.7 Million In Checks From Mail - March 9, 2022

James Lancaster was the former Manager of Customer Service at the Indianapolis' New Augusta Post Office. He has been charged with conspiracy to commit bank fraud and theft of mail.

Lavaris Yarbrough and Jordan McPhearson were charged with bank fraud and conspiring with Lancaster to commit bank fraud.

Between May 11, 2020, and June 23, 2021, Lancaster stole checks from the mail. Lancaster gave the stolen checks to McPhearson, sometimes receiving cash in exchange. McPhearson fraudulently negotiate the stolen checks, depositing them into an account belonging to someone other than the intended payee. Occasionally, McPhearson provide stolen checks to Yarbrough who fraudulently negotiate them.

Throughout the course of the conspiracy, Lancaster stole more than 270 pieces of U.S. mail from the New August Post Office. This mail contained checks from more than 50 different local businesses. In total, the value of the stolen checks was around $1.7 million. (Source)

Former IRS Employee Arrested For Assisting In Preparation Of $191,000+ False Tax Returns, Identity Theft - March 25, 2022

Fredrick Louis served as a "ghost preparer," meaning that he prepared tax returns for compensation but failed to sign or otherwise declare the tax returns he prepared for other individuals.

Louis worked as a Tax Examiner for the IRS from 1985 to 1994. It is alleged that due to his prior IRS employment, Louis knew that by law individuals who are paid to prepare or assist in preparing tax returns must have a valid Preparer Tax Identification Number (PTIN) and sign and include their PTIN on the returns they prepare. Louis also held himself out to be an accountant who prepared tax returns for pay or as a favor to friends. In actuality, Louis does not have an accounting degree, is not a Certified Public Accountant, and did not have a PTIN.

From at least January 2016 and continuing through at least March 2021, Louis prepared tax returns that contained false Schedule C business expenses, false Schedule F farming expenses, false Schedule A itemized deductions, claimed false dependents, and / or claimed false filing statuses on certain tax returns to generate fraudulent inflated tax refunds to which the taxpayer clients were not entitled. It is further alleged that Louis allocated portions of the refunds to himself, often unbeknownst to his client by directing the fraudulently inflated refunds be direct deposited in one of the following ways: (1) the entire refund was sent to Louis or (2) some portion of the refund was sent to bank accounts owned or controlled by Louis. As a result of the scheme, the IRS issued over $191,000 in fraudulent federal income tax refunds. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

National Security Agency Employee Charged For Willful Transmission And Retention Classified Information Using His Personal E-Mail Address 13 Times - March 31, 2022

Mark Unkenholz is as an employee of the National Security Agency (NSA). He held a Top Secret / SCI clearance.

On 13 occasions between Feb. 14, 2018 and June 1, 2020, Unkenholz willfully transmitted classified information to another person who was not entitled to receive it. The information transmitted was classified at the Secret and Top Secret / SCI levels. Unkenholz transmitted the classified information using his personal email address to the other person's private company email addresses. The person receiving the information held a Top Secret / SCI clearance from April 2016 until approximately June 2019. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

City School Administrator Found Guilty In $10 Million Virtual Education Fraud Scheme Involving Co-Conspirators - March 21, 2022

A Montgomery, Alabama Athens City Schools administrator, William Carter, was convicted for his role in a scheme to defraud the Alabama State Department of Education (ALSDE).

According to court records and evidence presented at trial, Carter, conspired with other school officials to fraudulently enroll students in public virtual schools and then falsely reported those students to the ALSDE in order to illegally receive additional education funding. Carter's co-conspirators include former superintendent of the Athens City Schools district Dr. William Holladay, David Tutt, Gregory Corkren, and former superintendent of the Limestone County School district Thomas Michael Sisk.

The submission of this false documentation allowed payments to continue from Alabama's Education Trust Fund to the Athens City Schools district and the Limestone County Schools district. Carter and his co-conspirators then received, for their own personal use, portions of the state funding. They skimmed the state money through direct cash payments and payments to third-party contractors owned by the various co-conspirators. During the course of the scheme, the total potential loss was approximately $10 million. (Source)

Former State Employee For Department Of Public Health Sentenced To Prison For $2 Million+ Fraud Scheme That Benefited Families & Friends - March 3, 2022

Schenelle Flores used her employment at the Office of AIDS, within the California Department of Public Health, to coordinate the fraud scheme between December 2017 and November 2018.

Flores's scheme involved directing a state contractor to make payments allegedly on behalf of the Office of AIDS and causing the contractor to charge those payments to the state. As part of the scheme, Flores caused the contractor to pay for personal expenses on its debit cards, order gift cards for personal use, and pay false invoices to shell companies for services allegedly provided to the Office of AIDS. Flores, other participants in the scheme, and their families and friends obtained at least $2 million in personal benefits, including cash, luxury suites at sports games, and vacations. (Source)

Sales Rep Charged In $75,00 Fraud Scheme At Elementary School Involving Principal & Others - March 15, 2022

The alleged fraud at the North Side's Brennemann Elementary School has led to more federal charges, this time for a sales representative for a Chicago Public School (CPS) vendor.

Debra Bannack has been charged with three counts of wire fraud and one count of mail fraud in an indictment by a grand jury. She is accused of participating in a scheme to fraudulently deliver iPhones, iPads and prepaid gift cards to administrators and others at the school for personal use, allegedly cheating CPS out of $75,000.

Already facing charges in federal court are former Brennemann Principal Sarah Abedelal, former business manager William Jackson, and former Assistant Principal Jennifer McBride.

