ACFE
Association of Certified Fraud Examiners
New York Chapter #14

SPRING 2020 / ISSUE 4

TABLE OF CONTENTS

Photo courtesy LHK

Letter from the President

Dear NYCFE Members,

It is my honor to serve as the newly elected President of our Chapter for the 2020-2021 term and I appreciate the overwhelming support of our members who reached out to me during the election! As an active participant in the NYCFE over the past seven years as chapter member, training director, and in various board roles as an officer, it has been a thrill to see the growth and expansion of our membership. I would like to thank the board of 2018-2020 for their efforts in support of our chapter.

Our new term began with a chapter meeting on March 9th at Fordham University and our planning for training changed immediately after that.

On April 29th our chapter made history with our very first webinar which was well attended and an indicator that our live-stream format is welcomed. We will continue hosting webinars for members to earn NASBA and CPE credits, and welcome non-member participants. Please check our website for the latest schedule of events and details.

President Dora Gomez

Our board remains committed to the fight against fraud and is actively working on many initiatives to bring this chapter to the next level. Some of these include:

Our Events

I will continue to serve as Training Director and aim to continue to introduce top experts on Fraud Risk; IT Security; Investigations; Governance; Data Analytics; Forensics; Cybercrime; Ethics; Whistleblowing, and other topics as we continue to prevent and detect fraud.

Membership Drive

We value our members and will provide the best benefits possible by launching some special perks for referrals and are evaluating group discounts while we continue to extend member preferred rates for all our events. Be sure to check the NYCFE website for our digital brochure available for

download via the homepage to learn more about the advantages of joining our chapter.

Students

We want to engage students from various curriculums who are our future CFEs and we welcome them! We are actively recruiting student members to join the NYCFE and participate in student specific initiatives that will be led by a new board member.

Your Involvement!

This newsletter is our way of sharing updates, events and fraud articles and we welcome your participation in our semi-annual newsletter.

The current coronavirus pandemic has impacted us all, yet it also serves as a reminder of the importance of our NYCFE community in staying connected. We look forward to hosting in-person conferences and seminars when we are permitted to gather once again.

We know how important it is to network with your peers and appreciate your support throughout this changing process in bringing our training events in a completely different method.

These are very trying times, especially in New York City and the Tri-State area with the Covid-19 restrictions. We hope you have not been affected by the virus and are following the restrictions for quarantine until further updates. We want to lend a hand and have made a significant donation to NYU Langone Hospital where health care workers are making a difference serving Covid-19 victims.

We are a group of passionate CFE volunteers committed to serving our members the best way possible.

Our entire board thanks you for your continued support and are enthusiastic to have you join us as we look forward to a successful year ahead!

Let's continue to make a difference in the fight against fraud!

Your NYCFE Chapter President,

Dora Gomez, MS, CFE, CRMA, GRCP

ABOUT THE NYCFE

Our NYCFE chapter is managed by our board of directors on a completely volunteer basis according to guidelines set forth by the global Association of Certified Fraud Examiners, headquartered in Austin, TX. The NYCFE board members maintain the chapter's website; manage chapter correspondence, CPE credits, membership rolls, and fees; develop, organize, and host NYCFE conferences, seminars, and gatherings; facilitate and host ACFE events held in New York City, and assist ACFE International with its local seminars. We welcome the participation of current NYCFE members in our volunteer opportunities. To learn more, please contact:

President Dora M. Gomez: President@nycfe.org
For General Questions: Info@nycfe.org
For Newsletter Questions, Comments and Submissions: Newsletter@nycfe.org
For Training, Events, Speaker and Sponsor proposals: Training@nycfe.org

ACFE NEW YORK CHAPTER BOARD OF DIRECTORS

Chairman of the Board: Ernesto Castillo, CFE, CFCS
Vice Chairman/Governance Director: Bruce Hulme, CFE, BAI
President/Training Director: Dora M. Gomez, MS, CFE, CRMA, GRCP
Vice President/Membership Director: Ozan Gurel, CFE
2nd Vice President/Treasurer: Judy S. Juan, CFE, CFCS, CPA
Board Director/Finance Director: Daniel Killourhy, CPA, CFE
Board Director/Newsletter Editor: Laura Hynes-Keller, CFE
Communications Director: Emmah Padilla, CFE
Recording Secretary/Student Relations Director: Gregory M. Boylan, MA, CFE
Member at Large: Jon Newcomb, CFE
Board Member: Patricia Kalaz, CFE, CAMS
Founder and President Emeritus: Anthony Luizzo, PhD, CFE, CST, LPI
Chapter Counsel: Kenneth C. Citarella, Esq., CFE, CIPP

"Money as a Weapon" – *What Target or Metric?*

Wilem S. Wong, CFE, CAMS

The views expressed are those of the author and not of the U.S. Army, U.S. Marine Corps, the New York City Police Department, or his previous affiliations.

Introduction

The U.S. military has many weapon systems and the concept that money can be employed as a weapon by military service members in combat zones to influence in-conflict and post-conflict operations is not new.

In 2003 two U.S. Army Sergeants and their subordinates of the 3rd Infantry Division found hidden metal boxes of sealed, uncirculated $100 bills totaling $650 million during searches of residences of Saddam Hussein's Ba'athist regime officials. This fortunate find became the catalyst of what is now known as the Commander's Emergency Relief Program (CERP) that operationalized the concept of *"Money as a Weapon."*

Within the second presidential term of President George W. Bush, this fortuitously funded CERP program enabled over eighteen thousand projects covering nearly two dozen broad categories ranging from condolence payments, medical facility repairs and school re-construction to entrepreneurial micro-grants, literacy programs, and agricultural development.

CERP was envisioned to fund projects that would facilitate the stabilization of military units' area of operations. An integral part of the vision of CERP was to improve inter-agency cooperation, increase stability in areas of operations, and build governance capacity by collaborating with local officials via Provincial Reconstruction Teams (PRTs) that were established first in Afghanistan and later in Iraq.

CERP provided funds to tactical units in coordination with PRTs in those countries to meet urgent humanitarian relief and reconstruction needs at the local level. PRTs (if led by U.S. personnel) are usually commanded by a military officer branched as a Civil Affairs Officer with various representatives from the U.S. Department of State (DOS), United States Agency for International Development (USAID), United States Department of Agriculture (USDA), United States Department of Justice (DOJ), as well as various civilian advisors on policing, cultural affairs, and economic development.

Over time CERP became so highly demanded by ground commanders that Congress bolstered the program by allocating additional funding of nearly $7.5 billion. However, all these billions of dollars didn't translate into longer term sustainable tactical metrics or achieve strategic outcomes. From the author's point of view as a Certified Fraud Examiner, there were ongoing signals of the three interrelated factors of the fraud triangle: pressure, perceived opportunity and rationalization.

Overall, the *"Money as a Weapon"* concept has subsequently been more closely scrutinized for its effectiveness in a combat zone, most significantly in Iraq and Afghanistan.

The U.S. military engaged in operating a reconstruction and development program in a post conflict environment after WWII.

Yet operating reconstruction and development programs in a counter-insurgency environment-- with persistent threats of terrorist activities--as well as a highly organized enemy that is operating its own development and political programs (shadow government) --are beyond the core competencies of the U.S. military.

The U.S. military isn't called into an ideal situation, as the reconstruction and/or stability phases of military operations are usually conducted in a predominately "non-kinetic" or "non-shooting" part of military operations.

Non-Kinetic

The reconstruction and stability phases of combat operations employs other non-military assets that have been mentioned on PRTs including various military specialties within Civil Affairs (CA), such as combat engineers, uniform medical personnel, and Agriculture Development Teams to engage the local populace, restore civil institutions, build/rebuild infrastructure, as well as improve the local governance in that society.

We have engaged in many "non-kinetic" efforts, such as agricultural development. Both

Operation Iraqi Freedom

In 2008, I was the Public Health Officer on a 9-member Civil Affairs Functional Specialty Team attached to the XVIII Airborne Corps at Camp Victory, Baghdad, Iraq. As the C9 governance action officer, I was on the teams for the Iraqi provincial election planning and Iraqi national literacy campaign, then later as economics liaison officer working in the non-kinetic future operations projects. The joint efforts involved millions of dollars of CERP funds as detailed below:

Iraqi Provincial Elections – As a member on the Iraqi provincial election planning team, we were part of a larger joint effort in coordination with Iraq's Independent Higher Electoral Commission, International (Inter-Governmental) Organizations, and the DOS to ensure that Iraqi voters were offered fair and credible provincial elections across Iraq. CERP funds were utilized to bolster security measures to ensure a safer environment to cast votes. Iraq provincial elections were held on January 31, 2009 with a high voter turnout and the elections results were recognized by the Iraqi people.

