ACFE
Association of Certified Fraud Examiners
New York Chapter #14

FALL / WINTER 2018-19, ISSUE 2

TABLE OF CONTENTS

Letter from the President
Chelsea Binns, Ph.D., CFE P. 1
About the NYCFE P. 2
Expert Views
Summer Day Camp: *Director Knows How to Skim*
Adam J. Fox, MS, CPA, CFE P. 3
Five Questions with...
Janice L. Tyson, CFE P. 5
Fraud Snapshot:
By the Numbers P. 6
Arson Investigation
Bruce Hulme, CFE, BAI P. 7
Member Highlights P. 8
Event Photos Pp. 9-12
Book Corner P. 13
Tech Talk
Approaching Blockchain
Laura Hynes-Keller, CFE P. 14
Submission Guidelines P. 16



Photo Courtesy: Dora Gomez

LETTER FROM THE PRESIDENT

Dear Members,

I am pleased to welcome you to the second issue of our new, revived newsletter and 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.

I encourage all NYCFE members to participate in our newsletter. We welcome information about professional achievements, awards, photos of "fraud fighters at work," along with articles outlining your expert views on a topic pertinent to the CFE community, which will be considered for a future issue. We would love to publish news about your accomplishments, and see your expertise recognized by our wide audience!

NYCFE Events

Our mission at the NYCFE is to provide high quality continuing professional education in fraud prevention, detection and deterrence, and top line networking opportunities, at times and locations convenient to our membership.



Chelsea Binns, NYCFE President

Our meetings this year have been very well attended, including our "sold out" spring conference in April, our breakfast meeting in May, our networking event in July, our "sold out" dinner meeting in September, and our "full day" conference in October.

Some of the topics covered by speakers and presenters included in-depth discussions of corporate fraud, cybersecurity, investigations, AML, fraud risk management, data analytics, blockchain, cybercrime and elder fraud, corporate fraud, and whistleblower matters.

Through these continuing education opportunities, we can discover and learn more about innovative methods used to commit fraud, and ways to prevent, detect and deter it from top experts in their respective fields.

We really appreciate your participation in these events, and according to the feedback we received, you were quite pleased with our high-quality speakers and venues.

Nearly all NYCFE events offer CPE credits. For more information about our events, and to register, please see our home page at www.nycfe.org.

If you would like to suggest a topic or speaker for a future event, and/or if you would like to serve as a sponsor, please contact our Training Director, Dora Gomez at training@nycfe.org.

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 underway, 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.

ACFE 2019 Conference

Planning for the 30th Annual ACFE Global Fraud Conference to be held June 23-28, 2019, in Austin, TX is underway.

The NYCFE will provide a discount code to our members who register through our group.

We are continuing to circulate information to our membership about joining the group as the conference date approaches. It's just one of the features of NYCFE membership!

I welcome your feedback at president@nycfe.org.

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 have a fantastic slate planned for 2019, and 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:

For General Questions: Info@nycfe.org

For Training, Events, Speaker and Sponsor proposals: Training@nycfe.org

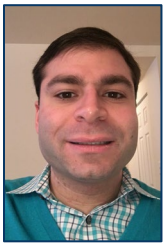
ACFE NEW YORK CHAPTER BOARD OF DIRECTORS

President: Chelsea Binns, PhD, CFE, LPI
Vice President/Training Director: Dora M. Gomez, 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: 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

Summer Day Camp: *Director Knows How to Skim*

A School District Fraud Case Proven Through Data Analytics

By Adam J. Fox, MS, CPA, CFE



Fraud is prevalent in all industries, but it can be especially common in the education industry. In this article, I will be discussing a fraud case in a school district, specifically related to a Summer Day Camp program which occurred during the Summer of 2015. In this instance, the fraud was proven using data analytics. Notably, the three elements of scholar Donald Cressey's "Fraud Triangle," – *pressure, opportunity, and rationalization*, were present as key factors of influence.

