ACFE
Association of Certified Fraud Examiners
New York Chapter #14

TABLE OF CONTENTS

Letter from the President
Chelsea Binns, Ph.D., CFE P. 1
Photos P. 2
Expert Views
Personal Encounters with Fraud: It Could Happen to Anyone!
Daniel Killourhy, CFE, CPA P. 3
Are you ready for GDPR?
Brett Fisher, CFE P. 5
The Case of Undue Influence: Contested Proceedings
Bruce Hulme, CFE P. 7
Looking Forward, Looking Back
Steven R. Levine, CFE P. 9
Book Corner P. 11
Fraud Prevention Resource Guide
Laura Hynes-Keller, CFE P. 12
Submission Guidelines P. 14



View from NYCFE Training Session at Thomson Reuters in Times Square on April 20

Event Photos Courtesy: Dora Gomez

SPRING / SUMMER 2018, ISSUE 1

LETTER FROM THE PRESIDENT

Dear Members,

Welcome to the Summer 2018 issue of the NYCFE Newsletter.

I am honored to assume the role of president of the New York Chapter of the Association of Certified Fraud Examiners for the 2018-2019 term, and would like to personally thank our chairman Jon Newcomb, who led our Chapter to new heights during his previous term as president, along with all of our past and current board members, and the entire membership for your interest and participation.

Our mission at the NYCFE is to provide high quality continuing professional education and networking opportunities, while raising fraud awareness. Our chapter is filled with many experts in their respective fields, along with those eager to learn and advance in fraud prevention matters, including students, and early and mid-level professionals. Working together, we have a terrific opportunity to make a difference in the fight against fraud.

Throughout the year we offer an array of training and networking options at locations throughout NYC--held at various times of day--to accommodate all working professionals. At each of our



events, we feature very talented speakers who educate us on cutting-edge fraud topics, and attendance has been very strong.

This year is no exception, with fantastic events organized by NYCFE Training Director Dora Gomez touching on topics including cybersecurity, ethics and data analytics. Those events have included several evening meetings and an all-day Spring Conference.

If you do not already participate, we encourage you to become active in our Chapter, and we hope to see you at the ACFE conference in Las Vegas from June 17 through 22.

We have a Chapter networking meeting planned for July, and the ACFE will be in NYC to lead special 2-day training sessions in

Obtaining, Managing and Searching Electronic Evidence and *Financial Institution Fraud* from August 6 through 9. Another NYCFE training event is slated for September, and the full day NYCFE Fall Conference will be held in October. All events offer CPE credits. For more information about our events, and to register, please see our home page at www.nycfe.org. We also welcome you to invite others with our shared interests to join our Chapter. We recently launched a membership drive and are offering a special gift to current members who refer new ones. Membership applications can be found on our website.

In this newsletter we feature fraud-related educational articles contributed by our members Daniel Killourhy, Brett Fisher, Bruce Hulme and Steven Levine. Designed and edited by board member Laura Hynes-Keller, we welcome your suggestions for future issues, and submission guidelines can be found below. We will be adding a professional development section to our next issue, Fall/Winter 2018, to highlight the professional achievements of our membership. Please contact Laura via email laura.hyneskeller@gmail.com to propose content. I also welcome your feedback at president@nycfe.org.

Thank you to our newsletter contributors, and to all of you for being a valued member of our organization. We look forward to continuing a great year at the NYCFE!

Chelsea Binns
President, NYCFE

❖



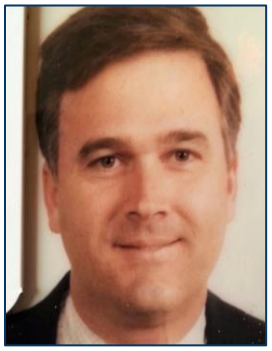
NYCFE Board Members: Training Director Dora Gomez, Chairman Jon Newcomb, President Chelsea Binns at Full Day Training Conference on April 20th in New York City



NYCFE April 20th Event keynote speaker and whistleblower Tony Menendez, CFE and ACFE Sentinel Award Recipient

Personal Encounters with Fraud: *It Could Happen to Anyone!*

By Daniel Killourhy, CFE, CPA



My career now spans over 40 years. When I was a senior at St. John's University in New York City listening to my auditing professor talk about the Equity Funding[i] and similar scandals of the 1970's, it all seemed so academic. After all, these types of things only rarely occurred and hence appeared to be a bit of a novelty. One felt as a student that the chance of encountering and being personally challenged with a fraudulent situation was going to be pretty remote. Correct?