Iraqi National Literacy Campaign – As a member on the Iraqi National Literacy Campaign Committee, we were part of a larger joint planning effort to offer the Iraqi people an opportunity to attain a literacy proficiency that will be a gateway for military age males to employment in the Iraqi Army or the Iraqi Police, but also for others to be eligible to enroll in vocational training for better employment opportunities. Moreover, a literate populace is better able to resist insurgent propaganda. CERP funds were utilized to refurbish and furnish schools; hire instructors and administrators; as well as provide a stipend for students to attend class.

Iraq and Afghanistan each have a proud agrarian society, but continuous conflicts of recent decades have destroyed untold acres of farmlands. Moreover, generations of acquired agricultural knowledge has been lost.

These type military assets, working in coordination with the DOS, USAID, and the USDA through the respective nations' ministry of agriculture have made progress in restoring Iraq's and Afghanistan's agrarian legacies.

The "non-kinetic" is not tangible and, therefore, more difficult to quantify, but that does not diminish the significant longer-term impact in securing the peace.

How did I become involved in the "non-kinetic" fight? Over 30 years ago, I began military uniform service to our great nation as an U.S. Army enlisted Soldier.

Prior to September 11th, I served as a combat medic and practical nurse on Humanitarian Civic Assistance (HCA) missions in El Salvador and Panama.

As a result of September 11th, I began my civilian uniform service to New York City in 2004 as a NYPD Police Officer. I also continue in the military today as a U.S. Army Reserve Health Services' Planning, Operations, and Training Officer.

In 2008, I was deployed to Iraq as a Public Health Officer on a Civil
Affairs Functional Specialty Team.
Civil Affairs' Soldiers assist military commanders and governments by coordinating efforts with civil authorities and civilian populations to lessen the impact of military operations during times of conflict and national disasters. Our teams implement programs/projects on economic development, education, governance, infrastructure, public health, rule of law, and security through coordination with the host country and designated U.S. government agencies. In addition, Civil Affairs may partner their efforts with international organizations such as the United Nations or non-governmental organizations (NGOs) such as the Red Cross/Red Crescent, Mercy Corps or International Medical Corps.

The following are accounts of how I saw CERP funds utilized in Iraq and Afghanistan. For more details, the projects highlighted in the Operation Iraq Freedom and Operation Enduring Freedom breakout boxes were a few projects I was involved with during my time in Iraq and Afghanistan.

CERP Funds in Iraq and Afghanistan

Through the CERP program, Iraq has received $4.1 billion and Afghanistan $2.3 billion since 2003. The U.S. military had been efficient in funding projects in these two theaters of war, as well as

demonstrating short term positive effects of smaller projects.

However, it had not been as effective in transitioning projects to the respective host nations to sustain them for longer term positive strategic outcomes. For example, the surge of funds in these theaters of war contributed to an economic bubble that had adversely driven local merchants out of business.

Overall, the fierce competition of U.S. forces to fund more projects as a measure of performance became the easiest metric with which to measure success for the military unit initiating the project, since the metrics for those measures of performance and their effectiveness would be beyond the unit's time in the combat theater.

The culture of "*funding more projects*" was analogous to "*spray and pray*" type project funding, which was counter-intuitive to applying funds with more precision, such as accounting for each round military service members fire from their weapons.

This type of "*funding more projects*" mindset signaled a "Perceived Opportunity" in the Fraud Triangle, which may have contributed to certain local nationals behaving with the intent to inflate project costs, knowing that service members might equate bigger projects to bigger successes.

Moreover, in certain areas that may well be under the control of the insurgents or Taliban, a certain percentage of the funds from the designated project was expected in exchange for permitting the project to proceed—or allow it to continue—due to the "pressure" factor.

In addition, even within the respective host nation, a certain amount of skimming from government officials was anticipated and accounted for in each of the project costs (especially the bigger projects).

The concept of corruption is seen from the local nationals' perspective as a duty to take care of one's family in those host nations, since it is not seen as for "greed," but for "need," which speaks to the "rationalization" factor.

Operation Enduring Freedom

In 2011, I was on a special assignment with the United States Marines at Camp Dwyer, Helmand, Afghanistan, as a Team Leader of a Human Terrain Team. We conducted socio-cultural research to better understand the grievances, motivations, interests, and friction points of tribal factions and individuals within tribal factions in order to facilitate combatant commanders to make better strategic and operational decisions to stabilize and develop military units' areas of operations. These joint efforts involved millions of dollars of CERP funds as detailed below:

Agro-Economic Mindset of Agriculturalists – to understand the economic mindset of farmers as to which specific crops they choose to plant and how this information can be used for better allocation of resources. This information can be used to assist in blunting the poppy harvest that the Taliban rely on to secure funds for operational needs to conduct attacks against GIRoA and CF. Ultimately, it is to foster an environment conducive for farmers to sell fruits and vegetables to consumers in the domestic and international markets. CERP funds were utilized for offering crop substitution instead of growing poppy as well as providing refrigeration to reduce spoilage before fruits/vegetables goes to market.

Interim Security Critical Infrastructure (ISCI) / Afghanistan Local Police (ALP) – to understand the recruitment and retention challenges as well as opportunities of ISCI/ALP. CERP funds were utilized for recruitment and training of Afghan males of fighting age to join ALP instead of the Taliban or insurgents.

Religious Engagement Program – to work in coordination with U.S. Navy Chaplains to understand and build positive relationships with the Afghanistan National Army (ANA) Religious Cultural Advisor Officers (RCAOs). CERP funds were utilized for training of new RCAOs and coordination of hosting religious shuras (consultation) within local communities.

Target or Metric?

The question lingers, *"Money as a Weapon" – What Target or Metric?* The response, solution, or way forward to address the aforementioned question is to cultivate a better cultural understanding of the host nation operating environment and its measures of success, as well as the achievability and sustainability of first world measures of success.

An agreed upon point within this gap is needed by the host nation and major coalition stakeholders.
However, the heavy presence of western coalition forces (with its higher ethical standards) in the Middle East for the past 18 years may have indirectly influenced the region's recent reporting on fraud and corruption. Leading organizations in the Middle East have allocated at least 40% more money into their anti-fraud programs during the past two years. This is more of a measure of performance as compared to a measure of effectiveness. Is this the longer-term strategic metric? I believe the better longer-term strategic metric as a measure of effectiveness is to look at Transparency International's Corruption Perceptions Index (2018) and monitor the change in rankings of Iraq (168 out of 180 countries) and Afghanistan (172 out of 180 countries). The higher up in the ranking means a respective country is relatively less corrupt than a lower ranking country. A possible leading indicator(s) is to monitor the change in rankings of Saudi Arabia or Jordan (both at 58 out of 180 countries) since both countries have strong regional influence that may lead other Middle East countries to improve the effectiveness of their anti-corruption programs.

About the Author:

Wilem Wong, CFE, CAMS, has over 20 years of combined service to New York City/New York State. Currently, he has over 15 years for the NYPD and holds the rank of Sergeant (Special Assignment). In his military capacity, he has served over 31 years in the United States Army Reserve as a Combat Medic, Licensed Practical Nurse, and Health Services Planning, Operations and Training officer. Currently, he holds the military rank of Lieutenant Colonel. He is a veteran of Operation Iraqi Freedom and Operation Enduring Freedom – Afghanistan. He earned his B.S. in Finance from New York University and a M.A. in Management and Leadership from Webster University.
Contact:
wilemwong2020@gmail.com

References:

- Bate, J. & Walker, D. (2018, July 3). "Buying Victory: Money as a Weapon on the Battlefields of Today and Tomorrow." Modern War Institute.
- Johnson, G., Ramachandran, V., & Walz, J. (2012, March). "CERP in Afghanistan – Refining Military Capabilities in Development Activities." Prism 3, No.2, 81-98
- Martins, M. (2004, February). "No Small Change of Soldiering: The Commander's Emergency Response Program in Iraq and Afghanistan." The Army Lawyer, 1-20
- Wilder, M. (2019, May/June). "Middle East Fraud and Corruption Enigma." Fraud Magazine, 8-9
- Wong, W. (2015, September). "Lights of Liberty." The American Legion, 34-38.

TOP DATA BREACHES, EXPOSURES AND HACKS OF 2019

First American Financial Corp.: 885 million records exposed online including bank transactions, social security numbers and more.

