ACFE®
Association of Certified Fraud Examiners
New York Chapter #14

SPRING / SUMMER 2019, ISSUE 3

TABLE OF CONTENTS

Photo courtesy: LHK

LETTER FROM THE PRESIDENT

Dear Members,

I am pleased to welcome you to our Spring / Summer 2019 newsletter. I would like to share an update on our meetings and events this year.

First, I would like to acknowledge the talented individuals who have contributed to our newsletter. We are pleased to feature their original content regarding timely, fraud-related topics.

Our mission at the NYCFE is to provide high quality continuing professional anti-fraud education and networking opportunities. True to our mission, our events this year have provided several high-quality events for our members. So far, we have hosted several "sold out" meetings, including a breakfast meeting and a spring conference, where attendees earned CPE credits. We have welcomed high quality speakers at these events, who have delivered incredible anti-fraud training. At the conference, attendees won amazing prizes, including ACFE branded merchandise, books, and CFE Exam Prep courses.

If you did not win a prize, don't worry, there will be several more opportunities coming up. At our fall conference, we will also have special prizes for attendees. At the end of this year, we will also

Chelsea Binns, President

be giving away a ticket to the ACFE conference and two tickets to our NYCFE conference to members who have attended the most chapter events this year.

Right now, we are actively planning our fall conference to be held on Friday, October 18.

We are very excited to welcome Bruce Dorris, President and CEO of the ACFE to deliver our keynote address. This event is going to be very popular and capacity will be limited. I suggest signing up early to secure your spot. Please stay tuned for updates and information on how to register. If you would like to be a sponsor for this event, please contact: president@nycfe.org.

We are also working on updating our website, to better serve our members. The new site will feature an updated layout and

will provide a better member experience. We think you will really like it, and we look forward to unveiling it by the end of the year.

Membership Drive

There is no better time than now to become active in the NYCFE and begin enjoying the benefits of membership! Our membership drive is ongoing, and if you are not already a member, I invite you to join our chapter.

Becoming a member of the NYCFE provides an opportunity increase your anti-fraud knowledge and make new friends and professional contacts across an array of industries.

To apply, please use this NYCFE member application link.

We invite current members to refer a friend; once a friend signs up, members will receive a special gift as a "thank you" for the referral. Please have the new member provide your name on their application form, and a gift will be sent to your designated address.

Working together, we can continue to make a difference in the fight against fraud.

On behalf of the entire board of directors, I would like to thank you for your support. We look forward to seeing you at a future meeting.

Chelsea Binns
President, NYCFE

❖

❖

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 Chelsea Binns: 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

President: Chelsea Binns, Ph.D., CFE, LPI
Vice President/Training Director: Dora M. Gomez, MS, CFE, CRMA, GRCP
2nd Vice President/Treasurer: Judy Shalini Juan, CFE, CFCS, CPA
Recording Secretary: Ozan Gurel, CFE
Corresponding Secretary: Emmah Padilla, CFE
Chairman of the Board: Jonathan Newcomb, CFE
Chair Emeritus: Michael Richard Powers, Esq., CPA, CFE
Director/Legislative Liaison: Bruce Hulme, CFE, BAI
Member at Large/Past President: Alan I. Blass, CPA, CFE, PC
Member at Large: John Reuther, MBA, CPA, CFE, GISF GISF
Member at Large: Laura Hynes-Keller, CFE
Past President Directors: Steven R. Levine, CFE
Ernesto Castillo, CFE
Noel Barreto, CFE
President Emeritus: Anthony Luizzo, PhD, CFE, CST, LPI
Chapter Counsel: Kenneth C. Citarella, Esq., CFE, CIPP

Nine Questions with...JOHN REUTHER, MBA, CPA, CFE

John has more than seventeen years of law enforcement experience derived from a combination of federal and state investigations as well as private investigations. During that time, John has also managed numerous technology implementation projects, including the design and development of an internal IT system used for Agency-wide restructuring efforts. Currently John is assigned as an investigator to a federal task force charged with the responsibility of investigating financially motivated cyber-crime. His investigative experience includes email compromises, malware/ransomware, ATM intrusions, Point-of-Sale compromises and credit/debit card fraud, among others.

John has been on the board of Directors of the NYCFE for eight years, including four as the Treasurer. He holds a Bachelor's in Accounting, a Master's in Economic Crime, and is a Certified Public Accountant, Certified Fraud Examiner and an FBI authorized Digital Extraction Technician.

Q: *How did you develop an interest in becoming a Certified Fraud Examiner?*

A: My interest in fraud investigations began immediately after high school when I accepted a part-time job as an insurance fraud investigator for a small private investigations firm in New Jersey. It didn't take long for me to get hooked. I remember catching my first fraudster, a claimant with severe back injuries, power washing his roof in broad daylight. Not only did I become addicted to the hunt, I learned that one of the largest motivating factors of the criminal mind is financial gain. I also learned that I needed a bridge to fill the gap between Law Enforcement and the traditional teachings of accounting in college. I felt the CFE was that bridge. It is specialized enough to combine Law Enforcement with financial analysis but broad enough to touch on all aspects of fraud; it is a mile wide and an inch deep. It was the perfect first step in my career as a financial crime investigator.

Q: *What skills or education best prepared you for conducting investigations at the nexus of financial crime and technology?*

A: While studying accounting I became most interested in the concentration of Accounting Information Systems. This included the tools used to create financial statements as well as systems designed to report metrics on large datasets of financial information. These skills developed into a knack for relational databases and structured query language. Before I knew it, I found myself in the unique situation of possessing an educational background in accounting and information systems, while working for one of the greatest Law Enforcement agencies in the world. This combination of skills presented unique opportunities to test and evaluate new and emerging law enforcement technologies as well as develop reporting standards for crime statistics. Looking back, my step away from investigations and into technology project management ultimately led me to investigating financially motivated cyber-crime.

Q: *Did you have any mentors? If so, what kind of mentoring experience did you find useful?*

A: Not specifically, but as an investigator, I was trained to always keep my ears and eyes open and be willing to learn something new from anyone. Everyone can teach you something--even if that something is what you should NOT do; you just have to listen.

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

A: Learn through doing; don't be afraid to assist on cases where you lack experience. This area of investigations can be very humbling. The average person thinks a financial crime investigator knows all things financial crime, but the truth is that it evolves so quickly and so often that it can be very difficult to keep your finger on the pulse. There are various blogs, news threads and seminars but I feel the best way to be aware of the threats is to involve yourself in as much case work as you can. I don't think there is an investigator in the world that would turn away a helping hand and in return, there is always much to learn. As Richard Branson said, "If somebody offers you an amazing opportunity but you are not sure you can do it, say yes – then learn how to do it later!"

Q: *Ransomware and Business Email Compromise (BEC) present ongoing challenges for leadership in every industry, as well as for not-for-profit entities. What are key steps CFE's can take to help their teams?*

A: I cannot stress enough the importance of email security. I am frequently shocked by the resourcefulness of criminals and their ability to leverage information from an inbox. Ransomware and BEC's can both be deployed through email campaigns but that is the end of their similarities. Regarding ransomware, there are virtually no guaranteed preventative methods. Most ransomware campaigns result in one choice for businesses owners to access their own information: a large payout. If that is not an option, the only other alternative at this point in the lifecycle of ransomware defense techniques are redundancy and/or offline remote backups. On the other hand, I feel that businesses have much greater control in mitigating losses stemming from BEC's. Our Fraud 101 class taught us that the separation of duties and having proper checks and balance are the first steps in prevention. It's no different in the case of a BEC. Every business should have in place a well-defined process for the initiation of wire transfers.

Here are a few steps to consider: Do not share private identifying information via email; have a two factor authentication system in place; require at least two approvals for the initiation; and lastly, a simple phone call (dialing the number saved in your phone, not the number provided in the email) to the recipient to confirm the account information, goes a long way.