The indictment alleges that Abedelal, Jackson and other CPS employees would order items for their personal use from Bannack and her company, and the company would supply those items. Abedelal, Jackson and other CPS employees would then allegedly submit bogus paperwork claiming to order legitimate supplies like paper, ink and toner; and they would allegedly submit false invoices from Bannack and a colleague seeking payment for those supplies.

Bannack and her unnamed colleague delivered the iPhones, iPads and more than $40,000 in prepaid gift cards to Abedelal and other CPS employees, according to the indictment. All told, Abedelal, Jackson, Bannack and others stole about $75,000 from CPS, it said. (Source)

Former Township Employee Charged With Embezzling $160,000 Of Funds - March 28, 2022

From 2013 through 2017, while Linda Tarlecki was as an employee and Township Supervisor of Conyngham Township.

Tarlecki embezzled approximately $160,000 of township funds. The embezzlement was accomplished in part by Tarlecki writing unauthorized checks to herself from the township's bank account and forging the signatures of other township supervisors on these checks. (Source)

FOREIGN GOVERNMENT ESPIONAGE / INSIDER THREAT PROBLEMS

Former Canadian Government Employee Extradited To United States To Face Charges For Ransomware Attacks Resulting in the Payment Of Tens of Millions of Dollars in Ransoms - March 10, 2022

Sebastien Vachon-Desjardins has been charged with conspiracy to commit computer fraud and wire fraud, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer arising from his alleged participation in a sophisticated form of ransomware known as NetWalker.

NetWalker ransomware has targeted dozens of victims all over the world, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims.

From April through December 2020, conspired to and did intentionally damage a protected computer and transmit a ransom demand in connection with doing so. The indictment also alleges that the United States intends to forfeit more than $27 million, which is alleged to be traceable to proceeds of the offenses.

Canadian law enforcement officers arrested Vachon-Desjardins in Quebec, Canada on Jan. 27, 2021, and executed a search warrant at his home. During the search, officers discovered and seized 719 Bitcoin, valued at approximately $28,151,582 as of today's date, and $790,000 in Canadian currency. (Source)

Former Comptroller General Of Ecuador Charged For Accepting $10 Million+ Bribe To Purchase / Renovate Real Estate, Purchase Restaurants, Dry Cleaner & Other Businesses - March 29, 2022

Carlos Ramon Polit Faggioni (Polit) is the former Comptroller General of Ecuador. He allegedly engaged in a scheme to use the U.S. financial system to launder money to promote and conceal an illegal bribery scheme in Ecuador.

Between approximately 2010 and 2016, Polit allegedly solicited and received over $10 million in bribe payments from Odebrecht S.A., a Brazil-based construction company. This was in exchange for using his official position to influence official actions by the comptroller's office in order to benefit Odebrecht and its business in Ecuador. Polit is alleged to have received a bribe from an Ecuadorian businessman in or around 2015 in exchange for assisting the businessman and his company in connection with certain contracts from the state-owned insurance company of Ecuador.

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 certain associates, often without the associates' knowledge. The conspirators also used funds from Polit's bribery scheme to purchase and renovate real estate in South Florida and elsewhere and to purchase restaurants, a dry cleaner and other businesses. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Police Officer Sentenced To Prison For $50,000 Fraud Scheme - March 22, 2022

Former St. Louis Metropolitan Police Officer (SLMPD) Brad Stephens to one year and one day in federal prison for 3 counts of Mail Fraud by obtaining taxpayer moneys from the Tower Grove South Concerned Citizen Special Business District (Tower Grove South) by means of material false representations.

Stephens was employed as a police officer by "SLMPD since October 6, 2014.

Tower Grove South was established to provide special police and / or security for the protection and enjoyment of the property owners and the public within the district. The administration and operations of the business district are taxpayer funded. City Wide Security (CWS) is a private company that contracts with businesses and organizations to provide private security patrols. CWS contracted to provide security patrols in the Tower Grove South Neighborhood beginning during 2010.

Stephens was employed by CWS beginning in approximately 2015 to work during some of his off-duty hours to patrol the Tower Grove South Neighborhood. Stephens falsely represented to CWS 169 day and night patrol shifts he agreed to work as part of the CWS security patrol in the Tower Grove South Neighborhood when, in fact, Stephens did not actually work those assigned shifts. During 2018, Stephens falsely represented that he worked 93 days, and during 2019, Stephens falsely represented that he worked 76 days. CWS was paid approximately $50,000 by the Tower Grove South organization based upon Stephens' false representations, all taxpayer funds. (Source)

Former Police Clerk Sentenced To Prison For $29,000 Of Overtime Fraud - March 14, 2022
Marilyn Golisano was a former clerk for the Boston Police Department's (BPD) District A-1 Detectives Unit.

Golisano who handled the overtime paperwork for the unit, submitted dozens of false and fraudulent overtime slips in 2017 and 2018 claiming she had worked extra hours, with many of those slips bearing forged signatures of her supervisor. Although Golisano's work was done primarily on the computer, Golisano never logged into the BPD computer system at all during many of the overtime shifts she claimed to have worked. Furthermore, on several occasions when Golisano was supposedly working overtime in downtown Boston, cellphone location information placed Golisano well outside the city. In total, Golisano stole $11,000 from BPD in 2017 and $18,000 in 2018 as a result of the fraud. (Source)

Las Vegas Police Officer Charged In Casino Robbery - March 10, 2022
A Las Vegas Metropolitan Police Department (LVMPD) officer made his initial appearance in federal court for allegedly robbing a casino.