Facebook: 540 million user records exposed on the Amazon cloud server. In early 2019 it admitted it had not properly secured the passwords of as many as 600 million users since 2012.

Zynga: Number of records hacked: 218 million

Dubsmash: Number of records hacked: 161.5 million

Capital One: Number of records hacked: 100 million. Unlike other major hacks, the data accessed during the Capital One breach included sensitive data, such as Social Security numbers.

Houzz: Number of records hacked: 48.9 million

Quest Diagnostics: Number of records hacked: 11.9 million

Fortnite: A flaw in the Fortnite video game exposed players to being hacked. The game has 200 million users worldwide, 80 million of whom are active each month.

ROBOCALL RECORDINGS ABOUT THE CORONAVIRUS

Fake tests for Medicare recipients

Free test kit scam

Sanitation supplies

Health insurance pitches

Mortgage scam

Social Security Administration scam

Small business listing scam

Recordings courtesy of Nomorobo

Consideration of Incentive Compensation Plans When Conducting Fraud Investigations

Daniel J. Killourhy, CFE, CPA, MBA

With the current collapse of sales and earnings due to the Coronavirus crisis, most enterprises are having trouble meeting sales and profitability targets. Manipulation of financial results is a very real risk.

The almost universal existence of incentive compensation plans in the private sector offer the incentive for financial statement and related frauds to occur. Some individuals will seek to maximize personal financial gain by reaching various financial targets. This could result in criminal or at least unethical behavior.

Due consideration needs to be given to these risks. When an investigative auditor or financial crimes investigator is tasked with conducting a fraud investigation in an organization, planning of the engagement requires that decisions made by a Controller, CFO or other senior executive need to be closely examined. Some of these decisions will impact the organization negatively but be personally rewarding for the financial or senior management executive.

As part of the planning of the assignment, a financial crimes investigator should request, if possible, the incentive compensation plans for the organization as a whole and for specific individuals who can be considered potential targets. By examining these incentive compensation plans, the investigator can obtain insight as to what may be driving decisions by various executives.

What types of situations can we expect to see?

I will draw on my own extensive experience as a former Audit Director for a major international organization with extensive manufacturing operations and point out some of the possibilities.

Manipulation of Inventory, Accounts Receivable and Other Reserves

Manipulation of reserves is a classic earnings management technique used down through the generations by financial statement fraudsters to meet financial targets. When the end of a fiscal period is looming, a financial executive will sometimes make the case that previously established reserves are no longer needed and can be reversed back into income since risks previously identified have been resolved or diminished. In these cases, the investigator must examine appropriate documentation

and interview key decision makers in depth to be sure that the organization is not managing earnings.

I had Audit Director responsibility for a manufacturing operation which had several major contracts to manufacturer trains and light rail vehicles for various cities in the U.S. These contracts were multi-year in nature and had a demonstrated long history of technical problems and project delays resulting in increased costs and reported losses.

In one noteworthy fiscal year, cost overruns were occurring due to engineering, manufacturing and supply chain problems, resulting in labor, material and manufacturing overhead cost overruns which were being debited to work in progress project inventory accounts on the General Ledger. These should have been charged immediately to P&L.

The division CFO, scheduled to return to a higher position back at corporate headquarters in Europe, was reporting over the past several quarters in the financial statements to all concerned that prior problems had been resolved and that the division had "returned to profitability." I'm sure this helped garner him the career promotion he was now returning to. The fact that this division was reported to have "turned around" earned it a highly coveted award from corporate headquarters. The increase in reported profits also meant that the Division Vice President, the CFO and many other executives were receiving inflated incentive compensation payments, and, in the case of the CFO, a promotion back to headquarters in the home country to boot.

This CFO did return to a higher-level position back at headquarters. However, the Controller, who reported to the CFO, had been pressured for several quarters not to record project cost overruns and felt quite uncomfortable and distressed by the situation. Since we had a good working relationship, he called me as soon as the CFO departed.

An investigation was commenced, and tens of millions of dollars were charged off to expense just prior to year-end. The CFO was ultimately disciplined. Needless to say, "Tone at the Top" was a big issue in this situation.

Cost Accounting Manipulations

I found cost accounting somewhat boring in college. It wasn't until I became quite involved with manufacturing operations that I realized that unethical cost accounting techniques can be employed to distort financial results.

How Can This Occur?

Consider that in a manufacturing operation, general and administrative costs are charged to expense as they are incurred while direct costs of production are charged to work in process inventories and thus capitalized onto the Balance Sheet until the goods are sold. Capitalized inventory consists of materials, labor and importantly, allocated manufacturing overhead.

Sometimes in a bad economy or in an industry with problems, the amount of manufactured product decreases significantly.

In a period of sharp reductions in business/manufacturing activity, the manufacturing overhead pool needs to be analyzed and in the interest of conservative valuations, consideration be given to allocating some of the overhead costs to period expense versus being capitalized onto the Inventory account on the Balance Sheet. Accounting literature allows for some interpretation of period costs vs. capitalized costs, thus opening the door for those who would like to manipulate financial results for their own purposes.

Manipulation of Repair & Maintenance Expense

Controllers and manufacturing managers will sometimes defer budgeted maintenance to conserve cash and reduce reported expenses in the current year. This can, however, result in damage to buildings and machinery and equipment. The resulting costs will be borne by future accounting periods but higher net income (and resulting higher current year incentive compensation payouts) will be reported in the current fiscal year. Financial fraud investigators and auditors should examine the reason for current year budget vs. actual favorable variances and also analyze the reasons for declines in this category of expenses versus prior years.

Revenue Recognition Schemes/Distribution Channel Stuffing

In manufacturing and distribution businesses, unethical financial and other executives will sometimes persuade a customer to accept shipment of goods just prior to the end of a fiscal period with a verbal agreement that these goods can be returned to the seller just after year end. Big four auditors are required by GAAP to test for proper revenue recognition cutoff.

Some Final Thoughts

Many of the problems discussed above exist in other industries, not just manufacturing. At Wells Fargo, it was a pervasive practice throughout the organization to engage in unethical sales practices in order to meets sales and profit goals. If you didn't go along with the program, your incentive compensation and perhaps your job could disappear!

An old boss once told me, "Remember, no one likes to deliver bad news or hear bad news." Disappointing financial reporting numbers fall into this category. So, to avoid the "shoot the messenger" syndrome, individuals responsible for financial reporting will sometimes resort to criminal or unethical practices to achieve the desired results.

As fraud investigators, we have to be aware of the often-pernicious practices relating to incentive compensation practices which are out there and the impact on our investigations.

As I've often said to many of my colleagues over the years, and only partially in jest, "Incentive Compensation plans are the root of all evil!" ♦

Daniel J. Killourhy, CFE, CPA, MBA is Finance Director and a Board Director of the NYCFE. He is a Financial Crimes Investigator and Forensic Accountant. Email: daniel.killourhy@gmail.com

Tips on Solving P-Card Fraud Mysteries!

Judy S. Juan, CFE, CFCS, CPA, MBA

Some people are bold enough to use their Enterprise's procurement card (P-Card) for personal use. To give you a little background, typically only full-time employees at an Enterprise are eligible to hold P-Cards.

The P-Card is used to make small purchases, usually up to the threshold of $2,500 for a single item, for business purposes only. This amount can vary depending on an Enterprise's size, and the types of purchases made. An employee receives training and is also explicitly told that he/she must not share or give the P-Card to anyone else. The P-Card policy clearly states this information as well and lists items that are not allowed to be purchased.

A Common Scenario Involving P-Card Fraud

A probable P-Card fraud has been detected via continuous monitoring using ACL data analytics, Machine Learning and Excel. Some vendors, such as Amazon, offer a detailed description, called "Level 3" details. Level 3 details show exactly what item(s) were purchased with the P-Card, as well as the date of purchase, the P-Card number used, and the name of the related owner stated on the card. Level 3 details also list the suppliers and their addresses, and in some cases, the destination where the item(s) are shipped, the product code, and other details. A simple Google search of the product code reveals the related item. Level 3 details are contained in a report obtained from the Enterprise's bank.

Despite a clear policy set by the Enterprise, P-Card holders oftentimes manage to violate the policy and commit fraud. For example, they purchase items for personal use, such as Apple Air pods, Apple watches, groceries, cameras and related accessories, X-Boxes, televisions, handbags, wallets, graduation balloons, flowers for Mother's Day and men, women and children's apparel and shoes. There have also been instances where the charges were split because the item cost more than $2,500. This is another violation of the policy.

Curious as to how employees are able to make such non-business-related purchases?