Q: *Many recognize the utility of distributed ledger technologies, the underlying "blockchain" infrastructure that supports cryptocurrencies. However, some influential business leaders, money managers and economists have called cryptocurrencies a "delusion," comparing the industry to the Dutch "tulip mania" of the 1600's. What are your views? Are cryptocurrencies here to stay?*

A: First, I am not an investment advisor, and this is not investment advice. That being said, it is important to differentiate between investing in cryptocurrency such as Bitcoin and investing in crypto companies that develop the technology used to support cryptocurrency. Purchasing cryptocurrency such as bitcoin is purely speculative, and I do not feel the currencies should be included in an investment portfolio (unless gambling is considered an investment strategy). However, the substantial demand that exists for cryptocurrencies is based on factors other than the traditional investment model of increased earnings. People demand crypto for the anonymity it provides, the combination of high risk, high reward stakes as well as the technology itself. And for these factors, as opposed to increased earnings, I do feel that demand for crypto will continue to be high enough to support its ongoing existence and expansion. Moreover, I feel that the demand for the underlying technology is in its infancy and has great potential for expanding well beyond its current uses.

Q: *Hacking cryptocurrency exchanges is on the rise; industry researchers recently estimated cyber criminals generated around $1 billion in revenue in 2018. What are your views about cryptocurrency exchanges, and the safety of investments?*

A: Any connected device or virtual account is hackable, but the likelihood is based on the criminal's perceived value of the resulting reward (which may be financial, political, vengeful, or otherwise). Due to the value of cryptocurrencies along with the anonymity it provides, I believe crypto will always be a prime target for theft. In my view, one of the factors in determining the likelihood of a hack is based on the intent of the investor. If an investor's main objective is anonymity, then that investor would be more inclined to utilize an exchange in a jurisdiction with less regulation. These jurisdictions, however, tend to provide less prosecutorial protections due to the lack of structured system of justice, thereby increasing the potential risk of loss. Given how calculated cyber-criminals are, they will likely consider this lower risk of attribution when choosing their victims. On the other hand, exchanges based in the U.S. (or other well-regulated locales) are better regulated, supported by a well-defined criminal justice system and are themselves held accountable to U.S. laws. These factors afford less anonymity but lower the risk of loss. Based on public reporting, there has not been a major hack resulting in financial loss to a U.S. based crypto exchange since 2014. My personal advice to those who want to invest in a market that is not insured or regulated, use an American-based exchange.

Q: *Decentralized Finance (DeFi), the nascent decentralized financial system built on public blockchains, is attracting more interest. Do you have any perspective to share about DeFi with our CFE community?*

A: As I mentioned above, the underlying technology supporting cryptocurrencies, i.e. the Blockchain, has enormous potential for expansion. I anticipate this expansion to occur well beyond the financial industry. The Blockchain delivers a solid foundation for checks and balances, and can also provide for quality assurance, among other

attractive solutions. Some of the areas I anticipate the Blockchain supporting include, inventory control, claims processing, currency transfers and personal identification, among others. I highly recommend that fraud professionals begin familiarizing themselves with the details of a Blockchain. CFE's should be aware of the infrastructure of a Blockchain, the type of data a particular Blockchain retains, how and where it stores data and the steps to extract data, among other items. The devil is always in the details, and one tiny detail buried in a Blockchain might have great meaning in a case.

Q: *What are your views about coding skills for CFE's? Do you foresee CFE's learning coding languages such as Python and R as essential?*

A: No, I do not see those types of skills as essential. However, I would recommend being familiar with them to the degree that you can identify the different languages and their uses and locate any information in the coding that might assist in an investigation. My reasons are because they can be difficult to learn and very easy to forget if not used routinely. Secondly, 99% of the time your basic spreadsheet application will suffice. Most importantly, investigations are not conducted by one person, they require a team effort. A team assembled with varied skills. I may be a CPA and CFE, but right now in my career I am an investigator first. I rely on forensic accountants as well as computer scientists on a routine basis to provide me with detailed, actionable intelligence. I feel that scripting languages are specialized skills reserved for people who use them routinely. ♦

**Nine Questions provided by the editor.*

SEC UPDATE

This year Securities and Exchange Commission voted to adopt amendments to modernize and simplify disclosure requirements for public companies, investment advisers, and investment companies under the FAST ACT mandate. These amendments, announced in a March 2019 press release, are expected to benefit investors by eliminating outdated and unnecessary disclosure and making it easier for them to access and analyze material information.

Among other things, the amendments:

• Simplify disclosure or the disclosure process, including changes that would allow registrants to omit confidential information from most exhibits without filing a confidential treatment request, and changes to Management's Discussion and Analysis that allow for flexibility in discussing historical periods;

• Revise rules or forms to update, streamline or otherwise improve the Commission's disclosure framework by eliminating the risk factor examples listed in the disclosure requirement and revising the description of property requirement to emphasize the materiality threshold;

• Update rules to account for developments since their adoption or last amendment by eliminating certain requirements for undertakings in registration statements; and

• Incorporate technology to improve access to information by requiring data tagging for items on the cover page of certain filings and the use of hyperlinks for information that is incorporated by reference and available on EDGAR.

Inline XBRL

On June 28, 2018, the SEC adopted amendments requiring the use, on a phased in basis, of Inline XBRL for operating company financial statement information and fund risk/return summary information.

Viewing Inline XBRL filings is simple and does not require any specialized software because the Commission has incorporated an Inline XBRL Viewer into the Commission's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. Anyone using a recent standard internet browser can view an Inline XBRL filing on EDGAR. (Recent standard internet browsers are ones that fully support HTML 5 and JavaScript, such as Chrome 68 and later, Firefox 60 and later, Safari IOS 11 and later, Microsoft Edge Windows 10, and Internet Explorer 11.)

This 5-minute video demonstrates some of the features and capabilities of the open source Inline XBRL Viewer.

FTC: *A Force to Fear?*

With Perspective on GDPR & CCPA; Investigative News Update

By Bruce H. Hulme, CFE, BAI, Legislative Liaison Board Member

Although much of my federal government affairs activity is spent with reference to Congressional legislative issues, my monitoring of federal agencies and their regulatory roles over the activities of investigative professionals are equally important.

One such regulatory body is the Federal Trade Commission (FTC). It not only enforces provisions of the Fair Credit Reporting Act (FCRA) that affect employment background checks and workplace investigations, it has played a key role with reference to privacy issues, such as pretexting, information brokers, security breaches, and the like. Since the enactment of the FCRA in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, it expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace.

The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, with regard to a wide variety of other laws, ranging from the Clayton Act to the Fair Credit Reporting Act. Under more than 75 laws, it pursues a vigorous law enforcement program, and the impact of its work is significant; its competition enforcement program is critical to maintaining competitive markets across the country. The FTC is expanding its role in the prosecution of illegal business practices and in some cases imposes draconian monetary sanctions that can cripple a business.

As part of its mission to protect consumers, the FTC also tracks down and curtails some of the most egregious scams that prey on consumers, including criminals who promote business opportunity scams, deceptively pose as the government or well-known tech companies, or blast consumers with illegal robocalls. It has also brought cases challenging false and unsubstantiated health claims, including those targeting older consumers and individuals affected by the opioid crisis.

The Commission's primary source of legal authority in the privacy and data security areas is Section 5 of the FTC Act, which prohibits deceptive or unfair business practices. Under that section and other authorities granted by Congress, it has aggressively pursued privacy and data security cases in many areas, including information brokers, children's privacy, financial privacy, health privacy, and the Internet of Things.

To date, the Commission has prosecuted over 65 cases alleging that companies failed to implement reasonable data security safeguards, and more than 60 general privacy cases. Recent prosecutions under the Children's Online Protection Act (COPPA) against the operators of the online websites and a video social networking app resulted a settlement of a $5.7 million civil penalty, the largest COPPA penalty ever. The FTC alleged that they violated the COPPA Rule by failing to obtain parental consent prior to collecting personal information from children, as well as failing to protect children's personal information. The FTC's complaint also alleged that the company stored and transmitted users' personal information in plain text, failed to implement an intrusion detection and prevention system, and failed to monitor for potential security incidents. As a result, a hacker accessed the personal information of approximately 2.1 million users, including 245,000 users under the age of 13.

Section 5 is not without its limitations. It presently does not allow the FTC to seek civil penalties for the first offense. It also excludes non-profits and common carriers from the Commission's authority, even when the acts or practices of these market participants have serious implications for consumer privacy and data security. Senator Ron Wyden (D-OR) has introduced a bill in the Senate to address some of these issues. The House is also doing the same. I expect that members will offer privacy and data security legislation enforceable by the FTC, which would grant the agency civil penalty authority, targeted rulemaking authority, and jurisdiction over non-profits which would be an expansion of its powers.