On February 27, 2022, Caleb Rogers entered a Las Vegas casino. He ran toward two employees in the sportsbook area and yelled: "Get away from the money. I've got a gun. I will shoot you!" Rogers climbed over the counter and shoved one of the employees to the floor, before grabbing money and placing it into a bag.

Rogers fled when the employees triggered an alarm. As Rogers ran toward the parking garage, a casino security officer tackled him. Rogers drew a revolver and, with his finger on the trigger, threatened: "I'm going to shoot you!" Security officers were able to disarm Rogers and restrain him until LVMPD officers arrived. The officers arrested Rogers and seized his firearm. Checking the revolver's serial number, officers learned that it belonged to the LVMPD.

The criminal complaint further alleges that: (a) on November 12, 2021, Rogers robbed a casino in the western part of Las Vegas (obtaining approximately $73,810); and (b) on January 6, 2022, he robbed a casino in North Las Vegas (obtaining approximately $11,500). (Source)

Former Police Chief Charged For Stealing $25,000+ Of Drug Money From Evidence Locker - March 10, 2022
Between February 2020 and February 2021, Jason Cross stole over $25,000 from the police department evidence locker and the city's drug purchase fund. (Source)

State Corrections Officer Arrested For Receiving Bribes From Inmates - February 25, 2022
Cory Young was receiving payments from inmates in exchange for products such as cigarettes. He had been exchanging funds through Cash App between February and May 2020.

Financial records as well as information provided by Cash App parent company Square Inc. show records of funds being transferred from inmates to his account. According to an arrest report, Young received a total of $880 from inmates. (Source)

Former Customs & Border Protection (CBP) Officer Pleads Guilty For Role In Conspiracy To Accept Bribes To Allow Smuggle Goods Into United States - March 8, 2022

Simon MedinaI was a CBP Officer who he admitted he helped others illegally bring commercial goods into the United States from Mexico.

Medina admitted that between May 25 and Aug. 6, 2020, he allowed several individuals to enter the United States with contraband in their vehicles on approximately 20 occasions. Although not assigned to the entry lanes at the Laredo Port of Entry, Medina would open a lane and allow his co-conspirators to pass through without inspecting their cargo. Medina also accepted gratuities from his partners (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee Sentenced To Prison For Stealing $1.7 Million From Her Employer Over 12 Years - March 15, 2022

Between August 2008 and January 2021, Julie Azim who was a long-time employee of a New York bank, stole approximately $1.7 million from her employer. Over the course of approximately 12 years, Azim executed hundreds of wire transfers of the banks funds to co-conspirators and related companies, who then sent portions of the ill-gotten funds to Azim's personal bank account. (Source)

Former Bank Employee Charged In $8 Million Fraud And Bribery Scheme Involving Co-Conspirators - March 15, 2022

From 2013 through 2019, Kurt Phelps and his conspirators carried out a scheme to defraud Phelps' employer, a bank. They obtained millions of dollars of credit from the bank for Starnet Business Solutions Inc. (Starnet), a now-defunct New Jersey based printing company, where Phelps' conspirators worked. Phelps' conspirators paid him large cash bribes in connection with the fraud scheme.

In 2013, Starnet received a line of credit from the bank after providing materially false financial information. The bank not only allowed Starnet to maintain the line of credit, at various times it increased the line of credit. By 2018, the line of credit was worth approximately $8 million, and Starnet has not repaid it.

Phelps was aware that financial information Starnet provided to the bank for the line of credit was materially false, and coached Starnet on how to defraud the bank. Phelps would review draft financial information for Starnet and provide feedback on how his conspirators should falsify the information before submission. Phelps also worked to ensure that the bank did not detect the fraud scheme by helping Starnet avoid audits and other quality control measures employed by the bank.

Phelps solicited large cash bribes – tens of thousands of dollars at a time – from Starnet in connection with the fraud scheme. Phelps's conspirators pooled cash to pay Phelps bribe payments. Over the course of the conspiracy, Phelps accepted hundreds of thousands of dollars in cash bribes. (Source)

Bank Employees Involved In $600,000 Fraud Scheme To Steal Bank Customer Identities To Make Unauthorized Cash Withdrawals - March 7, 2022

Lamar Melhado, was charged with conspiracy to commit bank fraud.

From August 2016 through August 2017, Melhado conspired with Jamere Hill-Birdsong, of Camden, and others, to defraud a Mount Laurel, New Jersey, bank. Hill-Birdsong worked inside the banks's call center and recruited other call center employees to participate in the scheme by stealing the identities and account information of customers who called into the bank's call center.

The conspirator bank employees would then take photographs or screenshots of the bank customers' account information and signatures and would send that information to Hill-Birdsong and Melhado. The conspirators then had phony identification documents made in the names of the bank customers, and used various runners to go into bank branches and make unauthorized cash withdrawals. The conspirators also used the stolen identity information to conduct unauthorized online transfers of monies from the customer's accounts. Hill-Birdsong was indicted in March 2021 on conspiracy to commit bank fraud, bank fraud and aggravated identity theft; those charges remain pending. (Source)

Former Bank Teller Admits To Stealing $144,000+ - March 1, 2022

Ana Amesquita was the head teller at the Inwood branch of City National Bank, in West Virginia.