Part of the implementation of the scheme has to do with policy violations. According to the P-Card policy, purchases must be shipped to the Enterprise's business address. Employees then contact the vendors and change the delivery destination to a personal address, or the address of a non-associate of the Enterprise. The supporting documentation the employee is required to upload into the system, or maintain on file in his/her office, would not reflect the actual purchase made. Some employees go to great lengths to carefully alter receipts and supporting documentation to reflect the purchase as a business-related item or goods. The other part of policy violation occurs whereby the Approver "mass" approves P-Card purchase transactions. Instead of reviewing individual purchases and the related receipts as required by policy, an Approver would simply approve all the transactions for that monthly cycle without looking at any receipts or supporting documentation. There are instances when the P-Card holder would not upload any documentation, and with mass approval, there is no way to catch this. Some P-Card holders are aware that an approver may not be diligent, so they use this to their advantage to commit fraud.

So how do we deter P-Card fraud?

Be proactive!

Fraud investigators perform continuous monitoring of data, and when potential fraudulent transactions are identified, the related P-Card Holder and card transactions are selected for further detailed review. Fraud Investigators review the business purpose of the noted transactions and seek confirmation with the department as to the legitimacy of the purchase.

For instance, they perform analyses of the dates and times of purchases, including those that are made on holidays, or when someone is out on vacation or sick leave so should not be using the card.

Oftentimes, the "Destination" zip code is captured, and this is useful as it signals that the purchases were delivered to an address other than one belonging to the Enterprise. Once it is determined that non-business-related purchases were made with a P-Card, and with the Enterprise's Legal Counsel's written approval, Fraud Investigators may review the

individual's business emails related to P-Card transactions.

Many times, the P-Card holder will house documentation from the vendors listed above, with the actual purchases made, yet the documentation or receipt he/she uploads into the system for review is altered to reflect a business-related purchase transaction.

Upon more scrutiny, Fraud Investigators can clearly see that the original documents have been altered, as P-Card holders usually forget to change the dates and/times of purchases made on holidays, vacation and sick days, or times that are after the hours of normal business operations. Usually the data analytics programs have already flagged and identified the fraudulent purchases as well.

The next step is for Fraud Investigators to interview various individuals who may be in the same department or division as the P-Card holder, to obtain information relevant to the purchases made.

Fraud Investigators prepare spreadsheet(s) of clearly documented information and attach pertinent documents to support their findings. The P-Card holder is usually the last person to be interviewed. At least two fraud investigators are present at an interview. Human Resources and Law Enforcement Officers are rarely present. An individual may or may not confess.

However, the Enterprise terminates the person once there is documentation to support the wrongdoing.

To send a message and deter fraud, today cases are more frequently referred to Law Enforcement to pursue criminal charges against the individuals and seek restitution.

Prior to advances in data analytics, fraud investigators would usually perform monthly P-Card audits which were time consuming and arduous, and they were reacting to fraud after it occurred.

By utilizing data analytics such as ACL and Machine Learning, auditors and fraud investigators can quickly identify anomalies to detect fraud sooner and prevent it from multiplying.

Fraud investigators oftentimes work hand-in-hand with Data Analytics Specialists to develop programs that detect and signal a P-Card holder is likely committing fraud, then generate various reports to document the anomalies.

A typical report would include comparisons of information, e.g., the actual items purchased based on data received directly from the bank, matched to the information the P-Card holder writes as verification, and the documentation they upload to the system.

Depending on the type of Enterprise, the vendors the P-Card holders "shop" may be different, but many purchases are made from companies such as Amazon, Apple, Best Buy, B&H Photo and Staples, along with apparel retailers, grocery stores and pharmacies.

ACL data analytics and Machine Learning--along with the reliable, trusty Excel program--continue to transform P-Card fraud investigations and help solve P-Card mysteries. ♦

Judy S. Juan is Treasurer and a Board Member of the NYCFE. She is employed as a fraud investigator. Email: judyjuan12@gmail.com

econsumer.gov is where you can report international scams and learn about other steps you can take to combat fraud. Your complaints help consumer protection agencies around the world spot trends and work together to prevent international scams.

Nine Questions with...Michael Van Sertima, CPA, CFE, MS

Michael Van Sertima, CPA, CFE, MS, is partner at Gould, Kobrick & Schlapp, P.C., one of the few CPA firms licensed to practice in NY and NJ that specializes exclusively in providing audit, accounting, consulting, and related services to labor organizations and employee benefit plans.

Q: ***How did you first become interested in obtaining the credential of Certified Fraud Examiner?***

A: Our firm was invited to respond to an RFP to provide financial statement audit services. The new administration of the entity was concerned that the prior administration had committed fraud and kept asking about our ability to conduct a fraud examination. I did my best to explain that most experienced auditors, especially those who have investigated fraud (like myself) could perform fraud investigations even though they are not CFEs. Nevertheless, the organization seemed to want an auditor with the CFE credential. I registered to take the CFE exam that same week. And no, we did not get them as a client.

Q: ***How do you use your expertise as a CFE in your work?***

A: My CFE training complements my work as a financial statement auditor because it adds a dimension to audits that would not otherwise exist. Audits are geared to provide reasonable assurance that material misstatements are not present in the financials. Consequently, audits are designed more to unearth material errors and fraud in financial statements rather than detect employee fraud (misappropriation of assets--which are generally not material in any given year). This is consistent with the low percentage of fraud revealed by external audits; the profession trains auditors to focus on material or key items. This is supported by generally accepted auditing standards. Nevertheless, I do impress upon the firm's professionals the need to be alert for signs of fraud, even if potentially immaterial. I see this as a value-added service to clients and as a means to avoid the inevitable fallout in the event we do not discover an immaterial fraud at a client. We encourage staff to maintain a healthy level of professional skepticism.

Q: ***Tell us about your work as an instructor.***

A: Obtaining the CPA designation provided an extremely strong foundation as a professional; completing those 60 credits in liberal arts for my undergraduate degree helped me to understand the world a little bit more; and studying management for my graduate degree helped me to understand the dynamics of organizations and the basics of human behavior. Nevertheless, and I impress this upon my undergrad students, book knowledge is merely the first step in the journey of a professional; the challenges encountered on the job ensures one has to keep learning – there's just no amount of work in the classroom that prepares a student for the job of a CFE or CPA. As a professional, maintaining a certain curiosity and work ethic is necessary to keep learning and improving. As an adjunct instructor for some 20+ years, I've had the privilege of teaching a few different courses in the college's accounting curriculum (currently teaching cost accounting). Like anything else, one gets better with practice, and teaching is no exception. I wish I could do it over with the first few batches of students.

Q: ***Did you have any mentors?***

A: I try to emulate what I believe are the best practices, ideas and principles whether they're from those in technology, business, politics or entertainment. I don't believe any one person or group of persons knows it all.

Q: ***Do you have favorite tools, techniques or insights to share with other CFEs?***

A: Do your homework, whether it's prepping for a deposition or planning an engagement; learn the industry and the client; maintain objectivity.

Q: ***What would you tell a young professional just starting their career as a CFE?***

A: Have patience, as career growth doesn't happen overnight; prepare for opportunities – expand your leaning; integrity and ethics are paramount.

Q: ***What do you do for fun or relaxation?***

A: I play AT golf; I recommend professionals get involved in the game as it is an effective way to network. More importantly, golf teaches things about oneself that might otherwise remain latent.

Q: ***Do you have a favorite author, TV show, movie or hero of fiction that has to do with investigations/CFE work?***

A: Not particularly – I try to find something useful in whatever I read or watch. Nevertheless, there have been a few excellent eye-opening movies over the years: *Wall Street; Margin Call*; and *The Big Short* come to mind.

Q: ***What do you find most meaningful in your membership in the NYCFE?***

A: The people I've met and the speakers at events.♦ *Michael Van Sertima is a member of the NYCFE. Email: mvs@gkspc.com*

Crisis Communications in the Era of Covid-19

Laura Hynes-Keller, CFE

Economic disruption caused by the coronavirus pandemic has shocked enterprises of every size, in every industry. From a communications perspective, the impact of Covid-19 spans the three main types of crises: ***Immediate***, such as earthquake, hurricane or tornado; ***Emerging***, when the scope of crisis becomes more apparent and efforts are made to mitigate its effects; and ***Sustained***, with a continual rollout of consequences stemming from the main event.

Different types of crises can also occur at once to further complicate the situation, creating a perfect storm of trouble.