This Summer Day Camp program involved children from Kindergarten through Grade 8 who attended a half-day program which took place at two of the Elementary Schools within their school district. The program was run by the Summer Playground Program Director, who was also an English teacher during the regular school year. The program was open to all students who resided within the school district, including students who attended private or parochial schools. Students had the opportunity to participate in a variety of activities, including arts and crafts, sports, and movies on days when the weather was inclement. There were also various field trips offered to the students, depending on their age group.

The fraud began during the registration process, as there were two designated evenings during the month of June during which parents completed the registration. The parents would travel to one of the elementary schools within the district and complete a registration form for each child. A slightly higher price was charged for the students who attended a private or parochial school. In addition, the Program Director instituted a deadline for the registration of the program to a specific day. If a family was still interested in the program after this registration deadline, a specific late fee would apply. The amount of this late fee would depend on whether the student attended the public school, or a private or parochial school.

After completing the registration form, the parents then provided a form of payment for their child or children. Parents had the option of paying by personal check or by cash. However, many of the parents elected to pay via cash. This option turned out to be a mistake made by the school district, as the Program Director was the only person present on the evenings during which the registration took place.

After the payment was submitted by the parent, the Program Director would then pocket the cash. This clearly gave her the "opportunity" to commit the fraudulent act, which is one part of the well-known "Fraud Triangle." This type of fraud is known as skimming, as she stole the cash which was collected prior to it being recorded on the accounting system of the school district.

These actions were rumored by observers for several months after the Summer Day Camp program ended in August of 2015, until the allegations finally reached the offices of the District Superintendent and other administrative professionals. These allegations signaled the need for an investigation. That was when the school district personnel summoned my CPA firm to examine this scenario. Although we were initially engaged to complete an Internal Audit assignment and other testing work, we were tasked with a separate investigation into this matter.

After substantial meetings and correspondence with various school district employees, it was decided by the supervisor with whom I worked that this fraud would best be proven analytically. This would mean reconciling the dollar amount of registration and late fees collected to the original corresponding registration forms completed by the parents of the student participants.

I began this process by creating a Microsoft Excel spreadsheet workbook for each classroom and its corresponding grade level. I then went through various file boxes of registration forms, which were organized by building, grade level, and classroom. I reviewed each individual registration form, the number of students indicated on each form (if there was more than one child per family), and the dollar amount collected.

This data was then entered in my spreadsheet accordingly, and each tab within the spreadsheet was designated for a classroom and grade level of students. Based on the school district's website and the registration forms, I was able to obtain the tuition for each student. I also indicated whether or not the student attended the public, or private or parochial school based on the amount of tuition paid, as well the late fees, if applicable. I continued this process until I had reviewed all registration forms from each of the respective file boxes.

After several hours of reviewing these forms, it was found that the total number of students multiplied

by their respective registration fees did not match the total amount of revenue indicated by the Program Director and the school district. It was then proven that something was clearly attempted to be hidden, and that the Program Director was being dishonest about the registration process for this program.

My immediate supervisor and I discussed my findings. He felt as if I had clearly found an anomaly, and that a fraud was prevalent. He then continued the investigation process by first interviewing the District Superintendent to discuss my findings with her. She expressed her profound dissatisfaction regarding the incident, and the material amount of money which had been misappropriated by the Program Director. She promised that this person would not only not be allowed to run this program again, but she would also be demoted to a lower-level teaching position within the school district.

Next, the Program Director herself was interviewed. Several questions were asked of her regarding the situation. The Program Director was in denial regarding many of the questions, as she naturally attempted to cover up her actions, and would continue to lie when specific issues were posed to her. However, it was clear that the registration funds were misappropriated, and the Program Director had used the money for her own personal gain. The Program Director had a motive for her actions. She felt as if she was not being recognized by the school district for the hard work which she had done, not only as the Summer Playground Program Director, but also as a teacher. She believed that she was therefore not compensated fairly (the "pressure" leg of the Fraud Triangle). She also felt that she could enhance the program by providing additional supplies and snacks using the cash which she had stolen (the "rationalization" leg of the Fraud Triangle). For example, she would use the stolen cash to purchase art materials for projects, and ice cream bars for the children. She also utilized some of her own personal money for these purchases. It was also rumored that she provided the counselors (high school students who resided within the district) with additional compensation which was not part of their contract.