In June 2019, Amesquita began a scheme to process ATM deposits without the supervision of a second bank employee, violating the bank's policy. She would then take some of the cash for her own personal use and misrepresent the facts in the general ledger. As a part of the plea agreement, Amesquita agreed to pay $144,661 in restitution to the bank. (Source)

Former Bank Employee Sentenced To Prison For Role In 2 Fraud Schemes Involving Co-Conspirators - March 3, 2022

Between approximately June 2014 and November 2018, Rushell Harris engaged in two separate wire fraud conspiracies. In the first conspiracy, Harris exploited her position at Nantucket Bank by obtaining personally identifiable information of a customer and surreptitiously taking photographs of the victim's account information. Harris then shared that information with co-conspirators who attempted to transfer funds out of the customer's bank account without authorization.

In the second conspiracy, Harris helped perpetuate a fraudulent lottery scheme targeting at least 13 victims who were contacted by via phone, informing them that they had won large prizes, and that in order to receive the funds they needed to pre-pay taxes on their winnings. In reality, no such prizes existed. After victims made an initial payment, they were advised that additional advance payments were required for expenses such as insurance, transportation or other international customs' fees. Harris and her co-conspirators transferred proceeds of the scheme to associates in Jamaica and in the United States.

Harris was also ordered to pay restitution in the amount of $161,038 and forfeiture of $90,925. On Oct. 8, 2021, Harris pleaded guilty to two counts of conspiracy to commit wire fraud. (Source)

2 Bank Employees Charged With $165,000+ Fraud And Identity Theft Scheme - March 7, 2022

The Florida Department Of Law Enforcement (FDLE) arrested Tiwuan Williams and Stephon Pugh-Davis.

The investigation began in June 2021 when a local financial institution reported suspected internal fraud being committed by employees Williams and Pugh-Davis.

FDLE agents discovered that Williams recruited other employees, including Pugh-Davis to provide him with customer account details in order to facilitate fraudulent transfers into money mule accounts.

The investigation showed that Williams attempted to facilitate the transfer of more than $165,000 through more than 30 victim accounts, while Pugh-Davis assisted with more than 20 of the fraudulent transfers. (Source)

Former Bank Teller Sentenced To Prison For Embezzling $63,000 Of Customer Funds - March 17, 202
Between December 3, 2018 and December 6, 2019, Demetria Silvio forged approximately 66 checks that were drawn on IberiaBank accounts belonging to five customers. Silvio deposited the fraudulent checks into her own bank accounts with Chase Bank and Capital One. (Source)

Credit Union President Sentenced To Prison For $2 Million+ Of Embezzlement - March 25, 2022
Susan Romero worked for the Winslow Santa Fe Credit Union for more than 30 years, mostly in leadership roles, including as manager, president, and chief executive officer.

During a routine audit, the credit union found discrepancies in the financial records. A subsequent investigation showed that, over the course of many years, Romero embezzled more than $2.2 million from the credit union. Romero admitted that she stole the money through unauthorized cash withdrawals, checks issued with forged signatures of other employees, and transfers from the credit union account to her family members' accounts. She covered her tracks through false entries in the financial statements, such as falsifying the amount of cash stored in the vault and offsetting the stolen money with fictitious assets. (Source)

Former Bank Branch Manager Sentenced To Prison For Stealing $169,000+ Of Social Security Benefits From Account Of Deceased Customer - March 31, 2022
Jeffrey Piecka is former Branch Manager with JPMorgan Chase Bank.

Piecka devised a scheme to steal $169,967.63 in government benefits from the bank account of a deceased individual. Suspecting that the account owner had passed away, Piecka manipulated the bank account to create online account access for himself, and he proceeded to withdraw significant sums of money from the account by various means, including by making online payments to credit card companies, a utility company, his apartment complex, and his car lender. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE & STAFF

Former Insurance Firm Chief Financial Officer (With Help Of Co-Conspirators) Sentenced To Prison In $33 Million Scheme To Steal Client Healthcare Funds - March 28, 2022
Erin Verespy was sentenced to 66 months in prison for her participation in a widespread, $33 Million scheme to misappropriate client healthcare funds and defraud multiple lenders through her role as the Chief Financial Officer of Employee Benefit Solutions LLC (EBS).

A significant amount of purported checks listed on the EBS check register invoices were never actually deposited by the healthcare providers. Instead, approximately $17.87 million in healthcare payments were misappropriated, with the overwhelming majority simply transferred by EBS into its own operating account, where they were used for non-healthcare expenses by the managers and owners of EBS. A review of bank records indicates that the funds were used by Verespy's co-conspirators to pay their home mortgage expenses, as well as a personal credit card account with expenses relating to boating, luxury cars, and golf. Verespy personally made over one million dollars from her participation in the fraudulent scheme. (Source)

Former Medical Clinic Employee & Co-Conspirators Sentenced To Prison For Bank Larceny Of Over $200,000 Using Patient Information Stolen From Clinic - March 18, 2022

Royale Lassai was employed in at a Louisiana medical clinic.

Lassai without authority, obtained personal information of patients including dates of birth, social security numbers and addresses. Lassi then sold the information to her cousin, Ashley Green who used this information to fraudulently obtain debit cards issued by the victim banks. These fraudulently obtained cards were mailed to an address controlled by Green. Green and Brandon Livas then used the cards to withdraw at least $200,000 from the victim's accounts. Lassai was paid at least $1,000 to pilfer the patient's information from the clinic.

Green, Livas and Lassai pled guilty to Bank Larceny. (Source)

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

Former Employee Of Children's Charity Ordered To Pay $4.65 Million+ For Stealing Charity Over 7 Years - March 31, 2022

While Director of Business and Finance at River Valley Child Development Services (RVCDS), Ruth Philips was responsible for all financial operations, including monitoring accounts receivable, creating and submitting invoices, reconciling bank accounts and issuing checks.