Crises such as financial setbacks; technological upheavals from power outages, data breaches, data exposures, and cyber hacks; terrorism, workplace violence, and corporate misdeeds can all wreak havoc on a company's bottom line, and reputation.

This inevitably creates extreme pressure on corporate leaders, even though the cause of the incident may be out of management's control.

For Certified Fraud Examiners, the coronavirus pandemic has activated scammers and fraudsters from around the world, some using old tactics, with others innovating with new technologies.

According to the Federal Trade Commission, there has been a significant increase in Covid-19 fraud-related activity, including economic impact payment fraud, scammers peddling cures and treatments with no proof they work, and the sale of faulty or non-existent personal protection equipment (PPE), such as masks and surgical gowns. Enterprises eager to protect employees must be vigilant in the procurement process.

Incident Response

How an enterprise responds to a crisis informs stakeholders and the public about its overall capabilities and expertise. Companies and institutions that have long standing incident response policies and procedures are well-positioned to handle communications with an array of stakeholders, from customers, employees and vendors to shareholders, boards of directors, and government policymakers and regulators.

But What If You Don't Have a Plan?

Clarity is a fundamental principle of crisis communications. But in many crises, like the Covid-19 pandemic, there is ongoing uncertainty, even panic, about what might happen next. Will a business reopen, or remain closed? If the business opens, will it remain open? Will furloughed or laid off workers get their jobs back? Will the customers come back? Will they trust your brand?

Your company may not have answers to those and other questions. Yet unanswered "bad" news can quickly deliver impactful damage on an enterprise's market share and reputation, and potentially harm its long-term viability.

Without regular communications, employees and other stakeholders will likely turn to the rumor mill, as any void is filled, one way or another.

Horror Vacui

The term, "Horror vacui," attributed to Greek philosopher Aristotle circa 300 BC, is commonly stated as nature abhors an empty space. For a PR practitioner, it is easy to pick out the "horror vacui" in the daily news cycle. Case studies cited by industry trade publication *PR Week* include WeWork (financial), Boeing (business practices), and Google and the Royal Family (reputational) as just a few examples of crisis communications efforts falling short, seriously damaging brand reputations.

Game Plan

A designated crisis response team usually involves the C-Suite, legal and heads of key business units who help assess the scope of any incident, with PR recommending an appropriate media action plan.

The media is the source of most questions relating to any crisis, but others may come from employees, shareholders and analysts. Sometimes government authorities or community leaders use the media to ask questions about an enterprise's status, policies or procedures.

Timing is a Complicating Factor

A damaging incident can happen in an instant, but it can also occur as slow, steady erosion of a company's profit center and reputation for varying reasons. Crises can happen when no one is paying attention, or when leadership's preferred risk management stance is "*We have other priorities,*" or "*I'll deal with it when it happens.*"

Then it is oftentimes too late. If the enterprise has not taken steps to anticipate crisis scenarios and map an action plan, then it is immediately playing "catchup" with media and stakeholders. The news cycle moves at warp speed. The moment for immediate and effective communications management in working to shape the narrative is time sensitive. A lack of planning inevitably results in a delayed response. In most cases, swift response to media during a crisis is

crucial to gaining control of the situation. A wire story via *Associated Press, Bloomberg* or *Reuters* can have enormous influence on how a company is portrayed.

Many local, national, and international media outlets base their own reporting on wire stories, so it is essential that reporters who may be filing the first stories obtain accurate information from the enterprise.

Media Interest in a Crisis Usually Reflects the Scope and Impact of an Incident.

At first, the media's questions will likely focus only on the immediate crisis. In general, small incidents are usually limited to basic questions, such as what, where, when and how an incident happened, who was involved, questions about the context and requests for explanations about the likely cause.

However, in a major crisis, media queries usually include a multitude of questions regarding the Company and the given project or incident.

Additional questions can emerge over time as investigative results and potential litigation matters are made public. An enterprise's risk management policies and procedures can be major theme in any ongoing media coverage.

Responding to Media

With a response plan in place, the designated team can work quickly to identify the crucial points that must be addressed, craft a strategy, draft the appropriate language, determine the manner of delivery most likely to counter the crisis at hand, then contact the media.

The company's response might range from a short, written statement or series of statements, to a full press release, to daily press briefings, or a combination of all, working on a case-by-case basis to determine the appropriate response.

In addition to traditional media channels and platforms, social media such as Facebook, YouTube or Twitter provide platforms for effective messaging and engagement opportunities, depending on the stakeholders.

However, there may be some circumstances in which it may be more beneficial for an enterprise to take a more reactive stance, and not directly address certain matters, for example, topics that may relate to any potential litigation.

Litigation Support

Incidents involving litigation that impact the bottom line and reputation of an enterprise usually require some measure of repositioning. Sometimes a company must wait until after the case is settled to comment extensively.

Countering misinformation and panic by disseminating correct messages to stakeholders and media is likely to help significantly reduce the intensity of a crisis, with the goal of returning as swiftly as possible to day-to-day business operations.

However, with Covid-19, uncertainty is the operational framework.

Call to Action

Today's communications related to Covid-19 include a "call to action" by public health experts and government authorities. Some of the preventative measures promoted to stop the spread of the disease include social distancing, hand washing, cleaning and disinfecting surfaces, covering coughs and sneezes, and wearing masks. Yet companies that do not practice even the most basic public health guidelines such as providing soap are vulnerable to complaints to the media from workers fearing infection and by the public through social media "trolling": **These Workers Packed Lip Gloss and Pandora Charm Bracelets. They Were Labeled "Essential" but Didn't Feel Safe.** ***ProPublica*****, 4/3/20.**

By pointing customers, employees and other stakeholders to expert resources, enterprises can work to avoid the reputation harming perception that leadership doesn't care. Familiar and accessible central communications hubs for employees such as Microsoft Teams, Slack, Google' s G-Suite, video conferencing platforms such as On24, GoToWebinar, Webex or Zoom, along with the Company's website, blog and social media accounts can keep employees and other stakeholders informed about resources and developments.

Media Monitoring

Issues that roll out over days, weeks, or longer require careful ongoing media relations management. The communications team continuously monitors media coverage about the crisis and provides updates on an as needed basis to executive leadership, internal and external legal teams, and, at times, board members.

Because circumstances can change quickly, having a communications plan in place can lay the groundwork for successful response implementation with media to avoid unnecessary headaches if and when an incident occurs.

To that end, developing and managing communications strategies requires forward thinking to anticipate, organize and facilitate crisis response. A good communications plan is a strong inoculation against a crisis growing out of control. ♦

Laura Hynes-Keller, CFE, is a speaker and founder of LHK Communications, LLC, a strategic advisory and media relations consultancy. Email: laura@lhkcommunications.com

European Union-U.S. Privacy Shield

Bruce H. Hulme, CFE, BAI

While this column is being written, this country and many other parts of the world are under attack by an invisible, silent, killer-disease---the Coronavirus, also referred to as COVID-19. Many of you may now be working from your homes and isolated from other family members, friends, and professional colleagues. Our work schedules have been drastically changed, as has the business world to which we have long been accustomed. Such an environment will most likely result in an increase in the number of frauds, particularly if the current situation persists over an extended period of time.

As a longstanding NYCFE board member, my role has often been concerned with legislative and regulatory issues. Examples include educating members of professional associations such as the NYCFE on the avoidance of Gramm-Leach-Bliley Act (GLBA) violations while locating assets or recovering ill-gotten gains and stolen property; compliance with the Fair Credit Reporting Act (FCRA) when conducting pre-employment and third-party workplace investigations; avoiding potential invasion-of-privacy lawsuits when conducting surreptitious surveillance or open-source intelligence and social media investigations; and the use of pretense, a recognized investigative tool when conducting interviews of witnesses and targets of investigations.

The European Union-U.S. Privacy Shield was created after two years of discussions between the U.S. Department of Commerce and European Union Commission for Justice, Consumers and Gender Equality to improve the protection of privacy around the world. It provides a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the U.S. in support of transatlantic commerce.

On August 1, 2016, the U.S. Department of Commerce accepted certifications by businesses to join and to comply with the Privacy Shield Framework's requirements. This article also reports on the disposition of a federal case prosecuted by the Federal Trade Commission against a New York company engaged in providing background checks and security services that continued to claim participation in the EU-U.S. Privacy Shield after its certification lapsed. The company conceivably stands to be monitored by the FTC for the next two decades.

The Privacy Shield Principles involve the International Trade Administration (ITA) of the Department of Commerce, which administers the program, and the Federal Trade Commission (FTC), along with the Department of Transportation providing enforcement of the Privacy Shield. Aspects of the E.U.-U.S. Privacy Shield also apply to Iceland, Liechtenstein and Norway as well.