The U.S. SAFE WEB Act is integral to the FTC's international work on consumer protection and privacy matters. Enacted in 2006 and renewed in 2012, the Act strengthens the FTC's ability to investigate cases with an international dimension. It allows the FTC to share evidence and provide investigative assistance to foreign authorities in cases involving spam, spyware, misleading health and safety claims, privacy violations, data

security breaches, and telemarketing fraud. During the last fiscal year, the FTC cooperated in 43 investigations, cases, and enforcement projects with foreign consumer, privacy, and criminal enforcement agencies. It works through global enforcement networks, such as the International Consumer Protection and Enforcement Network, the Global Privacy Enforcement Network, the Unsolicited Communications Enforcement Network, and the International Mass Marketing Fraud Working Group.

An example of data security enforcement is the FTC's settlement with Uber Technologies over their alleged failure to reasonably secure sensitive consumer data stored in the cloud. As a result, an intruder allegedly accessed personal information about Uber's customers and drivers, including more than 25 million names and email addresses, 22 million names and mobile phone numbers, and 600,000 names and driver's license numbers. Uber suffered a second, larger breach of drivers' and customers' data in 2016, and failed to disclose that breach to consumers or the FTC for more than a year, despite being the subject of an ongoing FTC investigation of its data security practices during that time. The final FTC order prohibits Uber from misrepresenting how it monitors internal access to consumers' personal information and the extent to which it protects personal information, with the threat of strong civil penalties if it fails to comply.

In 2018, the FTC resolved allegations that PayPal's Venmo peer-to-peer payment service misled consumers about their ability to control the privacy of their Venmo transactions and the extent to which their financial accounts were protected by "bank grade security systems." Another FTC initiative launched last fall resulted in hearings that examined whether broad-based changes in the economy, business practices, technologies and other developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy. Since then, the FTC has heard from over 350 panelists and received more than 850 public comments.

On May 8, 2019, the Federal Trade Commission testified before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce about its "efforts to effectively protect consumers and promote competition, while anticipating and responding to changes in the marketplace." Testifying on behalf of the Commission, were FTC Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips, Rohit Chopra, Rebecca Kelly Slaughter, and Christine S. Wilson. In essence they stated that the FTC is "committed to using its resources efficiently to protect consumers and promote competition through law enforcement, policy and research, and consumer and business education." They indicated that FTC law enforcement actions have helped return more than $1.6 billion to consumers during fiscal year 2018. FTC regulators received a sympathetic understanding at the congressional hearing, and will no doubt receive greater powers and funds to police privacy by way of increased fines against large aggregators of personal identifying information.

Although not specifically mentioning Facebook, Commissioner Rohit Chopra indicated that for large companies, fines are merely a "parking ticket." The FTC is aiming to increase sanctions against Facebook, including taking action against CEO Mark Zuckerberg personally to hold him in account for Facebook's failure to honor a 2011 agreement over past privacy lapses regarding its mass user base.

California Consumer Privacy Act (CCPA)

California's Consumer Privacy Act (CCPA), signed into law in 2018, follows a growing line of consumer privacy laws, such as the European General Data Protection Act (GDPR), Canadian Breach of Security Safeguards Regulations of the Personal Information Protection and Electronic Documents Acct (PIPEDA), and related New York Department of Financial Services Cybersecurity Rules and Regulations (NYCRR-500).

Like its European GDPR counterpart, California's privacy act establishes consumer rights and corporate responsibilities, which will be enforced with penalties up to $7,500 per violation. As motivation for the law, the California Act notably cites the tens of millions of people whose personal data was misused by the data mining firm Cambridge Analytica, a greater desire to heighten data privacy controls and transparency of data practices, and the people's desire for privacy and more control over their information. The Act, which becomes effective on Jan. 1, 2020, could have a serious impact on the economic models of many companies collecting and reselling data to other parties. Transparency in data movement and resale will open the eyes of consumers who, until now, blindly agree to user contracts and never question why an app on their phone needs access to their location, contacts, or other services.

Some of the specific provisions of the Act include:

- Full disclosure regarding the collection of personal information, including details of the collected information, sources, the purpose, whether the data is disclosed or sold to another party, and if so, the third party's details.
- An opt-out right to prevent a business from selling their personal information to third parties.
- The right to be deleted (like with GDPR's right to be forgotten) by

having their information wiped-off servers.

The Act mandates traceable transparency of consumer data collection, use, distribution, and the GDPR-like right to be forgotten. These requirements must be made public through general policy, by specific request, and cannot form the basis of bias or discrimination on the part of the business. A company cannot tie goods or services to the ability to resell consumer information or offer discounts or other incentives in exchange for this ability. This moves consumer privacy rights from the domain of *often ignored* fine print to the front page.

The GDPR now in force among European Union country members, among other provisions, mandates that companies notify data-holders of a breach within 72 hours. It also gives E.U. residents the "right to be forgotten" by having their data wiped off a company's servers. In the U.S., there is no comparable federal law that governs how all states handle data breaches and protects consumers' information. Expect that there will be measures offered in the 116th Congress to enact such with federal preemption over state security breach laws.

INVESTIGATIVE NEWS

Bribery

The latest report on global corruption enforcement from TRACE International shows the number of foreign bribery enforcement actions by the U.S. has increased by 50 percent over last year, while the number of investigations by Europe has grown so much that they now account for more than half of all foreign bribery probes.

The Global Enforcement Report (GER): Updated annually, the **GER** features graphic and textual analyses of all known enforcement events—including investigations and enforcement actions —since the first bribery cases were prosecuted in the United States following the enactment of the U.S. Foreign Corrupt Practices Act.

Despite the global denunciation of bribery, little information is publicly available on enforcement of anti-bribery regulations. This can make it difficult to recognize trends concerning the extent to which countries are enforcing anti-bribery laws or where bribery is most prevalent, even though such information is critical to promoting transparency in global business. TRACE publishes the **GER** annually to provide this essential information.

Key findings from the 2018 GER

While the number of open U.S. investigations into foreign-bribery allegations dropped slightly in 2018, there was a notable increase in the number of open investigations worldwide, with an expanding range of investigating countries. Europe saw its number of open investigations climb by approximately 37 percent, and the region now accounts for more than half of all foreign-bribery investigations.

The past year saw a notable growth in U.S. enforcement, with the number of U.S. enforcement actions increasing by more than half. The pace of enforcement actions by non-U.S. authorities remained essentially steady.

There was also an increase in the number of investigations concerning bribery of domestic officials by foreign sources, showing a rise of approximately 15 percent. The total cumulative number of domestic enforcement actions also demonstrated a healthy growth of approximately 22 percent.

The Financial Services industry remained the most heavily investigated by United States agencies in connection with foreign-bribery allegations, accounting for approximately 17 percent of all such investigations. In other jurisdictions, however, the focus remained elsewhere—most prominently the Extractive Industries, Engineering/Construction, and Aerospace/Defense/Security—with Financial Services accounting for only 6 percent of open investigations. ♦

2019 Verizon Data Breach Investigations Report

Corporate executives are increasingly being targeted by cybercriminals because of their access to data and ability to engage in social engineering, according to the 2019 Verizon Data Breach Report recently published. The report was based on the analysis of 41,686 security incidents in 2018. It noted 2,013 of those reports were confirmed data breaches. The analysis shows executives were compromised in 20% of data breach incidents studied in 2018. Also, 71 percent of data breaches were financially motivated, according to the report, and the median amount stolen in business email compromise scams was $24,439. The report also noted that 57 percent of total breaches took more than one month to discover. ♦

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

Clinical Approach to Crime Detection

By Anthony J. Luizzo, Ph.D., CFE, CST, PI (Ret. NYPD)

Licensed private investigators play a vital role in helping their clientele decipher both reactive and proactive crime-related risk exposures. Investigative firms that do not have a strong background in proactive crime control planning and security simply offer reactive solutions to identified crime problems.

Alternatively, investigative firms with extensive expertise in proactive crime control planning offer a much broader selection of services from both the reactive and proactive universe of security services. Having the capacity to offer both proactive and reactive crime solving techniques is a much wiser business model; especially in today's turbulent world.