Phillips admitted that between December 2013 and August 2020, she stole approximately $4,721,731 from RVCDS. During that period, she sent $1,142,500 to her personal checking account and sent another $3,395,500 to Attitude Aviation's bank account. Attitude Aviation has offices at Lawrence County Airpark in South Point, Ohio, and Tri-State Airport in Huntington and provides aeronautical services, including fueling, rental of hangar space, aircraft rental, flight instruction and maintenance.

Phillips agreed to forfeit substantial assets, including: $601,638.77 in proceeds from the sale of six airplanes, $304,576.49 in proceeds from the sale of a lake house, $169,954.58 in proceeds from the sale of anothe property. Phillips has also agreed to forfeit proceeds from the sale of her residence in Chesapeake, Ohio, and several vehicles, including a Lexus RX and a Chevrolet Corvette. (Source)

Former Newark Housing Authority IT Director Admits Embezzling $594,000+ Funds To Purchase 1,500+ Cell Phone / Tablets Then Resold For Personal Profit - March 31, 2022

Venancio Diaz is the former Director of Information Technology for the Newark N.J. Housing Authority (NHA).

From December 2013 to Aug. 10, 2021, Diaz bought, on behalf of NHA and using NHA funds, 1,509 electronic devices, primarily cellular telephones and tablets, from a telecommunications company. Diaz then caused those devices to be activated on NHA's account on the company's network for a short period of time – often only days or weeks. After the brief period of activation ended, Diaz posed as the owner of the devices and sold them to two different online electronics resale marketplaces. Diaz directed all the proceeds of the sales – a total of $594,425 – to his own bank accounts and kept the money for his own personal use. (Source)

Former Coal Company Vice President Charged In $143 Million Foreign Bribery, Money Laundering And Wire Fraud Scheme - March 31, 2022

A former coal company executive was arrested today on charges of violating the Foreign Corrupt Practices Act (FCPA), laundering funds, and receiving kickbacks as part of an alleged scheme to pay bribes to government officials in Egypt in connection with contracts with an Egyptian state-owned and state-controlled company, Al Nasr Company for Coke and Chemicals (Al Nasr).

Charles Hobson engaged in the bribery and money laundering scheme between late 2016 and early 2020. During part of that time, Hobson was the Vice President of a coal company in Pennsylvania and was responsible for the company's business relationship with Al Nasr.

Hobson and a sales intermediary paid bribes to Al Nasr officials in Egypt to obtain approximately $143 million in coal contracts. Hobson conspired to secretly receive a portion of the commissions paid to the sales intermediary as kickbacks. (Source)

Staples Store Manager Sentenced To Prison For $81,000+ Fraud Scheme Involving Co-Conspirator - March 1, 2022

Ricardo Voltaire was a sales manager at Staples locations in Dedham and Braintree. Voltaire was responsible for processing store credit card applications, among other things.

On at least 60 occasions, Voltaire processed fraudulent Staples' store credit account applications that were submitted by co-conspirator Wagner Sozi and his accomplice, each of which contained stolen personal identifying information of another individual.

Voltaire knew that his co-conspirators were not in fact the individuals named on the applications and opened store credit accounts under the stolen identities, which were then used to purchase more than $81,000 in Visa gift cards. Voltaire accepted approximately $8,000 in kickbacks from Sozi and his co-conspirator. (Source)

Former Office Manager Sentenced To Prison For Embezzling Over $230,000+ From Employer - March 3, 2022

Aurelia Stanton worked as an office manager from approximately June 2014 through May 2017 for a business. She was responsible for ensuring timely payment of bills and invoices, accurate bookkeeping, and managing the office.

From August 2015 through May 2017, she embezzled more than $233,000 writing checks to herself on the company's check stock. She used a computer software program to conceal the fraudulent disbursements by editing the company's bank statements to remove references to the fraudulently drafted, forged, and negotiated checks. In total, she deposited 187 checks with forged signatures. (Source)

Former Employee Sentenced To Prison For Embezzling $429,000+ From Employer / Used Funds For Gambling - March 3, 2022

Carol Broyles admitted that while employed at a small business in Tulsa from January 2012, through October 2016, she devised a scheme to misappropriate the businesses' funds to enrich herself and to pay for personal expenses. She used her access to the company's cash collections to take funds, and she cashed several checks from the company's account.

At sentencing, the victims described the financial devastation incurred because of Broyles' criminal acts. Broyles claimed to have stolen the money to pay for expensive family medical bills, but instead Broyles spent nearly all the money gambling. When Broyles became aware of the criminal investigation and throughout criminal proceedings, Broyles made little to no effort to make any restitution to the victims. (Source)

Former Company Accountant Sentenced To Prison For Embezzling $375,000+ From Employer Over 4 Years - March 14, 2022

Beginning in 2013, Angelo Kanaris worked as an accountant for a Cleveland-area company, where he was responsible for writing checks to the company vendors and preparing sales tax returns.

During this time, Kanaris began writing checks ostensibly on behalf of the company to third-party vendors; however, Kanaris used a mobile deposit feature to deposit these checks into his bank account for personal use. From in or around 2013 through 2017, Kanaris embezzled approximately $375,656.55 from the company while working as an accountant. (Source)

Former Bookkeeper For Construction Company Admits To Embezzling $600,000+ From Her Employer For Shopping & Travel - March 14, 2022

In 2013, M&D Construction, Inc., hiired Nicole Lopez as its bookkeeper. Lopez was given access to the company's business enterprise bank account.