As a result of our investigation, this program was offered in subsequent years, but was of course no longer run by the same individual. In addition, there is no longer a "registration night" held, and cash is not accepted as a form of payment. Instead, parents of the student participants are required to submit a registration form for their children via U.S. mail, and must pay the registration fees using a personal check.

This was clearly a good move made by the school district, as there is no longer a risk of cash being stolen. Once the registration forms and payments are received in the mail, two individuals are assigned to be present in the mail room to open each envelope, and log the payments received. This will prevent the checks from being stolen, and all registration data will be logged in an organized manner.

Even though this fraud was obviously not as severe as the well-known frauds of WorldCom and Enron, it is important to realize that an act of fraud can grow in its dollar amount over time. As the dollar amount of the fraud grows, the more significant is its overall financial impact. By uncovering this fraud, I was able to ensure that no additional money would be lost, as stronger controls were implemented for this program going forward. This gave me a strong sense of satisfaction.

Management and those charged with governance must show high levels of integrity in order to prevent such frauds from occurring. Weak controls and poor governance can set the tone for fraudulent activity to occur. A strong system of separation of duties and strong controls over cash collections is an important element of any internal control system. However, when these controls are overridden, and fraud does occur, diving into the specific details and data analytics can be a helpful tool to uncover acts of dishonesty. ♦

Adam J. Fox, MS, CPA, CFE is a Senior Auditor/Accountant for a regional accounting firm. E: ajf10686@gmail.com.

FIVE TAKEAWAYS

1. There must be a strong overall system of internal controls in place which management does not have the ability to override.
2. There must a strong "tone at the top" attitude among members of management.
3. There must be background checks performed on all employees hired.
4. There must be a clear separation of duties among staff members, particularly when it involves the handling of cash.
5. A fraud prevention system should be implemented within the education industry, as well as within other industries. This process will educate its employees and prevent fraud from occurring. This will strengthen management, as well as those charged with governance.

NINE QUESTIONS WITH... JANICE L. TYSON, CFE

Janice L. Tyson is a Compliance Officer focused on Investigations at Marsh & McLennan Companies (MMC). She has been with MMC for 17 years. Janice has a bachelor's degree in Political Science from Hampton University, a Master of Science degree in Business Ethics and Compliance from the New England School of Business and became a Certified Fraud Examiner in 2017. She worked in law enforcement for 12 years; eight years with the New York City Police Department and four years with the New York County Attorney's Office.

Janice is part of a three-person global team that leads and provides investigative support to various corporate functions and business practices globally within the MMC family of Companies, including subsidiaries. The team investigates fraud, policy violations, and activities by employees which may cause financial and/or reputational harm to the Company.

In addition to her investigation role, Janice manages the Ethics & Compliance Line administered by a third-party vendor. She provides Investigation and Ethics & Compliance Line statistical information to senior management and assists external auditors with their quarterly review of the Investigation function.

Janice believes an ethical workplace creates the best environment to increase creativity and productivity.

Q: *How did you become interested in becoming a Certified Fraud Examiner?*

A: My interest in becoming a CFE began while I was studying for my Master of Science degree in Business Ethics and Compliance. The fraud examination courses referred to work done by the CFE founders.

In addition, resource materials I used for my papers on ethics and fraud referred to work done by CFEs. I also thought it was important to obtain a certification for the investigation work I was doing.