This is especially true for corporate security in the business sector where security-enhancement dollars are scarce. One of the central reasons why security dollars are scarce is because oftentimes in the business sector security is not considered a profit contributor, but rather an expense that CFOs must keep in check.

Contradicting this premise however is an age-old truism: "*an ounce of prevention is worth a pound of cure.*" Companies may be saving money at their peril!

The technical definition of proactive crime control planning

Proactive crime control planning, aka crime prevention, is commonly defined as the anticipation, recognition and appraisal of a crime risk and the initiation of an action to mitigate identified risks. Security firms and corporate entities that employ community crime control planners (CCCP) have a step-up on their competition in that they have an internal capability to capture crime exposures before they have an opportunity to wreak havoc and possibly devastate a company's reputation and standing within the mercantile community.

Three recent articles authored by the undersigned speak to how the security survey is the go-to investigative tool often used by investigative firms to uncover business-related crime risk exposures, and the third article offers a menu of low-cost security enhancement strategies to help in the never-ending war against criminal wrongdoing:

- "The Security Survey: An Investigative Tool – Part I & II": Issues 156 /159 – *PI* Magazine
- "Squeezing the Most from you Security Dollar" – The Texas Investigator Magazine: Spring 2018

Is there a need for proactive crime control?

The simple answer is a resounding YES! Contemporary issues such as budget cuts, revenue shortfalls, terrorism, computer hacking, social unrest, and political tribalism among other issues, have left many security administrators searching for new and innovative approaches to crime control.

Fashioning a proactive security program

The building process begins by the investigative company pulling either one or two investigative operatives from the investigative assembly line and properly school them in the ABCs of proactive crime risk management. During their studies operatives are taught to evaluate crime risk exposures and formulate strategies to mitigate identified exposures. (This is an especially difficult aspect of training since many operatives are quasi-law enforcement/security-oriented candidates who work in a reactive role and are rarely asked to come up with proactive crime reduction remedies – it's simply not their job.)

Over and above education in theoretical proactive security axioms, operatives are taught to apply crime prevention and environmental design concepts and strategies utilizing today's sophisticated security technologies and machineries. The process begins by selecting the right candidate to work in this role. Selection criteria should include candidates who possess above-average reading and cursive skills and have the ware withal to get up in front of small and large audiences and effectively deliver the proactive security message effectively.

Sample proactive security curricula might include but should not be limited to:

- Introduction to today's new millennium security technologies
- Introduction to crime prevention 101
- Introduction to physical security 101
- Aspects of applying environmental design concepts
- The role of the crime prevention specialist
- Developing employee and/or citizen participation
- Using metrics in security evaluation and planning
- Evaluating programmatic impact

Tasks and responsibilities of proactive security advocates

In the main, proactive security advocates perform the following tasks:

- Preparation of security surveys
- Reviewing and analyzing incident reports, employee hot-line missives, complaints and other relevant correspondence
- Preparing and presenting lecture programming and special exhibitions
- Networking with facility engineers and architects on security design issues
- Reviewing the functionality of existing security systems
- Maintaining and/or establishing a security / safety library
- Conducting and/or updating facility security surveys. It's important to note that security surveys be prepared on an annual schedule to ensure that security and safety issues remain adequate
- Maintaining accreditation by taking required continuing education credits

Programmatic evaluation

A system of evaluation needs to be promulgated so that the actual program effect is accurately measured. It's most important that a schedule of before and after studies is developed to help determine actual crime level reporting numbers, decipher crime patterns, promulgate / maintain crime mapping initiatives, and help decipher crime dispersion patterns. All in all, a structured program of evaluation should accurately measure the entity's response to proactive crime control planning and the long-lasting effects of the promulgated strategies.

Using metrics in security planning

To better understand the role that metrics can effectively play in security and safety planning, the undersigned coauthored a trilogy of articles that directly address this issue: "An Alternative View in the Development of Security Metrics" -Vol. 31., No 2 - 2015 / "Resources Available for Applying Metrics in Security and Safety Programming" – Vol. 32., No. 1 – 2016 / "Applying Metrics to 21st Century Healthcare Security" - Vol. 33. No. 2 -2017: Journal of Healthcare Protection Management: a publication of the International Association for Healthcare Security and Safety. These three articles offer a roadmap to follow when using metrics in the security and safety habitat.

The financial value of using metrics

It's only recently that many security executives have begun speaking the language that all CFOs know and understand when going hat-in-hand asking for additional security dollars for their facility. In competent hands, metrics can vividly show fluctuation in service delivery variations, enhancement options, and service curtailment calamities among other yardsticks. As a practical matter, CFOs understand numbers very well (they usually are bean-counters), and security administrators need to make their case for additional dollars by showing simple verifiable facts to support their case. Support documentation includes: Response time inconsistencies, incident report upsurges, criminal activity spikes, calls for service hikes, square footage comparisons vs. other similar facilities, conjoining incident rates to visitations, and conjoining incident rates to response durations. These and other yardsticks will go a long way in justifying security expenditures to the individuals who control the company's purse strings.

The role that robotics might play in security management

Robert J. Gordon a professor at Northwestern University in his excellent work "Rise and Fall of American Growth: U.S. Standard of Living Since the Civil War": Princeton University Press, 2016 – whilst speaking of the possible use of robots in a wide variety of applications outside of the manufacturing and warehousing sectors including: supermarkets, restaurants, and hospitals; hypothesizes that the sixty million dollar question we should be pondering is: what role will robotics play in all industries in the coming decades? If innovation is said to drive commerce, I expect that robotics will have a central role in the coming decades simply because security technologies are becoming smarter and smarter. Just think how far we've come when the simple doorbell and smart phone can bring us into the inner environs of our home or business, whilst we are thousands of miles from the scene!

Looking to the future:

Private investigators and corporate security administrators should strongly consider establishing a proactive crime control operation that can effectively diagnose crime risks before they are able to breed further devastation. Community crime control planners serve as the agency's advocate to spread the gospel that "security is every one's responsibility". CCCPs also help senior security management make the financial case to CFOs that security is a profit center and not simply a cost contributor.

A final thought:

Security executives always have an extremely hard time trying to champion how much crime they averted, using Metrics could help make your case!

References:

- National Crime Prevention Institute: "UNDERSTANDING CRIME PREVENTION" - Butterworths – 1986
- C. Ray Jeffrey: "CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN" – Sage Publications – 1977
- K brown – Blog Entry "5 Steps for Creating a Proactive Security Plan": http://ibm.conres.com – June 2, 2016
- T Scholtz – "Seven Techniques for More Proactive Risk and Security Management" – https://cdn.ttgtmedia.com – 2014
- G Connell – "5 Benefits of Having a Proactive Incident Response Plan" – http://info.garlandheart.com/blog/5-benefits-of-having-a-proactive-incident-response-plan ♦

This article is reprinted with permission from PI Magazine; (Jan/Feb '19) issue.
Anthony J. Luizzo. PhD, CFE, CST (Ret. NYPD), Member: Board of Directors, Vault Verify, Inc. E: anthony@vaultverify.com

Auditing Construction Megaprojects: *Challenges Facing Internal Auditors*

By Nauman Rauf, CFE, CIA, CCSA, CRMA, CCA

How do we define Megaprojects?

Megaprojects are large-scale, transformational, complex ventures that cost $ 1 billion or more, take years to develop and build, involve multiple public and private stakeholders and partnerships that impact millions of people. As such, megaprojects require large amounts of capital and financing for their development and maturity, along with long-term commitments. Some of the largest construction megaprojects are usually in aerospace or energy, including hydroelectric dams and facilities, while others include bridges, tunnels, highways, railways and mass transit systems, etc.

Challenges Facing Internal Auditors

Internal Auditors face challenges auditing construction megaprojects both from the developer's, and the contractor's perspectives. Adopting suitable and effective audit strategies can assist auditors in overcoming the challenges which may emerge in different shapes and forms throughout the audit cycle:

• Since Megaprojects are capital intensive, they require independent and separate investment and financing decisions. They require large project funding from lenders, and their consortiums, or through public funds in the public sector. Executive, line management, and all related stakeholders must roll up their sleeves and accept the challenge of successful and timely development and maturity of a megaproject. The respective stakeholders should understand the importance of project management controls and processes, and their overall continuing governance role in the megaproject development.