When established in 2016, the U.S. Office of the Director of National Intelligence (ODNI) provided input regarding safeguards and limitations applicable to U.S. national security authorities. The U.S. Department of State described its commitment to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding the United States' signals intelligence practices. The U.S. Department of Justice put forth concerns regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

OVERVIEW: EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

While the United States and the European Union share the goal of enhancing privacy protection, the U.S. takes a different approach to privacy from that taken by the EU. The U.S. uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the U.S. with a reliable mechanism for personal data transfers to the U.S. from the EU while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issued these Privacy Shield Principles, including the Supplemental Principles (collectively "the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission's adequacy decision.

1. The Principles do not affect the application of national provisions

implementing Directive 95/46/EC ("the Directive") that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.

2. In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) ("the Department"). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory; organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission ("FTC"), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (other U.S. statutory bodies recognized by the EU may be included as an annex in the future); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them. The EU-U.S. Privacy Shield also applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein and Norway. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

3. The Department of Commerce will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Privacy Shield List"). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization's removal from the Privacy Shield List means it may no longer benefit from the European Commission's adequacy decision to receive personal information from the EU. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.

4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from the European Commission's adequacy decision that would enable those organizations to receive personal information from the EU. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.

5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.

8. Definitions:
a. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.
b. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
c. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

9. The effective date of the Principles is the date of final approval of the European Commission's adequacy determination.

FTC Gives Final Approval to Settlement with Background Services Provider over Allegations Related to Privacy Shield

In the Matter of T&M Protection Resources, LLC, a limited liability corporation --- On March 23, 2020, The Federal Trade Commission released the following:
Respondent T&M Protection Resources, LLC is a Delaware limited liability corporation with its principal office or place of business at 230 Park Avenue, Suite 440, New York, N.Y. 10169. The Federal Trade Commission has given final approval to a settlement with a New York company over allegations it misrepresented its participation in and compliance with the EU-U.S. Privacy Shield framework, which enables companies to transfer consumer data legally from European Union countries to the United States.

The FTC alleged that T&M Protection Resources, LLC, which provides security and background check services, continued to claim participation in the EU-U.S. Privacy Shield after its certification lapsed. In addition, the company failed to verify annually that statements about its Privacy Shield practices were accurate and failed to affirm that it would continue to apply Privacy Shield protections to personal information collected while participating in the program.

As part of the settlement, T&M is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization. In addition, T&M is required either to continue to apply the Privacy Shield protections to personal information it collected while participating in the program or to return or delete the information.

This Order will terminate twenty (20) years from the date of its issuance, (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of the Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of: A. any Provision in this Order that terminates in less than twenty (20) years; B. this Order's application to any respondent that is not named as a defendant in such complaint; and C. this Order if such complaint is filed after the order has terminated pursuant to this Provision. It provided further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

[The Order allows for pretexting the Respondent.] The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

The FTC also continued its strong enforcement of the EU-U.S. Privacy Shield framework by bringing 13 cases in 2019 against companies that allegedly made false promises related to the Privacy Shield.

FTC Releases 2019 Privacy and Data Security Update

The Federal Trade Commission on February 25, 2020, released its annual privacy and security update for 2019, highlighting a record year for enforcement actions aimed at protecting consumer privacy and data security.

For example, the Commission levied a $5 billion penalty—the largest consumer privacy penalty ever—against Facebook for violating its 2012 FTC privacy order and imposed new restrictions on the social network's business operations. The FTC also obtained a record $170 million penalty against YouTube and Google for alleged violations of the Children's Online Privacy Protection Act (COPPA). In its first case involving a stalking app, the Commission

alleged that Retina-X enabled its apps to be used for illegitimate purposes and in violation of COPPA.
On the data security front, the FTC—along with 50 states and territories and the Consumer Financial Protection Bureau—announced a global settlement totaling as much as $700 million with Equifax related to a 2017 data breach that affected approximately 147 million consumers. ♦

Bruce H. Hulme, CFE, BAI, is a Certified Fraud Investigator, Board Certified Investigator and a former Legislative Liaison Board Member New York State Licensed Private Investigator. Email: specialinvestigations@att.net

New Funding for Coronavirus SBA Loans Attracts Scammers

If you're a business owner, you may be planning to apply for a loan through the SBA's Paycheck Protection Program (PPP) or Economic Injury Disaster Loans (EIDL) program. These programs recently got hundreds of billions of dollars in new funding. But, while you're focused on getting a loan, scammers may be focused on you: hoping to trick you into giving them sensitive business information, like your bank account numbers, employees' Social Security numbers, and even your money.

Here are some "dos" and "don'ts" to help you stay clear of scammers as you apply for a small business loan.

DO:

Get information about SBA loans directly from the SBA's website: sba.gov/coronavirus.

Once on that page, go to "Funding Options" and follow the instructions.

Find more information about the PPP and EIDL programs at the U.S. Treasury Department's website.

DON'T:

Don't pay in advance for information. All the information from the SBA is free at sba.gov/coronavirus.

Don't pay in advance for a government loan. You don't have to pay up front to get an SBA loan.

Don't give your information to someone who calls, emails, or texts you out of the blue. The SBA won't call unsolicited to find out information about you or your business, or to ask you to apply for a loan. The SBA is not going to send you emails or text messages asking for sensitive information. If you get an email or text like this, delete it. It's a scam.

Don't apply for a loan without verifying the lender. Only SBA-authorized lenders can provide PPP loans, and other loans may be available through SBA directly. To find an SBA-authorized lender in your area, use this SBA tool.

Don't click on links or reply to emails or text messages from someone you don't know. If you click on the links, you could download malware to your computer or device or be connected to a scammer or hacker.

Warn your staff, too, to be alert for spoofed emails and bogus calls. And, if you or your employees spot a scam, please let us know at ftc.gov/complaint.

Demystifying the Investigation Process

Anthony J. Luizzo, Ph.D., CFE, CST, PI (Ret. NYPD) and John M. Gaspar, BAI, CFE

GENERIC DEFINITION OF AN INTERVIEW

Over the years, investigators have come up with several generic definitions for the investigative exercise. Our definition: An investigation is the medium through which facts are discovered, gathered, preserved and prepared as evidence for legal proceedings.

THE DIFFERENCE BETWEEN AN INTERVIEW AND AN INTERROGATION?

An interview is a leisurely conversation with a person of interest, which can rise to a fact-finding excursion where warranted. An interrogation is a probing conversation with normally unwilling or unknowing subjects to extract secretive information. The primary objective of the interrogation is to obtain incriminating evidence and ultimately get to the truth of what happened.

A WINDOW INTO THE INVESTIGATIVE PROCESS

One of the tenets of the investigative process is to gather as much pertinent information as possible during the interview. Oftentimes, the interview is analogous to a written play, and the interviewer and interviewee are the lead actors. The interplay between both is like a well-rehearsed symphony, wherein the interviewer tries to marry the apparently connected to the unconnected and the interviewee tries to either answer the questions forthrightly or attempts to dance around the truth. The investigative process follows the universal academic learning model: "Assess the facts, criticize assertions and integrate conclusions." From the business perspective, private investigators often call this exercise "connecting the dots" or "peeling the onion." As the layers of the onion are pulled back, the onion begins to reveal its true nature. Whether performing a law enforcement or business-related interview/interrogation, it's most important to always come to the interview or interrogation prepared. Being prepared includes, but is not limited to:

- Using control-type questioning—a control question is an incident related query intended to elicit a psychological response
- Observing kinetics
- Establishing rapport
- Controlling the flow of the interview
- Allowing uninterrupted dialogue
- Keeping an open mind
- Following the facts wherever they may lead.

Investigative experts instinctively know that active listening is the fulcrum upon which effective interviews are constructed. Often the interviewee is ready and able to tell what he or she knows, and interviewers should always allow him or her to tell their story uninterrupted. At times, interviewees are not interested in cooperating. In these instances, the interviewer needs to wear two hats and try to conduct both the interview and interrogation in one session. This takes tremendous skill and should only be performed by seasoned sleuths. The interrogation, on the other hand, is a formal session designed to elicit a confession of guilt and involves probing and extracting information from an unwilling subject by asking trenchant questions. The objective is to seek evidence and an admission of responsibility or guilt. The interviewer needs to leave the impression that the incident at hand has already been solved and that the interviewee is somehow involved.