Between 2017 and 2020, Lopez charged more than $600,000 on her personal credit card accounts for mostly consumer shopping and travel. To pay her personal credit card expenses, Lopez directed approximately $611,000 in 72 payments from M&D's business account into her personal accounts without the company's authorization.

Lopez's embezzlement scheme was discovered when she purchased a small boutique clothing store, called Sora & Co., in downtown Great Falls, and resigned from M&D. A new accountant hired to replace Lopez reviewed the books and determined that more than $600,000 was missing. (Source)

Former Chief Business Officer For Financial Technology Company Sentenced To Prison For $500,000 Embezzlement Scheme - March 16, 202

Brooke Solis was an attorney licensed to practice law in the State of California when she was hired by a San Francisco-based financial technology company as its general counsel.

In March, 2019, she was promoted to the position of Chief Business Officer at the company. Solis was given "Super Administrative" privileges within the accounting and expense management programs used by her employer. Solis acknowledged that she used these privileges to defraud her former employer and embezzle money from the company.

One method Solis used to defraud her former employer was by preparing and using fraudulent invoices. She requested payment from her employer to a shell company, The Paralegal Group LLC, that she created and controlled. .

Another method Solis used to defraud her employer was to seek reimbursement for fraudulent expenses. Two days after ending employment with her employer, Solis submitted a personal expense of $4,575 for a dog boarding company.

When she submitted the fraudulent expense, she had access to her previous employers account and still had super-administrative privileges which had not yet been taken away from her. Solis caused payment of the $4,575 to be paid by her former employer and the funds to be electronically deposited into her personal account.

Solis continued to defraud the company after she left. She diverted at least $400,000 of the company's money to her own personal checking account nearly two months after her employment ended. In total, Solis stole more than $500,000 from the victim company. (Source)

Former Power Company Employee Sentenced To Prison For $1.6 Million+ Fraud Scheme To Pay For Personal Expenses - March 18, 2022

Gregory Holland was employed at American Electric Power (AEP) for over 35 years and was responsible for managing AEP's interests during customer bankruptcies, including filing claims on behalf of AEP as well as processing and collecting customer payments.

In 2001, unbeknownst to anyone else in the company, Holland opened a personal checking account using AEP's name and address. Between May 2002 and January 2018, Holland admitted to depositing hundreds of checks intended for AEP into this account and used the money for numerous personal expenses, including membership dues at the Roanoke Country Club, lake house payments, car payments, clothing purchases.

The court determined today the total loss to AEP customers to be $1,616,591. (Source)

Former Office Manager Pleads Guilty To $63,000+ Embezzlement Scheme - March 21, 2022

Kimberly Jones was employed as an office manager at Guardian Retention Systems, LLC. As office manager, she handled accounts payable and receivable, petty cash, payroll, and taxes. She also had electronic access to the bank accounts to pay bills.

During her time as officer manger, Jones took several actions to embezzle from her employer. She used company credit cards in her name and the names of other employees to make unauthorized personal purchases. She directed unauthorized transfers from the company bank account and diverted customer revenue received by the company's electronic payment account. Jones also set up a business called KAB Enterprises, LLC to issue false invoices to Guardian Retention Systems. Jones would use the company credit cards and bank account to pay the fraudulent invoices from KAB Enterprises, LLC.

Jones also failed to report her embezzled funds as income on her tax returns for tax years 2016 through 2018. Jones acknowledged that she owes $63,580 to the Internal Revenue Service. (Source)

Former Office Manager Pleads Guilty To Stealing $500,000+ From Employer - March 23, 202

Jessica Pechtel was the Office Manager for a company. In that role, she had full access to the company's finances, including its accounting records, bank accounts, and company credit card.

Between January 2019 and March 2021, Pechtel used her access to the company's finances to make unauthorized purchases and transfers of funds to accounts that she controlled. This scheme had four distinct components. First, she transferred funds from the company's bank accounts to her own accounts. Second, she used the company's credit card to make unauthorized purchases from retailers such as Amazon or make payments via the online payment transfer system Venmo. Third, she drafted 17 unauthorized checks payable to herself that were drawn on the company's bank account.

And fourth, she stole almost $44,000 in COVID-19 relief funds that were intended for the company. Overall, Pechtel fraudulently obtained at least $587,219 from her employer. (Source)

Former Office Manager Employed For 25 Years Charged With $1 Million Of Embezzlement - March 22, 202

For approximately 25 years, Edward Ziegler was employed as the office manager for a small business, identified in the indictment as Company A.

As part of a scheme to defraud , Zeigler opened a bank account in his name and with the qualifying language "Doing Business As [Company A]." Over the course of several years, Ziegler sent invoices to the business's customers through both the U.S. Mail and e-mail, received checks from the customers for services provided, and deposited checks into the secret bank account he had established. Ziegler also made fraudulent entries in Company A's books and record keeping system to cover up the fact that he had diverted the checks and used the funds for his own benefit.

It is alleged that, through this scheme, Ziegler caused more than 400 checks totaling more than $1 million to be deposited into his secret account. (Source)

Former Bed And Breakfast Manager Sentenced To Prison For Embezzling $500,000+ Over 5 Years For Personal Use - March 24, 2022

Chiquita Blake was employed as a manager of a bed and breakfast in Savannah, Georgia from 2005 to 2020.

From around May 2015 through December 2020, Blake manipulated the inn's reservation system to fraudulently transfer funds from the inn's accounts and into bank and credit card accounts that she controlled. She then used those funds for personal use and to make payments to some of her nearly three dozen credit accounts. (Source)

Former Manager At U.S. Auto Manufacturer Allegedly Accepted $3.4 Million+ In Bribes From Foreign Parts Supplier Seeking Contract - March 24, 2022

Hyoung Nam So was a former manager at a U.S. based automobile manufacturing company.