Q: *Tell us about your transition from government services to corporate work. Can you please share some insights about your transition? Challenges? Opportunities?*

A: The transition from government services to corporate work was not too difficult. I faced one challenge when I transitioned from government service to corporate: (1) Coping with freak outs by individuals over matters that did not involve life and death. I made it my priority to complete the required tasks but did not allow myself to get caught up in the hysteria.

There were many opportunities afforded to me in government service and corporate because I was interested in the work and worked hard. My initial position in Compliance at MMC was made possible because of my work in the Police Department and D.A.N.Y.

The Company wanted to get a Compliance Department up and running with individuals they could rely upon. I was honored to be selected and have worked hard to improve my skill set. Becoming a CFE was an important part of demonstrating my intent and commitment to do my best.

Q: *What skills or education best prepared you for the transition to corporate life?*

A: My parents raised me and my siblings to have a strong work ethic. We were expected to study, do well at school and work hard. The training I received at the Police Academy classes stressed the importance of dealing with the public and I believe it shaped my ability to assess difficult situations and come up with resolutions.

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

A: Not in the true sense of mentoring. I am fortunate to work for and with individuals who answer my questions and encourage me.

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

A: Use the resources available at ACFE.com. There is wealth information on various topics. It is the first place I go to research new issues. Our Investigations team uses the I-Sight case management system which enables us to better coordinate our investigations with our Compliance colleagues globally.

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

A: Work on improving your observation and listening skills because both are important to improve your interview skills.

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

A: I enjoy doing Bikram Yoga and listening to classical music and jazz.

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

A: My favorite author is Elizabeth George. She writes the Inspector Lynley mysteries and my favorite television shows are "Death in Paradise" and "Hinterland." The police teams have individuals who are proficient in investigative and forensic accounting skills.

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

A: I enjoy meeting the members. Everyone has an interesting background and willingness to share their experiences. ♦

❖

FRAUD SNAPSHOT: *By the Numbers*

Top Ten Reported Data Breaches, Exposures and Hacks to Date:

1. Yahoo: 3 billion
2. Marriott: 500 million
3. Adult Friend Finder: 412.2 million+
4. Exactis: 340 million
5. Adobe Systems: 152 million
6. UnderArmour MyFitness App: 150 million
7. Equifax: 147.9 million*
8. EBay: 145 million
9. Heartland Payment Systems: 134 million
10. Linkedin: 117 million

**Often considered the worst data breach because of sensitivity of the information stolen.*

Arson Investigation

By Bruce Hulme, CFE, BAI



This arson investigation assignment dealt primarily with my identifying and locating a professional arsonist believed to have been paid to burn down a carpet factory in Dalton, Georgia, in order that the business owner might collect from the insurance company.

Dalton, and its surrounding area, is referred to as the "Carpet Capital of the World." The New England-based insurance company specialized in providing fire insurance to commercial entities, particularly factories. Their staff included experienced arson investigators and claims adjusters who combed the fire scene for evidence, including business papers and telephone records that had not been destroyed by the conflagration and were to contain important leads for me to develop.

After determining that the sprinkler system had been turned-off before the fire started, finding traces of accelerants and the factory owner with an air-tight alibi having been at a private club in the adjoining state of Tennessee, thus ruling him out as having actually set the fire, my assignment was to identify the arsonist and ascertain if the factory owner had hired same.

The insured sued the carrier for payment on the fire loss after the carrier, suspecting arson and retention of an arsonist by the insured factory owner, denied the claim. There was to eventually be two federal court trials of this claim.

I was retained by a New York City law firm hired by the insurance company. The insured retained a flamboyant northern Georgia trial attorney experienced in defending high profile plaintiffs in civil matters and criminal cases, as well as arsonists.

The trials took place in the U.S. District Court for the Northern District of Georgia in Rome. My services in connection with locating the actual arsonist who set the fire took me to Dalton and Rome, Georgia, Chattanooga, Tennessee and Newark, New Jersey. A Rome, Georgia law firm was also retained as local counsel for what was to be the second and final trial.