Not quite.

My first exposure to witnessing a fraud was with the Big 8 CPA firm which hired me. The partner, Bob, who interviewed me on campus, was instrumental in bringing me in for an interview, and I was subsequently hired. Along with many other Staff Accountants, Seniors and Managers, I was invited to his house in Connecticut for occasional parties, which were a lot of fun and well attended. Bob happened to be the firm's engagement partner on a major airline at that time. As partner on the airline account, Bob had free flying privileges, in part so that he could visit airline operations and locations. In those days, airline tickets were a multi-part paper document. Bob was taking one of the ticket part copies and submitting them for reimbursement on his expense report. This was uncovered by the senior concurring partner while Bob was rotating off the account. The airline CFO told the senior partner that the new engagement partner would have the same "free ticket" arrangement as Bob. The cat was out of the bag!

Bob was fired, his career severely damaged and his reputation destroyed. When I heard the story, I realized that Bob was financing the parties and his "living large" life style based upon the fraudulent reimbursement of the airline tickets. I liked Bob personally, so was dismayed when I found out what had happened. It made me wonder why someone in his position of trust would risk it all. However, this was not to be my last exposure to fraudulent activities in the workplace.

Eventually I left Public Accounting, and after a stint of several years as an Internal Audit Manager, in the mid-1980's I was recruited by the Owner/CEO to be the Controller for a family owned oil and gas drilling company. I quickly realized that fraudulent tax returns had been filed, and investors in his oil and gas company were being defrauded. Not willing to be a part of criminal activity, I found another position within several months and turned him into the IRS. The IRS finder's fee--which I collected several years later--was not worth it. Every day I worked at this family business Controller's position was a nightmare. I was sorry I had ever accepted the position, and resolved never again to work for a small, family owned business.

After this experience I resumed my career in Audit with a manufacturing conglomerate. I uncovered payments to "consultants" in Mexico where this conglomerate had major government contracts. The consulting payments were being shared with government officials. Not everyone in the company worked for at this time was happy that I shined a light on these FCPA[ii] violations.

This company was eventually sold, and I moved on to an Audit Director's position with a large foreign electrical engineering company. I was instrumental in breaking up a major fraud in the company's fleet operations costing the company many millions of dollars each year.

Here again I became aware of significant bribery of government officials (FCPA violations) and watched as senior management ignored the findings of the Audit Department. I even apprised the CPA firm partner on the account regarding what I knew, however, no action was taken. I had to act discreetly, or my career could have come to a quick end. Being an Audit Director provided only limited protection. This company eventually paid hundreds of

millions in penalties to the U.S. Department of Justice. These were only the major fraudulent activities I personally encountered. There were others. The message here to those still early in their career is: You most likely will have to deal with ethical and fraudulent situations and it won't always be easy to do so.

When you are confronted with an ethical and fraudulent situation--in addition to any legal considerations--it might be useful to review the ethics guidelines in the ACFE's 2017 Fraud Examiners Manual[iii] as an aid in your decision-making process.

Yet codes of professional ethics, nor the law, provide for guidance for every ethical or fraudulent situation, especially when it is up to an individual to decide on the proper course of action.

As Certified Fraud Examiners, we are held to a higher standard. Therefore, I encourage you to always "take the high road," even if it may not be easy, or popular. After all, the view is much better.♦

Daniel Killourhy, CPA, MBA, CFE, is Consulting Director, Operational Review, Catholic Medical Mission. Email: daniel.killourhy@gmail.com

[i] Equity Funding Corporation of America was a Los Angeles-based U.S. financial conglomerate that marketed a package of mutual funds and life insurance to private individuals, collapsing in scandal in 1973 after scores of company employees had engaged in organized deception of investors, auditors, reinsurers and regulatory authorities.

[ii] Foreign Corrupt Practices Act

[iii] ACFE 2017 Fraud Examiners Manual: "Ethics for Fraud Examiners" (4.901), "Code of Professional Ethics" (4.1001), and the "Code of Professional Standards" (4.1101).