INTERVIEW TYPES:

Initial Interview: Identifies the circumstances surrounding the incident, lists possible witnesses/suspects, catalogs physical evidence, and classifies the incident as a crime, civil event or as an informational report.

Canvass Interview: Usually completed as a follow-up to the initial interview and involves canvassing of neighborhoods, searching out witnesses, and following any and all possible leads. Oftentimes these canvasses are door to-door inquires of residences, business establishments, bus stops, delivery carriers (Federal Express, USPS, Parcel Post, etc.) and transportation companies (Uber, taxi cabs, car services, buses). In many instances, the canvasser is searching for evidentiary materials, including video camera footage, eye or ear witnesses, or any related information that can shine further light on the incident under scrutiny.

Victim Interview: Often involves searching for the who, when, why, how and where of the incident. Witness Interview: The objective of these interviews is to obtain eyewitness information from a wide variety of locations (stores, apartment complexes, shopping malls, etc.) captured during the initial interview, leading to sketch characterizations and other evidence-related exhibits.

Suspect Custodial Interview: The questioning of a person regarding their involvement or suspected involvement in a criminal offense or offenses. As a matter of course, suspect interviews are performed by law enforcement officers as part of their regular criminal justice process.

Non-Custodial Interview: These interviews are usually performed by private security personnel and are fact-finding exercises. In this type of interview, it's important that the interviewer establishes rapport with the interviewee and ensures that the interviewee is comfortable and relaxed.

NATIONAL VS. INTERNATIONAL INVESTIGATIVE CONSIDERATIONS

In a June 1995 article by the undersigned, "Investigating in a New Environment" in *Security Management* Magazine, discusses the unique differences associated with performing investigations in foreign lands. It's important to recognize that performing investigations and conducting interviews and interrogations abroad can be perilous. Because many corporations have multi-national footprints, the way interviews and interrogations are performed internationally should be carefully researched. First and foremost, it's imperative that investigative professionals entering these markets understand that they pose a markedly different, and sometimes dangerous, cultural and legal landscape. Many issues that are taken for granted in domestic investigative interviewing and interrogating exercises must be addressed in the context of the host country's political, legal and cultural climate. One of the most important issues that needs to be researched before interviewing and/or interrogating anyone is to seek legal counsel and check out the host country's legal system thoroughly. Every country has its own legal system, which affects all aspects of the criminal and civil justice process, including security and investigations. These systems vary greatly from country to country. Permissible investigative approaches in Mexico may be prohibited in France, for example. Protections that are taken for granted in the United States pertaining to search and seizure, self-incrimination, Miranda Warnings, interview taping, etc., most likely are quite different than our justice system requirements. The major exceptions to this rule are the United Kingdom and India. The U.S. legal system is an outgrowth of the English common law system, and many of the principles of the American justice system apply there. Beyond the legal system, it is equally important that the investigative specialist become extremely familiar with the host country's culture and language. It's also important that the investigative professional read as much about the host country as possible before endeavoring to jump in and perform any due diligence excursions.

It's imperative that investigative professionals entering these markets understand that they pose a markedly different, and sometimes dangerous, cultural and legal landscape.

THE HOMEWORK PHASE: ASPECTS OF PREPARING FOR THE INTERVIEW OR INTERROGATION

The key to ensuring success is being prepared. A successful interview and/or interrogation begins and ends with getting all your ducks in a row before beginning the exercise. Before contacting a witness or the subject of an investigation, whenever possible, review police and civilian reports and CSI reports, as well as comprehensive background, social media searches and computer-assisted dispatch (CAD) reports on the subject and location. If possible, talk directly to the responding officers and/or interested parties to obtain detailed accounts of the incident. Finally, it's most important that the interviewer determine whether one-party or two-party consent is required for electronically taping potential proceedings. This is especially important if electronic taping will be part of the investigative envelope.

PREPARING FOR THE INTERVIEW:

- Pre-plan interview questions
- Put the interviewee at ease—develop a rapport • Structure interview questions so that they are easily understood
- Show a personal interest in the interviewee
- Always keep interviews conversational
- Listen carefully to verbal and non-verbal dialog
- Refrain from interrupting the interviewee
- Determine information requirements before beginning the interview
- Schedule interviews at the time of the day when you have the most personal energy
- Select an interview location that is free from distractions
- Always allow ample time to conduct the interview
- Always maintain control of the interview flow
- Try to establish rapport with the interviewee
- Always accept emotive responses without criticism
- Refrain from taking extensive notes during the interview – shorthand helps
- Refrain from interrupting the interviewee
- Always leave the door open to follow-up interviews
- Obtain a written statement of facts at the conclusion of the interview
- When using interpreters, make sure that all communication takes place between the interviewer and

interviewee, not between the interpreter and the interviewee

NOTETAKING TIPS

- Refrain from trying to write verbatim responses—audio- or videotaping should be practiced whenever possible (in many states you need to let all parties consent to the being recorded)
- Avoid becoming distracted by your notetaking
- Always preserve interview notes for future use

SHORTHAND NOTETAKING SUGGESTIONS

- Q&A: question and answer
- RQ: repeat question
- RA: repeat answer
- IE: interviewee
- IR: interviewer
- IW: interview
- MVI: motor vehicle information
- PI: police information
- AKA: aliases
- MPH: miles per hour
- POB: place of birth
- DOB: date of birth
- NA: not applicable
- ID: identification
- CM: crime method
- ICB: internal control break (fraud and audit term)
- SSF: security system failure
- AF: audit failure (fraud and audit term)
- SF: security failure
- BSR: background search required

INTERVIEW METHODS

- Good Guy – Bad Guy: One interviewer attacks the interviewee while the other defends
- Role Reversal: The interviewer reverses roles with the interviewee, e.g., "If you were looking into this matter, what would you do?"

INTERVIEW TECHNIQUES

- Pregnant Pause: Asking a question … pausing—this often-uncomfortable silence creates the opportunity for the interviewee to continue conversing
- Trade-Off Technique: Offering a promise of helping the interviewee by suggesting that their assistance will be taken into consideration later, if necessary
- Breaking Down the Story Technique: The gradual process of obtaining the truth by pointing out inconsistencies in the facts, thus hopefully getting the interviewee to make broader remarks and possible admissions
- Graceful Exit Technique: Allowing the interviewee to furnish excuses for their behavior by offering a sympathetic ear, thus keeping the door ajar for future interactions

DECEPTIVE BEHAVIOR TRAITS: TYPES OF LIARS

- Panic Liar: Rarely wishes to face the consequences of his or her confession
- Occupational Liar: Has lied for years—it's a way of passage
- Tournament Liar: Loves the challenge lying brings
- Ethnological Liar: Taught over the years to never squeal on another
- Sadistic Liar: Will never give the interviewer the satisfaction
- Psychopathic Liar: No conscience whatsoever

HELPFUL INVESTIGATIVE HINTS

More astute interviewers never fail to take special notice of clothing, jewelry, tattoos, accents and other personal identifiers. To the perceptive sleuth, a college ring identifies schools attended; sports jackets, elbow patches and button-down shirts signify possible academician affiliation; bow ties often signify non-conformist characteristics; lapel pins showcase organization and association affiliation; the list goes on and on. It really pays to observe!

PERFORMING DUE DILIGENCE: TESTING INFORMATION ACCURACY

Once the interview and/or interrogation is completed, it's time for fact-testing. Each assertion offered during the interview and/or interrogation must be truth-tested. Witnesses must be located and interviewed, background checks and related due diligence performed, tips and leads verified, etc.

CONCLUSION

In the court of protection wisdom, conducting interviews and interrogations is truly both an art and a science. The art involves setting the proper environment and stage for the interview, whilst the science embodies using your observation and intuitive abilities to capture the ever-elusive truth. Interviewers spend countless hours probing, examining, researching, listening, observing and pondering before they tear a page from their "RX" pad and begin preparing their final report.

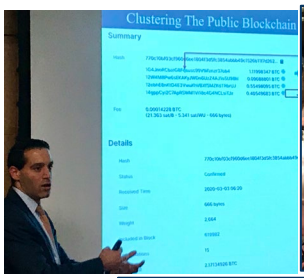
References: Lyman: publisher Pearson 6th edition ibsn# 3-978-0-13- 506057-5 https://pressbooks.bccampus.ca/criminalinvestigation/chapter/chapter-9-interviewing-questioning and-interrogation/ Luizzo, A. Van Nostrand G.: "Investigating in a New Environment" – Security Management Magazine – June 1995. Luizzo, A. "Interview Vs. Interrogation": Financial Fraud Report – Warren Gorham & Lamont / RIA Group Reuters – Thomson Publications – December 1999. Luizzo, A., Calhoun, C., "Fraud Auditing: A Complete Guide": The Foundation for Accounting Education / New York State Society of Certified Public Accountants – 1992, Rev. 1995.