Operational management at various levels must be aware of problems in their areas of expertise and jurisdiction and rely on independent assurance and audit recommendations brought by internal auditors. The Head of Internal Audit should work closely with executive management, and the Board of Director's Audit Committee members, to understand their expectations in terms of final deliverables for megaproject audits. The Internal Audit Department has the mandate to lead and execute the audit program for the business entity and should perform up to the expectations both executive management, and the Audit Committee to discharge their governance responsibilities effectively.

• The Head of Internal Audit needs to work closely with operational management to design and visualize the conceptual framework for conducting audits of megaprojects. Without an effective conceptual framework, the auditee may not be convinced or perceive the value of the benefits and rationale for conducting the audit of a megaproject.

• Developing effective audit methodologies is key to providing assurance to all stakeholders, consistent with their expectations. Stakeholders expect to receive value-added audit recommendations on project management controls, processes and procedures to improve the overall control environment and governance.

• The Head of Internal Audit needs to make a professional judgement on the types of audits required for megaprojects. These audits effectively use the approved conceptual framework as terms of reference and criteria for performing meaningful analysis and objective evaluations to arrive at reasonable conclusions for areas under review. The suggested audit tests could include high-level governance health checkups and comprehensive audits, including a combination of operational, financial and technical audits. This may require the services of subject matter experts, along with regulatory compliance and internal corporate procedural compliance audits. Audit procedures should be effectively designed to achieve the audit objectives.

• Large data is available for audit review due to various reporting layers involved. Data could include progress reports, construction reports and updates, financial

reports, management reports and executive updates. A risk-based audit approach can only be applied if these large data sets are reviewed properly to capture the risky areas on a real time basis.

• Another relevant challenge is to identify the number of key players and groups working together as a team to build the megaproject. Internal auditors should hold meetings with all involved groups during each stage of the audit process including planning and fieldworks. Significant time will be spent on coordination with all these groups including holding exit meetings to discuss the audit recommendations, obtaining their management responses, and action plans. These working groups can be identified on the face of the project's organizational structure. Other participating supporting departments may include personnel from the following departments:

  - o Construction managers
  - o Project managers
  - o Commercial managers and quantity surveyors
  - o Architects
  - o Project accountants
  - o Safety engineers
  - o Risk management group
  - o Project procurement

• Megaprojects require multiple years for their design, development and maturity. Internal auditors should be conscious of the timing of audits, since construction activities are fast paced in nature and every day the ground situation and site conditions may change with the progress of the construction work. The audits should be planned carefully to cover those years or multiple years wherein substantial and major construction activity is planned. This effective part of strategy will allow auditors to provide assurance on the major segments of the megaproject under construction.

• Megaprojects are often characterized by multiple remote locations and sites under construction and off-site facilities. Internal auditors should ensure that the major working sites and off-site facilities are covered for audit purposes where construction activity is in progress at the time of audit review.

• A team of auditors should be assembled and assigned to perform audits in line with the approved audit scope. The team should be proficient and composed of experts to achieve audit objectives. These may include professional auditors, accountants, professional engineers and safety experts, etc. The internal auditor should research additional best practices for construction auditing to provide advice on varied alternatives to improve risk management and control.

• Adequate time budgets should be allocated for performing the audits effectively. Travelling to multiple locations at various times is time consuming. Yet, a proper balance is essential in allocating for the time budget between the strategic planning stage, field work, and audit reporting, to maintain consistency and deliver value.

• The internal auditors should be knowledgeable of applicable legislation and statutory regulations for safety in the geographical location of the megaproject. Maintaining a safe work environment at the project should remain a main consideration for management and highlighted as part of their corporate strategy. In-depth knowledge of safety practices and legislation will enable auditors to determine the degree of compliance with safety regulations, and laws, and identify opportunities for improvement through process benchmarking.

• Value-added auditing principles require the auditors to identify opportunities for cost savings and cost avoidance for the megaproject under construction. A review of the following areas could uncover opportunities for potential cost savings and make a difference at the bottom line:

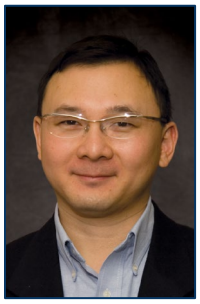
  - o Procurement of steel and permanent materials
  - o Change orders
  - o Progress billing and payment applications and reconciliations
  - o Progress reporting of work
  - o Equipment rentals
  - o External hiring of specialized and skilled labor through manpower companies
  - o Insurances and bonding
  - o Consulting agreements

Challenges faced by internal auditors in auditing construction megaprojects provide an opportunity for continuous learning and can assist with increasing specialized knowledge and practice. Therefore, these challenges should be seized upon and transformed into opportunities to deliver value. ♦

Nauman Rauf (CFE, CIA, CCSA, CRMA, CCA), an EY alumnus, has worked with large U.S.-based contractors, Fortune 500 companies, and multibillion-dollar Canadian corporations in senior leadership internal-audit roles during his professional career, which included stints in North America, the Middle East and North Africa. Currently, he is Senior Consultant at Auditax NYC Consulting and can be reached at info@auditaxnyc.com.

What CFEs Can Do About Digital Ad Fraud

By Augustine Fou, Ph.D., Independent Cyber Security and Ad Fraud Researcher



What is Digital Ad Fraud?

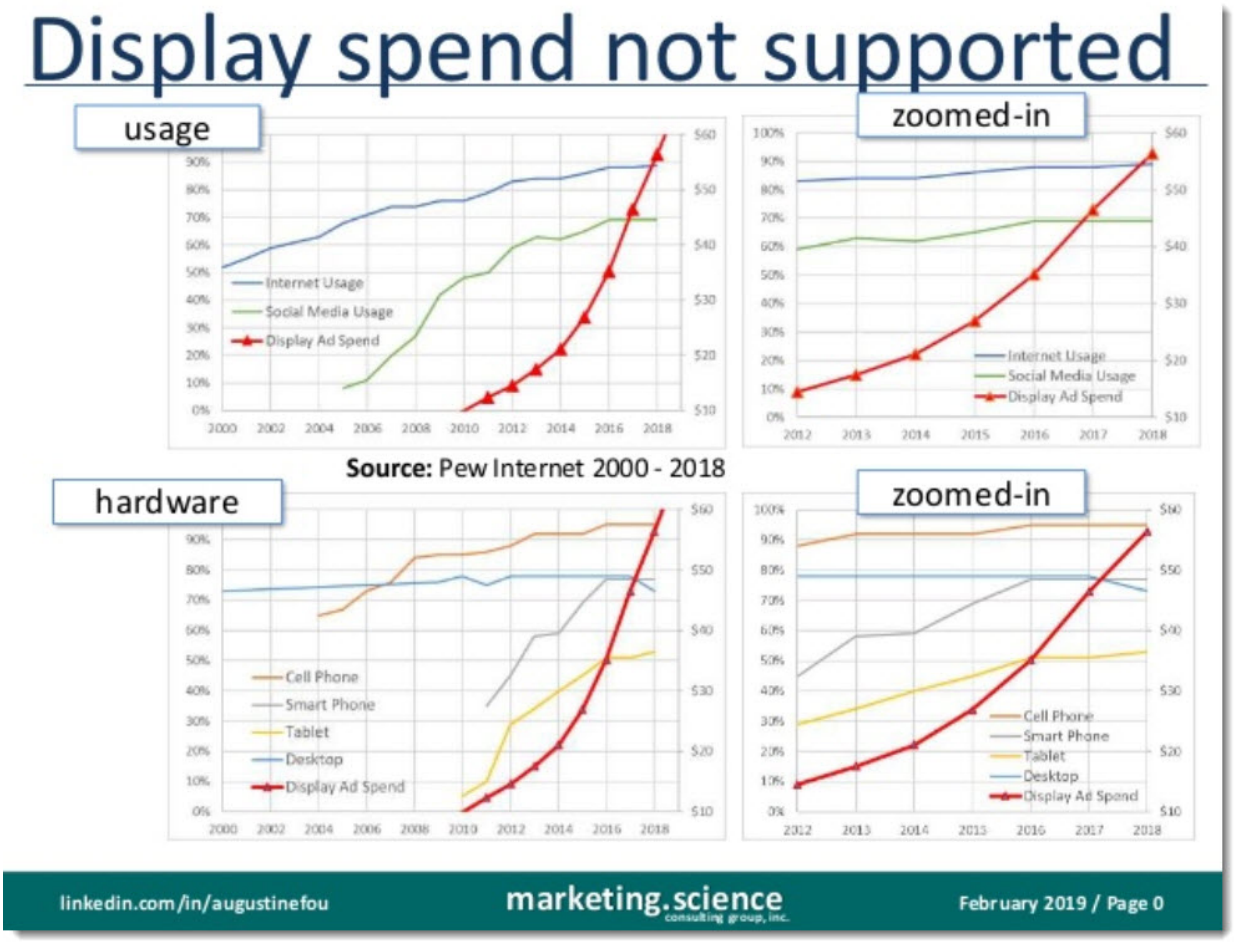
Answer: Ads shown to bots instead of to humans.