I was to eventually locate the professional arsonist in New Jersey. Arrangements were made for his arrest by the Georgia Bureau of Investigation and he was given immunity to testify against the factory owner plaintiff who he stated hired him.

Prior to the trial I recall having the following conversation with the New York lawyer who had retained me. I asked him, in light of the fact that no one had died in this fire, and that a New York City law firm and private investigator were representing a Yankee insurance company being sued by a "Northern Georgia Good Ole Boy," how he expected to win this case?

He replied: "You will be accompanying the arsonist up the courthouse steps where the insured factory owner will be waiting at the front door.

When the insured sees the arsonist, he will pull out his gun and shoot and kill the arsonist. That is what it will take for us to win this case." That didn't occur, nor did we win. The jury was just not going to find that someone colluded with an admitted arsonist in an insurance case when nobody died. ♦

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

❖



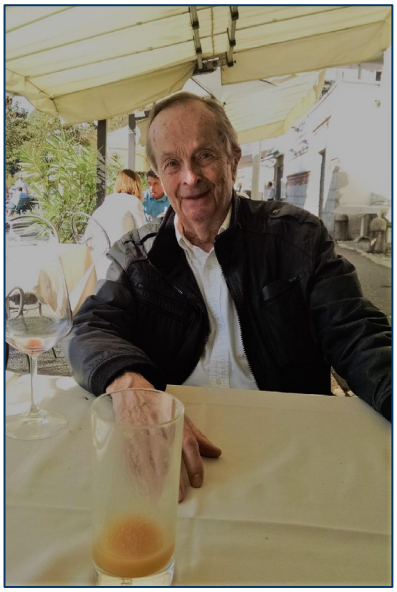
MEMBER HIGHLIGHTS

NYCFE President Chelsea Binns with daughter Samantha

8lbs, 4oz, 21 inches

BEST WISHES, CHELSEA & FAMILY!

CONGRATS, BRUCE!



Bruce Hulme, CFE Receives IASIR Life Member Award

On October 26, Bruce Hulme, CFE, BAI, a long-standing board member of the Association of Certified Fraud Examiners New York Chapter #14, received the prestigious **International Association of Security and Investigative Regulators *Life Member Award*** in Scottsdale, AZ at its annual conference. IASIR is an association of governmental, state, and provincial regulators in the United States, Canada. and France. The award was given in appreciation and gratitude for his contribution to the advancement of the association during its 25-year history and for his 14 years as the association's sole elected representative of the private investigation industry. He is the eighth member to be awarded this honor. IASIR is concerned with licensing, regulation, enforcement and training in the private investigative, private sector security, alarm, and armored car industries. For more than four decades, Hulme has served as a legislative advocate, officer, or board member on behalf of professional associations including the National Council of Investigation & Security Services and the Associated Licensed Detectives of New York, also serving as president of both, and more than two decades each with IASIR, NY ACFE Chapter, International Intelligence Network, and the Society of Professional Investigators.



Dora Gomez earned a Master of Science, Business and Information Systems from the College of Computing Science at NJIT in December 2018

CONGRATS, DORA!

NYCFE EVENT PHOTOS



NYCFE Breakfast Event/Speaker Lacey Keller, Gryphon Strategies/Topic: Data Analysis



NYCFE Dinner Event/Speaker Ondrej Krehel, CEO, LIFARS/Topic: Cyberextortion Legal Implications

The NYCFE would like to thank our 2018 event sponsors:

- Gryphon Strategies for its support of our May 22 breakfast meeting held at Slattery's Midtown Pub
- LIFARS for its support of our September 12 dinner event held at Battery Park Gardens

To learn more about how to sponsor or become a speaker at an event, please contact Training@nycfe.org

Training Event Photos:
Courtesy Dora Gomez

NYCFE FALL CONFERENCE

Snapshots of some of the speakers at the October 12 full day conference held at Fordham Univ.