The foreign parts supplier paid So a total of $3.45 million in cash. Homeland Security Investigations seized $3.19 million believed to be proceeds from the bribery scheme from a private vault in Los Altos, California in 2017.

As a manager and team leader at the Michigan-based car manufacturer, So oversaw the supply of parts used to build interiors for the company's automobiles in North America. In October 2015, So promised a contract to the owner of the South Korean parts company, in exchange for $5 million, which So demanded in cash.

The following month, the owner of the foreign company arranged to have $1 million in cash transferred to the United States through money brokers.

By the time the $1 million payment was made, So had learned that foreign company was not the lowest bidder on the contract. So arranged for information to be provided to the foreign company so it could revise its bid on the contract. On December 8, 2015, So recommended to his company's executives that the contract be awarded to the foreign company. (Source)

Former Hewlett-Packard (HP) Planning Manager Pleads Guilty To $5 Million+ Wire Fraud Scheme For Personal Use - March 24, 2022

Shelbee Szeto was employed by as an executive assistant and finance planning manager from approximately August 2017 until June of 2021. In these roles, Szeto was responsible for making payments to HP vendors and was issued multiple HP commercial credits cards to make the payments on HP's behalf.

Rather than make payments in accordance with the company's policies, Szeto devised a fraudulent scheme whereby she sent approximately $4.8 million in unauthorized payments from her HP commercial credit cards to several Square, PayPal, and Stripe merchant accounts under her control.

As part of her employment with HP, Szeto was issued multiple American Express commercial credit cards that were intended only for business expenses. Szeto then set up bogus merchant accounts with PayPal, Stripe, and Square that she maintained under her control, but represented were for legitimate vendors. Szeto then unlawfully sent payments from the credit cards to the bogus accounts. To further her plan, Szeto uploaded falsified invoices to HP's internal system and falsely represented to HP that the payments were made to legitimate vendors. She also made false representations to Square that the payments sent from the credit cards were sent to HP's approved vendors for legitimate business transactions and falsely represented to her bank that the money from HP was for legitimate business transactions.

Szeto caused at least $4.8 million to be fraudulently from HP accounts to accounts she controlled and attempted to steal an additional approximately $330,000 from HP. Szeto acknowledged that the total loss and attempted loss from her scheme was at least $5.2 million.

Szeto identified list of cars, handbags, jewelry and other luxuryiItems that will be forfeited as part of a plea agreement. (Source)

Former Director Of Finance Pleads Guilty To Embezzling $270,000+ From Non-Profit Organization - March 3, 2022

Kristina Ballard worked for a nonprofit organization in Washington, D.C. Between August 2014 and December 2020, at which point she was fired for poor performance. She served as the organization's Director of Finance.

From January 2015 through December 2020, Ballard embezzled $271,465 from the organization. She fraudulently wired organization funds to bank accounts that she controlled, intercepted credit card rewards checks issued to the organization, and then deposited those checks into a bank account she controlled, and fraudulently charged personal purchases on the organization's credit card.

Ballard used the organization's credit card to pay $24,694 in restitution to the Arlington County Circuit Court for a prior embezzlement scheme for which she was convicted in Virginia.

Ballard concealed her fraud from the organization by listing various beneficiary names on wire transfers and creating fake invoices, often using fake company names. (Source)

Former Officer Administrator Sentenced To Prison For Embezzling $650,000+ From Employer Over 5 Years - March 25, 2022

Tina Wood was hired in 2013 by a supply company as an office administrator and secretary. Wood eventually became in charge of depositing payments from customers and had access to the company's accounting system.

For almost five years, Wood used the accounting software to embezzle checks from one of the company's biggest customers and deposited most of the stolen money into a personal bank account that she opened at a bank. Wood blamed the company's accounting software for her misdeeds, and she ordered deposit slips for her personal bank account that referenced the company name, likely to avoid scrutiny from bank personnel. In February 2019, when the company's owner realized something was amiss, he contacted Wood. Wood refused to talk to the owner and cleaned out her desk the next weekend. An investigation found 109 customer checks, totaling about $650,843, that Wood had deposited into her own account. (Source)

Contract Bookkeeper Pleads Guilty To $1.2 Million Fraud And Money Laundering Scheme From Clients - March 28, 2022

While Paul Harleman was working as a contract bookkeeper, he devised two fraud schemes to obtain money from three of his clients.

In the first scheme, from July 2018 to May 2020, Harleman formed a limited liability company with a name nearly identical to the name of a significant vendor to one of his clients, and then charged the client's credit card for more than $146,000 in fraudulent invoices.

In the second scheme, from September 2019 to his arrest, Harleman transferred more than $1,064,000 in a series of payments disguised as payroll from two of his clients to Harleman's limited liability company. Harleman moved money fraudulently obtained from his three clients from his personal checking account to a personal investment account, resulting in the money laundering charges. (Source)

Former Administrative Assistant For Used Car Dealership Sentenced To Prison For $4.3 Million Fraud Scheme (Had Help From Co-Conspirators) - March 28, 2022

Tammy Newsome was employed as an administrative assistant for Kentucky used car dealership Big Blue Motor Sales, which bought trucks at wholesale prices at auction, obtained hundreds of copies of Kentucky and West Virginia residents' driver's licenses, and fraudulently titled the trucks in the name of those residents.