Online advertising started in earnest in the mid-90s when websites sold ad space on their web pages to advertisers.

The assumption at the time was that ads would be shown to humans who visited the website; the ads would load when the web pages loaded. Fast forward 20 years to the present and we see nearly 100 trillion ad impressions bought and sold every year.

The assumption that ads are shown to humans is no longer; some of those ads are definitely NOT shown to humans. There simply aren't enough humans on earth, or enough time in a day, for such enormous quantities of ad impressions to be created by humans looking at web pages, using mobile devices, or consuming media.

The chart below shows that usage of the Internet and social media has plateaued and the usage of hardware such as desktop computers, tablets, and smart phones have all plateaued as well. But the red line (display ad impressions) shows a "hockey stick" shape that cuts vertically upward through the other lines. The rapid growth of display ad impressions is not supported by the growth in the usage of hardware or the internet.



So How Do So Many Ad Impressions Get Created?

Answer: Fraudsters register millions of domain names, stick some "ad tech" code on the page, and start generating ad impressions using bots (software programs that repeatedly load the web pages) – in other words fake websites with fake traffic causing fake ads to load.

Ad fraud is unique to digital advertising in both its size and scope because there are none of the physical constraints of the offline world. Offline, you can only stick a finite number of billboards by the side of the road; and offline fraud included examples like print publishers inflating circulation numbers to get more ad revenue. In digital, however, virtually limitless numbers of fake websites can be created to carry limitless quantities of digital ads, because there are no physical limits.

How Do We Know Something Strange is Happening?

Answer: We can observe the trend that prices in digital advertising have gone down for most of the last 20 years, despite billions of dollars flowing into digital from other forms of advertising. Given this surge in demand for digital ads, if the supply of ads were constrained, prices should have gone up. But instead, prices have gone down consistently because the supply surged even faster than the demand.

This surge in supply is not supported by 1) the growth in numbers of people coming online, 2) more people using more devices, or 3) the increase in time spent with various forms of media. The supply surge was created by fraudsters seeking to cash in on digital ad spending.

Further reading:
https://www.linkedin.com/pulse/digital-ad-fraud-101-2019-cybersecurity-ad-fraud-researcher/

Why Isn't Ad Fraud Detected?

Answer: Fraudsters are very good at avoiding detection and covering their tracks; and many of them use technology to help them do this.

Fraudsters would not be fraudsters if they abided by laws, followed the rules, and did things "above board." These white-collar criminals are using various technology tools to take advantage of the opportunity to make tons of money from digital advertising simply by creating "ad inventory" out of thin air and selling massive amounts of these ad impressions in ad exchanges.

Advertisers, after all, were demanding more reach and more frequency. The fraudsters' technology tools are also good enough to avoid detection, cover their tracks, or actively manipulate measurement (https://www.buzzfeednews.com/article/craigsilverman/newsweek-ibt-malicious-code-ad-fraud) to make everything look "valid."

The fraudsters are getting away with it because, on paper, it appears that the advertiser got tremendous quantities of ad impressions at incredibly low prices. The advertisers are happy. The media agencies that did the buying for them are happy. In fact, they may even have gotten bonuses for helping to get more quantity at lower prices.

There is a parallel to counterfeit goods here – some folks are very happy to buy a counterfeit LVMH handbag, because it looks like the real thing, but is one tenth the cost. And some might even object to actions that might eliminate or reduce the availability low-cost handbags and low-cost ads.

Advertisers also think that ad fraud doesn't affect them. For those that do know about ad fraud, they justify continuing to buy digital ads by saying "fraud is priced in." They think that because they are paying $3 for every thousand ad impressions, rather than $30 per thousand, that fraud is somehow acceptable. The point they are missing is that now they are buying 10 times the quantity of ads at $3, compared to when they bought at $30. So, they are not spending any less or saving any money. They are in fact buying a lot more fake ads that will never produce any business outcomes.

This is like a consumer who thought they bought a real Rolex watch, only to find out it was a counterfeit one.

Finally, even the advertisers who are concerned about fraud are lulled into a false sense of security when industry trade associations issue press releases saying ad fraud is low and going down and they are "winning." This is inaccurate because it is like saying the crime rate of an entire city is low and going down because the crime rate of one house was low and going down; this was the one house that was observed. The claim is inaccurate because it assumes that all forms of fraud were measurable and taken into account. There are many forms of ad fraud; good guys have simply not discovered them yet.

Further reading:
https://www.linkedin.com/pulse/your-ad-fraud-verification-vendor-ripping-you-off/

Why Hasn't Ad Fraud Been Stopped?

Answer: Just like before the financial crisis, all the banks were making so much money, no one wanted it to stop; in digital advertising, the large quantities created by ad fraud are making a lot of people a lot of money, so no one wants it to stop.

In digital, too many ad-tech companies are making money; too many people who work at ad-tech companies don't want to lose their jobs. Ad fraud dramatically inflates the quantities of ads that flow through the system and practically every company in the supply chain makes more money when there is more volume. If fraud were reduced, then the volumes would be reduced. So, most ad-tech companies have an incentive to keep the status quo and not disrupt this money-making machine.

How Big is Ad Fraud?

Answer: There have been many estimates over the years, ranging from $9 billion to $19 billion. The most recent estimate from Juniper Research is $42 billion lost to fraud in 2019, worldwide. While the exact amount of fraud is hard to estimate from different data sets, what is well known is the amount of digital ad spending. In the U.S. digital advertising surpassed $100 billion in 2018, and globally digital is over $330 billion. Whatever the fraud number, the dollar amount of ad fraud is large.

Yet it hasn't been solved. Just as it was during the financial crisis, even the ratings agencies were in on it – they rated the junk bonds triple-A, so everyone felt comfortable continuing to buy. In digital, the trade associations and certification bodies make advertisers comfortable in continuing to buy from ad-tech companies that are labeled "certified." Unfortunately, these "certifications" are entirely useless, because companies are allowed to self-attest that they are clean, honest, and fraud-free. They complete the paperwork, pay the fees, and get their "certified against fraud" logo. These loopholes make it easy for bad guys to continue operating in broad daylight, because advertisers think they are certified. Keep in mind the tragedy of the Boeing 737 Max, when the FAA allowed Boeing to self-certify. (https://www.washingtonpost.com/investigations/how-the-faa-allows-jetmakers-to-self-certify-that-planes-meet-us-safety-requirements/2019/03/15/96d24d4a-46e6-11e9-90f0-0ccfeec87a61_story.html?noredirect=on&utm_term=.b131c611b9cf)

Bad guys are not necessarily Russian, Chinese, or Korean hacker gangs. While there are hackers who make and maintain large botnets, they are usually not the ones committing ad fraud. Instead, they simply rent out their botnets to generate traffic that fraudsters buy to commit ad fraud.

Remember, fake sites have no traffic, so they have to buy all their traffic in order to create ad impressions. Also, some companies may find that "sourcing traffic" is the only way to reliably increase ad revenues when their human audiences grow too slowly to drive the desired revenue increases. And in other cases, an ad exchange may have committed to selling a certain quantity of ad impressions, contractually ahead of time. What happens if they are running behind and are at risk of not hitting their numbers? In a panic, they go out to buy traffic so they can make their number. But common sense will dictate that there aren't large numbers of humans sitting around with nothing to do but to go to specific sites when they are told to. Therefore, everyone is incentivized to keep everything going as it is.