Keynote Speaker Greg Coleman
Coleman Worldwide Advisors
"Wolf of Wall Street" retired FBI Investigator



Roger Hockenberry, Partner, Cognito/
Topic: Fraud Detection and Block Chain Technologies

Kirby Plessas, President/CEO, Plessas Experts Network, Inc.





Keynote Speaker Tom Hardin, "Tipper X"

NYCFE HOLIDAY PARTY 2018




Held in conjunction with the HTCIA and Infragard







Fordham University, Dec. 13, 2018

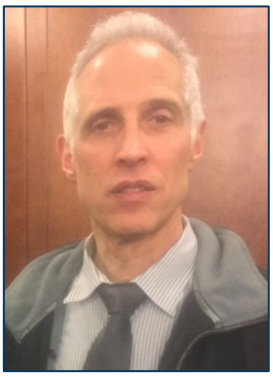










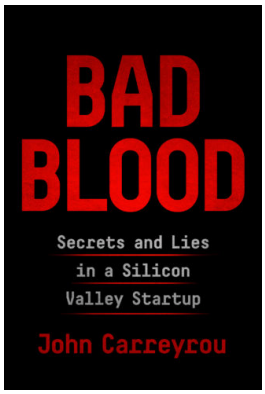




Holiday Event Photos: Courtesy LHK

BOOK CORNER

Editor's Picks for Suggesting Readings



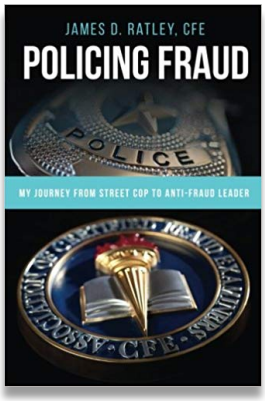
Bad Blood

Secrets and Lies in a Silicon Valley Startup

By John Carreyrou

John Carreyrou is a two-time Pulitzer Prize-winning investigative reporter at *The Wall Street Journal*. For his extensive coverage of Theranos, Inc., Carreyrou was awarded the George Polk Award for Financial Reporting, the Gerald Loeb Award for Distinguished Business and Financial Journalism and the Barlett & Steele Award for Investigative Journalism in 2016.

"You will not want to put this riveting, masterfully reported book down. No matter how bad you think the Theranos story was, you'll learn that the reality was actually far worse."—Bethany McLean, bestselling coauthor of The Smartest Guys in the Room and All the Devils Are Here

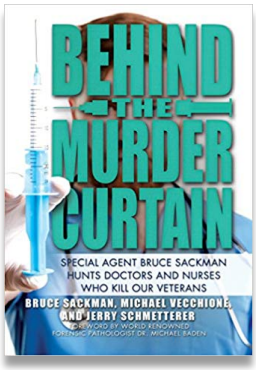


Policing Fraud

My Journey from Street Cop to Anti-Fraud Leader

James D. Ratley, CFE

In Policing Fraud, Association of Certified Fraud Examiners (ACFE) President James D. Ratley, CFE, shares detailed accounts of his life, from his time on the Dallas police force to his role in helping to create a profession and establishing the largest anti-fraud organization in the world.



Behind the Murder Curtain

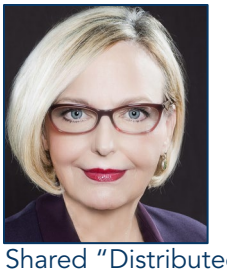
Special Agent Bruce Sackman Hunts Doctors and Nurses Who Kill Our Veterans

By Sackman, Michael Vecchione and Jerry Schmetterer

When Veterans Hospital patients on the road to recovery suddenly die in increasing numbers, it's up to VA Special Agent in Charge Bruce Sackman to find out why. His shocking discovery rips open the hidden world of what goes on behind the bedside curtains when a killer doctor or nurse decides a patient must die.

An Approach to Blockchain

By Laura Hynes-Keller, CFE



Blockchain. Bitcoin. Digital Disruption. The Fourth Industrial Revolution.