Newsome helped induce Toyota to repurchase hundreds of fraudulently titled trucks at 150% of value between 2013 and 2015, as part of a scheme to misuse its warranty extension program. The scheme relied on Newsome to make false representations to the Department of Motor Vehicles to obtain false vehicle titles in the names of false owners. The titles obtained by Newsome were then used by other scheme participants to induce Toyota to repurchase the vehicles.

Newsome admitted that she made false representations to the DMV, delivered cash bribes to other scheme participants, and forged signatures of false owners so that checks issued by Toyota in the name of a false owner could be deposited into Big Blue Motor Sales' bank account. (Source)

Former Financial Secretary - Treasurer For United Auto Workers Union Pleads Guilty To Embezzling $2 Million+ To Purchase Vehicles, Firearms & Gamble - March 26, 2022

Between 2011 and 2021, Timothy Edmunds served as the Financial Secretary-Treasurer of union Local 412 of the International Union, United Automobile, Aerospace, and Agricultural headquartered in Warren, Michigan.

Edmunds systematically drained the Local 412 accounts of $2.2 million by (1) Using Local 412 debit cards for over $142,000 in personal purchases, (2) Cashing Local 412 checks worth $170,000 into accounts he personally controlled, and (3) Transferring $1.5 million from Local 412 accounts into accounts that he personally controlled. Edmunds then converted the funds for his own personal use.

To conceal his theft from other UAW officers and the Local 412 members, Edmunds created false bank statements and caused false Department of Labor ("DOL") reports to be filed with the U.S. DOL. Edmunds supplied the fake bank statements to international UAW auditors in an effort to conceal his embezzlement.

Edmunds used portions of the proceeds of his embezzlement to gamble extensively, to purchase firearms, and to purchase various high-end vehicles. For example, between 2018 and 2020, Edmunds used the UAW Local 412 debit card to make over $30,000 in unauthorized withdrawals at the Greektown Casino. While gambling at the Greektown Casino, records indicate that Edmunds had cash buy-ins of over $1 million, and he put over $16 million in play while gambling at the casino. (Source)

Former Bookkeeper For Interior Design Firm Arrested For Embezzling $180,000+ - March 30, 2021

Christina Iannelli was an independent contractor for an interior design firm.

Beginning in or about October 2018, Iannelli allegedly prepared dozens of fraudulent invoices with inflated totals derived from inaccurate math, and then issued herself checks for the inflated amounts due from the firm's checking account.

Beginning in or about July 2019, Iannelli issued herself dozens of additional unauthorized checks. In both instances, Iannelli allegedly used a signature stamp in the name of the firm's owner to issue the fraudulent checks.

To conceal the fraudulent payments, it is alleged that Iannelli made false entries in the firm's accounting records. In total, Iannelli allegedly embezzled over $30,000 through inflated compensation checks and over $150,000 through additional unauthorized checks. (Source)

Movie Theatre Owner & Chief Financial Officer Charged With Fraudulently Obtaining $749,500 In Covid Pandemic Loans To Buy Homes & Cars, Pay Relatives - March 29, 2022

John Hutchins, the owner, and Roberto Soliman, the CFO of the Rapids Theatre in Niagara Falls, were charged with multiple counts of conspiracy to commit wire and bank fraud and other charges for fraudulently obtaining $749,500 in Covid pandemic loans.

The proceeds from the loans allegedly were used to buy homes, make house payments, purchase a 2020 BMW and 2020 Cadillac, pay overdue fees on Hutchins' condo in Florida, and to pay relatives. (Source)

THEFT OF COMPANY PROPERTY

Former Yale Med School Employee Pleads Guilty To Stealing And Selling $40 Million in Electronics / Used Money For Cars, Real Estate, Travel - March 28, 2022

Beginning in approximately 2008, Jamie Petrone was employed by the Yale University School of Medicine (Yale Med), Department of Emergency Medicine. He most recently served as the Director of Finance and Administration for the Department of Emergency Medicine. As part of her job responsibilities, Petrone had authority to make and authorize certain purchases for departmental needs as long as the purchase amount was below $10,000. Beginning at least as early as 2013, Petrone engaged in a scheme whereby she ordered, or caused others working for her to order, millions of dollars of electronic hardware from Yale vendors using Yale Med funds and arranged to ship the stolen hardware to an out-of-state business in exchange for money.

Petrone falsely represented on Yale internal forms and in electronic communications that the hardware was for specified Yale Med needs, such as particular medical studies, and she broke up the fraudulent purchases into orders below the $10,000 threshold that would require additional approval.

The out-of-state business, which resold the electronic equipment to customers, paid Petrone by wiring funds into an account of a company in which she is a principal, Maziv Entertainment LLC.

Petrone caused a loss of approximately $40,504,200 to Yale. Petrone used the proceeds of the sales of the stolen equipment for various personal expenses, including expensive cars, real estate and travel. (Source)

WORKPLACE VIOLENCE

Chicago Transit Employee Arrested After Shooting Man During Altercation On Subway / Employee Was Not Authorized To Carry Gun - March 27, 2022

A Chicago Transit Authority (CTA) employee who was working as a customer assistant, was arrested after police said he shot another man inside a station.

Chicago police said a verbal argument between the employee and the man, led to the shooting.

The CTA confirmed in a statement to local news outlets, that "Based on our own investigation, we can also confirm that this employee was in violation of several CTA workforce rules, including one that expressly prohibits the possession of a firearm. CTA is pursuing termination of this employee." (Source)

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data (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)

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)

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)

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

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**3,500+ 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

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

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

https://twitter.com/InsiderThreatDG

Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **875+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

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

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

ITDG Training / Consulting Services Offered

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

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

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

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