What Can CFE's Do?

Answer: Read up on digital ad fraud and identify specific cases of fraud that can be documented and stopped.

Did you know there are no laws against digital ad fraud? Really, there aren't any. But why is what we described above considered ad fraud? Very simply, it's because the ads are not what the advertiser thought they paid for (ads shown to humans). The one case that made headlines in 2018 was the FBI indictment of eight individuals for ad fraud. However, they were not indicted for ad fraud; they were indicted for computer crimes and identify theft because they used malware on devices to load ads, and for stealing credentials and personal information.

But vast amounts of ad fraud don't involve malware on devices or stealing of personal information. Bots from data centers load the web pages of sites hosted in data centers. All of this simply drives huge numbers of ad impressions, reported in excel spreadsheets and paid for by millions of dollars of digital ad spend.

CFE's should push for detailed reports and greater transparency in digital ad spend accounting and reporting -- e.g., who got paid, where did the money go, etc.
With detailed reporting, CFE's can also look for discrepancies -- for example, the difference between campaign reports and ad server reports.

More specifically, when a bid is won, an ad should be served -- so there should be a 1-to-1 correspondence. The impressions in the campaign reports should match up with those in the ad server reports. If they don't, CFE's should investigate.

Even though there are no laws against ad fraud, other laws may have been broken to commit ad fraud -- for example wire fraud, conspiracy to commit fraud, aggravated identity theft, and financial fraud such as money laundering. There may also be securities fraud when artificially inflated user numbers (fake accounts) are used to inflate revenue growth numbers that drive stock valuations.

One thing is certain: fraudsters commit fraud. Whether it is by using bots to create fake traffic or fudging numbers in the books, they actively look for opportunities to exploit to make themselves rich, while costing honest businesses, both large and small, large sums of dollars.

Together CFE's can help to find fraud in digital advertising, close the loopholes, and thus protect legitimate businesses and their digital investments. ♦

Dr. Augustine Fou is an affiliate of the NYCFE who will present at the NYCFE's Fall 2019 Fraud Conference, where he will share analytics and case examples of how ad fraud was found and reduced, saving clients millions of dollars. Dr. Fou earned his Ph.D. in Materials Science at MIT. He a published author and adjunct professor at Rutgers and NYU. Email: augustine.fou@gmail.com

A Las Vegas CFE Who Loves New York

By Kyle Johnson, CFE

Except for a handful of New York City CFE's, I personally have not met most of you in person. As some of you read this, many might think it to be a little strange that a CFE from the Las Vegas area is a member of the New York Chapter #14.

There are several reasons for this, so let me explain. During my very first time in New York (during which I attended my first annual CPE session), I absolutely fell in love with it. I mean I truly have a great affection for all of New York City and everything it has to offer. The people, the neighborhoods, the vibe – it's all exciting to me and although I now have been three times, and will be back again in the fall, I know I have only witnessed a small portion of what it has to offer and want to keep experiencing more and more each time.

Another reason I joined the New York chapter is because of my friend, and chapter member, Laura Hynes-Keller, whom I met the first time I was at a CPE session. She couldn't say enough good, positive comments about this local organization, and encouraged me to join as there are so many great members and educational opportunities.

So, I thought why not? What a tremendous opportunity to meet and network with more of my peers in a city that has quickly become my favorite.
During my twenty-three plus years working for a financial institution, I have always been fascinated in not only how fraud is perpetrated, but also how it's detected, and the investigation process itself. I have worked financial institution fraud cases for approximately fifteen of those twenty-three years. My role has also branched out into internal auditing, as well as overseeing compliance, risk management and BSA.

Several years ago, while attending a credit union specific conference, another attendee told me about an organization called the Association of Certified Examiners, of which he was a member.

He explained in detail the organization's mission and goals, as well as the networking, educational and employment opportunities. He also explained that it could be somewhat of a challenging process to earn the CFE credential, but the result was well worth the time and effort, and quite an accomplishment. Other than letting this conversation recline in the back of my mind for quite some time, I did not proceed.

Fast forward a couple of years later, and I finally decided the timing was right to put forth the effort and begin the journey to earning the CFE credential. I attended the week-long CFE exam review course in Los Angeles and was, to say the least, a little overwhelmed by the amount of material and the examinations involved in the process. But the plethora of fraud types and different topics that were covered was some of the most fascinating subject material I had ever listened to in a classroom setting (just as interesting as when I obtained my bachelor's degree in Criminal Justice). The ACFE instructors were not only knowledgeable about the information presented, but they were passionate about the intent of the organization itself and the commitment by all members to fight fraud. Ultimately, I passed all four exams and earned the credential.

Being a part of this organization has been a tremendous experience. My one wish would be to use the education I have gotten, and the credential itself, and be able to apply it even more in my day-to-day job duties. It has helped with some of the financial fraud investigations I have been responsible for, but I know there is so much more to applying the skills and knowledge I worked for.

Currently, my primary responsibilities are compliance, risk management and BSA, and fortunately my organization does not have a multitude of fraud cases. But applying this specific education and learning from other CFE's who are experienced in fraud examinations would be exciting as well.

Thank you for allowing me to be included in your local organization. I will always welcome dialog with additional members of the New York City chapter, and although I cannot attend the global conference this year, I am open to connecting with anyone should they visit the Las Vegas area, or the next time I am in New York. My name is Kyle Johnson, and I am not only a proud member of the ACFE itself, but I am also a proud member of the ACFE's Chapter #14 in New York City. ♦ *Kyle Johnson, CFE investigates financial fraud. Email: skjohnson2@centurylink.net*

Data Literacy and the Experimental Mindset

By Laura Hynes-Keller, CFE

In today's marketplace, navigating a company's ocean of data to extract valuable insights is increasingly vital to the strategic positioning and ongoing success of an enterprise.

As companies seek new levels of competitive advantage, businesses of all types and sizes are capitalizing on new insights extracted through data mining, with aim of strengthening and gaining market share and winning new business.

Data Literacy, merged with an *Experimental Mindset*, can contribute to the design of exciting approaches to data modeling and products.

Since many structured and/or unstructured datasets contain hundreds of millions of records, the sheer volume of available data calls for fresh thinking and innovation. Efforts to foster critical thinking about the datasets, aimed at capitalizing on business opportunities, can also offer a platform to employers for cultivating both individual expertise and team functionality.

> *"Over 2.5 quintillion bytes of data are created every single day, and it's only going to grow from there. By 2020, it's estimated that 1.7MB of data will be created every second for every person on earth."*
> *Domo, Inc. Data Never Sleeps Report, Sixth Edition*

Data, Data Everywhere

Presently myriad personal technology products, services, gadgets, apps, gaming, mobile and other devices launch at dizzying speeds, with each set to continually generate data.

But it's not just connected individuals producing approximately 1.7MB of data every second.

Each linked car on the road, vessel on the ocean, plane in the sky, and satellite orbiting the earth steadily brings forth reams of data every moment. Adding to the constant data generation are businesses that outsource operations to third-party vendors for "managed services" such as:

- Blockchain as a Service (BaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

For example, Salesforce, which provides customer relationship management software (CRM) via its Software as a Service (SaaS) platform, uses Amazon Web Services (AWS) for Infrastructure as a Service (IaaS), resulting in the collection of multiple layers of data at the enterprise level.

As a result of these combined technological advancements, the scope of available data far surpasses what was imaginable in 1989, when the term "*Knowledge Discovery in Databases*" was first introduced.

Data Literacy

Acquiring proficiency in data matters includes knowledge of its descriptive terminology, such as:

- Volume (*amount*)
- Variety (*types and sources*)
- Velocity (*speed*)
- Validity (*accuracy*)
- Volatility (*length of time data is stored*)
- Veracity (*quality & trust*)
- Variability (*range*)
- Value (*results*)

Yet data literacy encompasses more than knowing definitions, utilizing certain software tools, or AI/Natural Language Processing (NLP) and/or Machine Learning/Deep Learning methodologies, when accessing, cleaning, visualizing and analyzing datasets.

It involves a willingness to think about and consider data in new ways, by developing an experimental mindset.