Shared "Distributed Ledger Technology," or "blockchain," still in its infancy, offers the promise of streamlining business operations in myriad industries. Blockchain is about the exchange of value, such as bitcoin, allowing participants to exchange assets without relying on a third party to manage the transactions.

Like an accounting ledger where financial transactions are recorded, the blockchain, a digital "ecosystem" database, allows transactions and their details to be entered in multiple places at the same time, but without a central database or administrator. As such, blockchain has the potential to redefine and transform long standing business value chain processes and procedures, both within--and between--companies and organizations of all types.

The World Economic Forum named blockchain as core to the Fourth Industrial Revolution; its *Deep Shift* survey suggested that 10 percent of global GDP will be stored on blockchain by 2027.[1] According to a recent International Data Corporation guide, blockchain spending is expected to grow at a robust pace throughout the 2017-2022 forecast period with a five-year compound annual growth rate (CAGR) of 73.2 percent. Worldwide blockchain spending is expected to be $1.5 billion in 2018, double the amount spent in 2017, with worldwide spending on blockchain solutions forecast to reach $11.7 billion in 2022.

Yet, while libraries discarded card catalogs in favor of digitizing collections, creating vast and valuable efficiencies, the Dewey Decimal System for classification wasn't discarded. What business processes, procedures and systems will transcend distributed ledger technology disruption? Is there a path forward for your company to position itself for a blockchain future?

Blockchain Basics

As a technology infrastructure, distributed ledger technologies are linked by cryptography and powered by inexpensive computer capacity running on "nodes" on individual computers around the world.

There are three primary distributed ledger technology categories, 1) Permissioned, which restricts participation on a blockchain to designated participants, 2) Permission less, which allows anyone to write to the blockchain, and 3) A consortium, or hybrid blockchain, which allows both.

As a distributed ledger, a blockchain is managed by a peer-to-peer network complying to a specified protocol for inter-node communication and validating new blocks. To make a change or addition requires an update to the entire blockchain.

Anyone can set up a blockchain, and any transaction in that specific distributed ledger ecosystem must be validated by all the participating members to create a "consensus," thereby making the transactions "immutable," which is beneficial in an audit setting. Proponents of blockchain often cite this aspect as the reason "trust" among parties and counterparties is not necessary.

Instead of manual paper processes, or documentation held on a computer server or in the "cloud," with access and oversight determined by a central administrator, every designated user of every computer has access to the designated blockchain.

One of blockchain's features is anonymity. For example, an anonymous user can create an

[1] Deep shift: Technology tipping points and societal impact, World Economic Forum, September 2015, weforum.org.

account on a blockchain, then load the assets using an existing email account. The user transacts based on those assets, and their growth. Blockchain can store info, events, ownership and activities of various types.

Describing blockchain, William Mougayar, author of *The Business Blockchain*, wrote "Imagine two entities (e.g., banks) that need to update their own user account balances when there is a request to transfer money from one customer to another...With the blockchain, a single ledger of transaction entries that both parties have access to can simplify the coordination and validation efforts, because there is always a single version of records, and not two disparate databases."

Challenges

Humans write the code for the "smart contracts," the "computerized transaction protocol" visible to all users. Smart contracts execute processes once certain criteria, such as terms of a contract, are met on the blockchain. Human error is a vulnerability in any ecosystem, and coding loopholes that cause bugs and security issues are not necessarily quickly or easily fixed.[2] Speed and scale are also challenges to widespread adoption.

For a Certified Fraud Examiner, questions arise: How safe is blockchain? How are users of the chain verifiable? What controls are in place? In what ways will companies, industries and regulators resolve authentication problems? What entities will provide the standardization and oversight?

While there have been ongoing discussions in blockchain circles about developing a global blockchain for authentication purposes, it would require massive public/private partnership coordination efforts between governments and the largest, most influential tech organizations in the world. Is that a realistic possibility?