Reprint Courtesy Professional Investigator Magazine November/December 2019

Anthony J. Luizzo. PhD, CFE, CST (Ret. NYPD), Member: Board of Directors, Vault Verify, Inc. Email: anthony@vaultverify.com

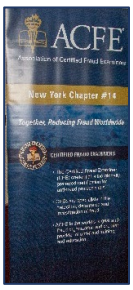
EVENT PHOTOS

NYCFE Seminar / Fordham University / March 9, 2020

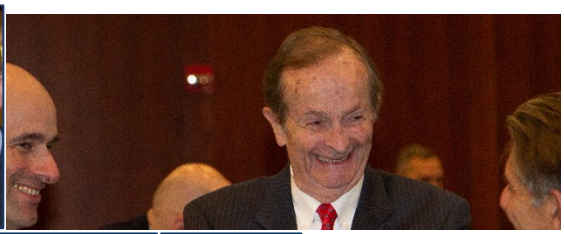


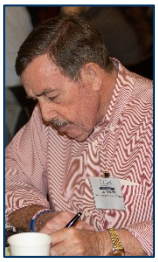
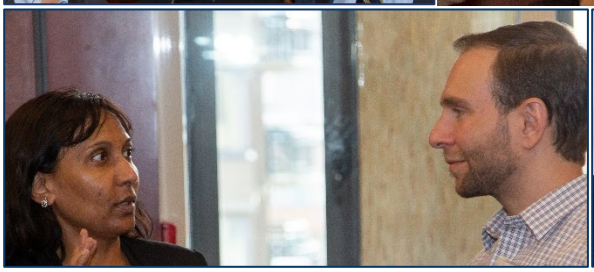
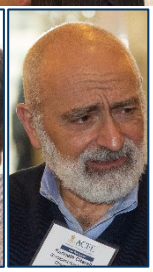


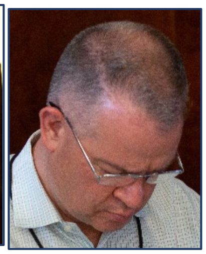
NYCFE Full Day Conference / Fordham University, Oct. 18, 2019



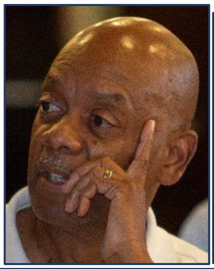




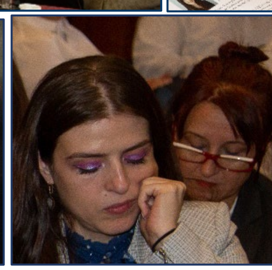
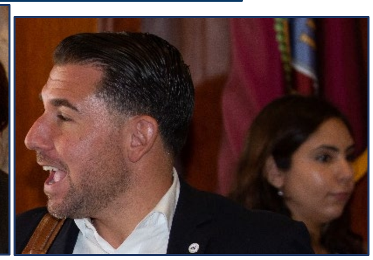
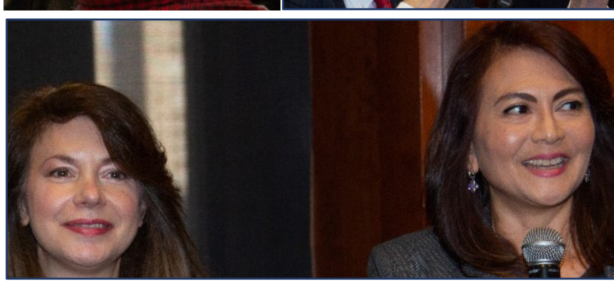










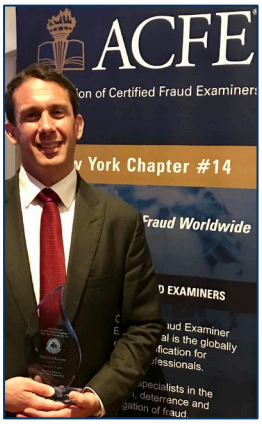

The NYCFE Thanks Our Fall 2019 Fraud Conference Event Sponsors

FORDHAM UNIVERSITY
THE JESUIT UNIVERSITY OF NEW YORK

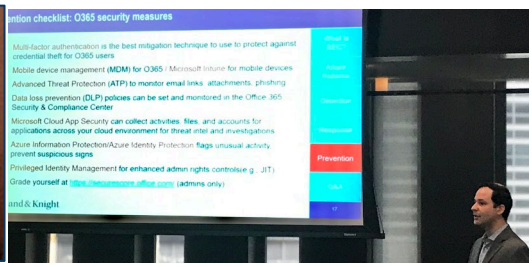
LIFARS
your digital world, secured

SATELLITE investigations
Get results, not excuses

NYCFE Seminar
Battery Park Gardens
Sept. 10, 2019



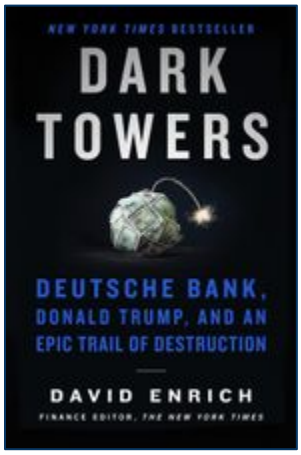
NYCFE & NY Metro Infragard Joint SeminFordham Univ. / July 17, 2019



NYCFE Seminar / Fordham University / May 22, 2019

BOOK CORNER

Editor's Picks for Suggesting Readings

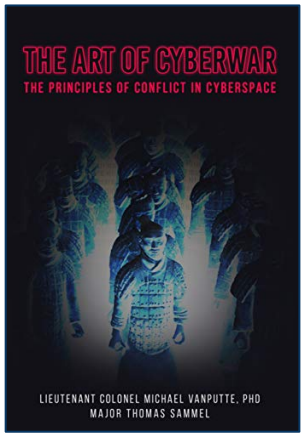


Dark Towers

By David Enrich

#1 *WALL STREET JOURNAL* BESTSELLER * *NEW YORK TIMES* BESTSELLER

New York Times finance editor David Enrich's explosive exposé of the most scandalous bank in the world, revealing its shadowy ties to Donald Trump, Putin's Russia, and Nazi Germany. Enrich is the author of the 2017 bestseller *The Spider Network: The Wild Story of a Math Genius, a Gang of Backstabbing Bankers, and One of the Greatest Scams in Financial History.* The book details the "LIBOR scandal," the fraudulent activity exposed in 2012 which involved bankers around the world manipulating the London Interbank Offered Rate (LIBOR) for profit.



The Art of Cyberwar: The Principles of Conflict in Cyberspace

By Michael A. VanPutte and Thomas Sammel

The information superhighway promised to connect the world's people. After thirty years we find governments, criminals, hacktivists, and amateurs using this man-made domain to attack other governments, defense contractors, commercial businesses, national infrastructures and social media. Public and private organizations spend billions of dollars struggling to defend themselves. Yet attacks continue. A lack of understanding the complexities of cyberspace and the nature of the conflict has led to a field based on myth, metaphor and wishful thinking. National leaders, corporate board members and executives, information security professionals, and average citizens should be concerned about the threats we face in cyberspace. Using clear English, "*The Art of Cyberwar*" describes the digital battlefield and the principles for conducting defensive and destructive operations. It provides the reader insights into the complexities and principles for maneuvering in the digital domain.

Now is a great time for you to volunteer and participate more fully in our NYCFE Chapter.

You can become more involved with event planning, recruitment, social media, and more!

For more information, please contact Dora M. Gomez at president@nycfe.org

❖

The NYCFE Newsletter is Designed and Edited by Laura Hynes-Keller

Special Thanks to All Authors

The opinions and statements contained in the articles are those of the authors and not necessarily of the NYCFE or its board of directors.

SUBMISSION GUIDELINES: We welcome submissions from current and affiliate NYCFE members including professional achievements and milestones, photos of CFE's at work or signifying accomplishments, original bylined articles, opinion pieces, case studies, links to pertinent research papers with an executive summary, along with additional tips, book recommendations, resources or suggestions in fraud prevention, detection and deterrence. Word count limit 2500. Photos and illustrations can accompany submissions. Publication of articles at editorial discretion.

Please email Newsletter@nycfe.org with submissions, questions, or comments. Thank You.

Things gained through unjust fraud are never secure.
Sophocles