Cultivating an Experimental Mindset

Because technology changes so quickly, employees working at every level of a company must be nimble in adapting to "the new," especially as data literacy migrates from mostly IT and operations research "silos" into business units spanning an enterprise.

Empowering those shifts requires a company's leadership to set a "tone at the top" that encourages "thinking outside of the box" in order to foster creativity and innovation, while being mindful of data privacy and cybersecurity matters.

Integrated with emerging business principles such as "agile" project management, featuring adaptability, rapidity, quality, and cooperation, it can be very challenging for employees to keep pace with

evolving business practices and ongoing tech changes, all while balancing regular job assignments. While many easily adapt to an increasingly digital environment, others struggle with learning new technologies and concepts centered around data mining.

Fostering a culture featuring an "experimental mindset" can lessen stress around learning and help cultivate new ideas and inventive advances to rethink long held business practices.

Concepts, Context and Critical Thinking

Conceptualizing and setting "context" to garner significant insights into vast datasets requires pre-production planning and careful design of a study prior to implementation.

While companies are hiring data scientists and analysts at lightning speed to collect insights, it's important that they not work in "silos."

A successful design process for the study of massive datasets is oftentimes a collaborative effort, with different competencies involved.

The pre-production design team should be diverse, with different areas of expertise offering ideas.

Determining the Objective

Conducting a SWOT analysis (*Strength/Weaknesses/ Opportunities/Threats*) to design the framework for a data study can help identify the business objective, along with where your company ranks relative to its competitors. Topics for discussion during the SWOT analysis could include:

- Key Challenges
- Top Business Drivers
- Business Opportunities
- Client Needs
- Budget
- Timeframe

The SWOT methodology can help focus a team's development of important questions, as well as to filter out unnecessary or replicative data, with the goal of improving accuracy in the results and in meeting the core objective.

To further frame the study's context, the SWOT process can be combined with the fundamentals of journalistic storytelling: *Who, What, When, Where, Why (*Known as the Five W's*),* and *How*. Of these, *Who, What*, and, especially *Why* are essential to the study's design.

Asking "*Why*" in the pre-production stage provides a juncture to check for algorithmic transparency, and accountability, in order to counter, prevent, and remove any algorithmic biases--both obvious and hidden--which may exist.

Experimenting with "*What If*" type questions can boost interest within the collaborative team--and across the enterprise--in thinking about and utilizing data in new ways.

CFE's can also use their training in "thinking like a fraudster" to be creative in crafting questions.

However, asking the *right* questions to accurately detect and analyze patterns in massive datasets--especially ones that exclude redundancies and/or algorithmic biases in the methodology--requires thoughtful and careful design.

By pairing a SWOT analysis with the "*Five W*" fundamentals, a proper pre-production "vetting" procedure of the study can be established.

Gathering Insights

With so much data available, it's easy to obtain answers to all kinds of questions. Yet without careful design, the results can be skewed. A book written in 1954 by journalist Darrell Huff titled *How to Lie with Statistics* is still relevant today.

Many programs can create automated dashboards featuring data visualizations that provide informative analytics and practical insights. But if the pre-production design steps are skipped, capturing signals relevant to the core business objective can easily be overlooked.

In that instance, generating a dashboard can be a waste of time, as it may showcase superficial results, or simply replicate findings available elsewhere. When millions of dollars in "spend" is on the line, it's imperative to garner meaningful insights from the data with as much accuracy as possible.

To learn more about data best practices, *Information Management* magazine (5/1/19) features a slide show listing the top sixteen platforms for data science and machine learning as identified by research and advisory company Gartner.

Many public libraries, including the New York, Queens and Brooklyn systems offer card holders completely free and unrestricted access to the learning platform Lynda.com (rebranded as Linkedin Learning) which offers data analytics training.

If you haven't yet taken the plunge into an ocean of data, go ahead, dive in and have some fun catching the data wave! ♦

Laura Hynes-Keller, CFE, CDS, is a speaker and principal of LHK Communications, LLC, a strategic advisory, market research and media relations consultancy. Email: laurahk@lhkcommunications.com

MEMBER NEWS AND HIGHLIGHTS

Iona College Appointment

Daniel Killourhy, MBA, CPA, CFE, has been appointed adjunct professor at Iona College in New Rochelle, New York, where he will teach 2 Auditing classes to MBA students beginning Fall 2019.

Seeking Participants for Personal Data & Identity Theft Study

My name is Jordan Brensinger, and I am a NYCFE member and Ph.D. candidate in sociology at Columbia University. My dissertation, the *Personal Data & Identity Theft (PDIT) Study*, examines identity theft remediation from the perspective of victims and the organizations they navigate. Through in-depth interviews with victims, I explore how individuals go about recovering their identities and detail the financial and emotional toll that experience takes on them and their families. I also investigate the equally crucial role different organizations and government agencies play in the identity recovery process by interviewing personnel and observing work in key organizational contexts. I am looking to connect with individuals who currently work, or have worked, in identity theft investigation or remediation for an organization, including government agencies, financial institutions and other businesses, and victim assistance organizations. If you would be willing to chat with me or know others who might be helpful with whom you could put me in touch, I'd love to hear from you. Your participation may help inform efforts to tackle the growing challenges caused by identity theft. If you have any questions or comments about my research, please visit the PDIT Study's website or feel free to contact me personally at j.brensinger@columbia.edu.

EVENT PHOTOS

Spring Fraud Conference Meet & Greet on April 12, 2019

The NYCFE Thanks Our Spring 2019 Fraud Conference Event Sponsors

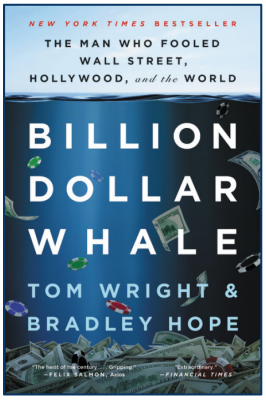
Thomson Reuters CLEAR

and Lifars

LIFARS
your digital world, secured

BOOK CORNER

Editor's Picks for Suggesting Readings

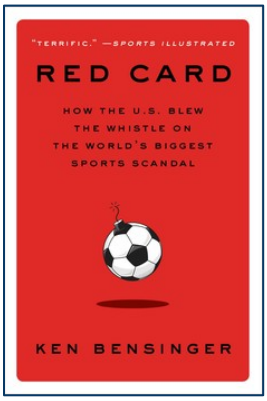


Billion Dollar Whale

By Tom Wright & Bradley Hope

Named a Best Book of 2018 by the *Financial Times* and *Fortune*, this "thrilling" (Bill Gates) *New York Times* bestseller exposes how a "modern Gatsby" swindled over $5 billion with the aid of Goldman Sachs in "the heist of the century" (*Axios*).

Now a #1 international bestseller, BILLION DOLLAR WHALE is "an epic tale of white-collar crime on a global scale" (*Publishers Weekly*, starred review), revealing how a young social climber from Malaysia pulled off one of the biggest heists in history.

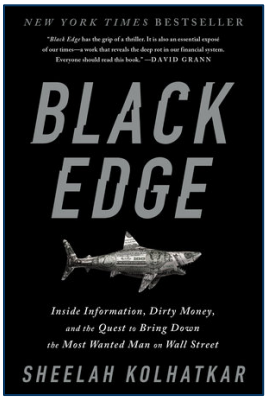


Red Card

How the U.S. Blew the Whistle on the World's Biggest Sports Scandal

By Ken Bensinger

The definitive, shocking account of the FIFA scandal—the biggest international corruption case of recent years, spearheaded by US investigators, involving dozens of countries, and implicating nearly every aspect of the world's most popular sport, soccer, including its biggest event, the World Cup.



Black Edge

Inside Information, Dirty Money, and the Quest to Bring Down the Most Wanted Man on Wall Street

By Sheelah Kolhatkar

"An essential exposé of our times—a work that reveals the deep rot in our financial system . . . Everyone should read this book."—David Grann, author of *Killers of the Flower Moon*

ONE OF THE BEST BOOKS OF THE YEAR--*The New York Times* and *The Economist*

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
Chelsea Binns
president@nycfe.org

❖

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

Special Thanks All Authors, and to Bruce Hulme and Ozan Gurel for Newsletter Copy Editing

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

Things gained through unjust fraud are never secure.
Sophocles