Positioning for the Future

Distributed ledger technologies offer new analytical frameworks. Where does your business stand today in the tidal wave of digital transformation? Is there a business case to be made for the implementation of blockchain at your company? If so, what is the business rationale?

How could a new blockchain "ecosystem" drive operational efficiencies that both create competitive advantage and result in significant cost savings for your business? How will data architecture, management and governance, and artificial intelligence and machine learning (AI/ML) fit together with blockchain?

Will costs associated with transitioning to and maintaining the blockchain ecosystem--including hiring humans with the necessary technical talent--cost less than maintaining the status quo? Will the current lack of clear standards and regulations in your industry curtail adoption and implementation, causing your business to possibly lose market share to digital disruptors?

Sectors leading the way in blockchain experimentation and implementation include financial services, health care, insurance, technology, media, energy and shipping, with various experts, trade associations and regulatory bodies launching task forces to study use cases.

According to a 2016 Deloitte survey entitled *Blockchain Adoption Varies by Industry,* "Thirty-nine percent of the senior executives at large U.S. companies initially surveyed indicate they have little or no knowledge about Blockchain technology. Many deemed it to be crucial for their companies and industries. Forty-two percent believe it will disrupt their industries."

Decision Trees as a Roadmap

How can executives approach decision-making about whether to implement blockchain initiatives?

A "decision tree" approach can be a useful way to determine whether a business

[2] A June 2016 attack on the decentralized autonomous organization (DAO), which was built as a smart contract on the Ethereum blockchain using an "open source" framework, drained $70 million in Ether tokens while developers on the blockchain worked on a solution that would gain consensus.

need can be met by implementing blockchain. Start with eight to ten simple questions about the specified line of business. The initial decision tree planning does not necessarily require statistical modeling with probabilities; instead, it can be designed as a navigational "if/then" and "yes/no" roadmap.

Multiple teams across various company divisions can develop decision tree roadmaps. The assorted departmental decision trees can be combined into an overlay. Then evaluate whether corresponding pain points across the enterprise offer signals as to whether further development and implementation of a blockchain ecosystem could resolve the bottleneck or problem.

In addition to offering a simple way to collaborate internally and move the overall discussion about blockchain forward, an initial "roadmap" strategy is an efficient way to determine whether there is a "match" for your use case, without a lengthy investment of time and money into examining different distributed ledger technologies, such as "Blockchain as a Service" (BaaS) offerings.

While the promise of distributed ledger technologies is enormous, beware of "vaporware," that is, software or hardware that is announced and promoted by a vendor, even though it does not yet exist.

It's easy to find examples of blockchain hype online, with comments such as *"You don't need to know how the blockchain works to use it."* The internet is bloated with examples of false claims regarding the capabilities of an array of technologies. A recent top example of vaporware is medical-testing startup Theranos Inc., which raised $700 million from investors by misrepresenting its capabilities.

However, sometimes it's not false claims, instead, a technology was relegated to the vast digital graveyard by the introduction of a "better mousetrap."

Investment costs to build out distributed ledger technology systems, and ongoing security challenges in automation and managing data remain. Participation by all parties in the designated ecosystem, such as buyers and sellers, financial institutions, and legal and government regulators are further barriers to acceptance and implementation. Plus, intermediary businesses who have served as trusted third parties may do what they can to slow adoption in their respective industries.

With the technology landscape continually evolving at a rapid pace, implementing a quarterly or semi-annual "decision tree" strategy to refresh your navigational roadmap and examine where your company stands on the blockchain front can position you, and your company, for future success. ♦

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

❖

SUBMISSION GUIDELINES: We welcome submissions from current 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 1500. Photos and illustrations can accompany submissions. Please contact newsletter editor Laura Hynes-Keller at Newsletter@nycfe.org with submissions, questions or comments. Thank You.

Things gained through unjust fraud are never secure.
Sophocles