Dan Killourhy (back row) pictured with colleagues at the Catholic Medical Mission Board Finance Conference in Nairobi, Kenya. He performs Management Consulting, Audit and Investigative work for CMMB. Photo Courtesy: CMMB

❖

Are You Ready for GDPR?

By Brett Fisher, CFE



What has been described by some as the most sweeping and comprehensive data privacy legislation in the past 20 years--the European Union's General Data Protection Regulation (GDPR)— goes into effect this month. The impact of GDPR will be that the use and access to personal data (at least that data belonging to residents of the EU) will be more restricted and transparent.

For anti-fraud practitioners, GDPR creates some unique challenges. Access to personal data is critical for conducting investigations or responding to incidents of fraud. Complete transparency is often not ideal either, as it may be necessary to keep a subject unaware that they are being investigated.

While it is probably not necessary to sift through the 99 Articles that comprise GDPR, most anti-fraud practitioners should be aware of the core principles of the legislation.

What is GDPR?

The *General Data Protection Regulation (EU) 2016/679*, signed into law on April 27, 2016, is scheduled to go into effect on May 25 of this year. What makes GDPR significant is an extensive scope and reach that far exceeds prior regulations (such as its predecessor, *Data Protection Directive 95/46/EC*). GDPR legislation provides extensive guidelines on the collection, processing, storage, use and destruction of data from any data subject (defined as an "identified or identifiable natural person") within the EU. Furthermore, GDPR provides strict guidelines on individual rights to ensure their data is accurate and used in a manner that is consistent with the stated purpose of its collection; it also contains provisions for subjects to inquire about what data a company has on them and, if requested, that data be destroyed.

GDPR is applicable not just to European firms, but to any company that offers goods and services to or monitors the activities or behavior of EU citizens and residents. If a company conducts any business with customers in the EU where data is collected, that company should assume they are subject to GDPR.

Penalties

Penalties for failing to comply with GDPR can be stiff. Depending on the infringement, a firm violating the provisions of GDPR is subject to fines of up to the greater of 20 million EUR (approximately $24 million US) or 4% of global revenue. A key shift is third party accountability. Organizations can be held accountable when third parties experience a breach and were lax in performing due diligence to ensure data was protected.

General Principles and their Implications

With 99 individual Articles and over 250 pages in length, GDPR is a bit of a read, to say the least. Most people are not expected to spend time dissecting the entire document in detail. It is important, however, for anti-fraud practitioners to understand the key principles.

Data Processed Lawfully, Fairly, and Transparently: Processing data requires the subject's consent or a valid business purpose and that data must be processed in a manner consistent with stated purpose. Organizations that collect or process data are required to communicate what data is being collected and how it will be used.

GDPR does consider fraud detection and monitoring as an appropriate business purpose. Care must be taken, however, as the subjects in fraud investigations are often unaware that their data is being monitored or otherwise utilized in this manner. Fraud investigators will need to balance having open access to personal data, exercising discretion regarding whose data is being used for investigation, and complying with GDPR use and transparency requirements.

Collect Personal Data for Legitimate Purposes: GDPR states that the processing of data

must not extend to purposes it was not originally collected for. The regulation also considers preventing fraud a legitimate interest of the data controller (for example, data provide to your bank or insurance provider). But reasonable determinations still need to be met to determine to what extent and degree such data can be utilized for fraud detection and monitoring purposes.

Only Collect Personal Data Needed: Data collection should be limited to the minimum required to meet the stated business purpose. Collecting extensive amounts of data, even in the interest of detecting and preventing fraud has the potential to place firms at risk or places a burden on those firms to justify the scope of their data collection.

Personal Data Must Be Accurate and Kept Up-To-Date: Firms are required to take measures to maintain the correctness of data and respond to rectification requests in a reasonable timeframe. While accurate and timely data has always been critical for fraud detection, GDPR raises some questions about the mechanism by which subjects might make corrections to their data. Particularly if data subjects are unaware that their data is being used as part of a fraud investigation.

Personal Data is Kept for No Longer Than is Necessary: A core tenet of GDPR is the *"right to be forgotten"* once collected data is no longer relevant or the subject revokes consent. This creates several potential challenges for fraud investigators. Legacy data may no longer be accessible, as firms dispose of data they are not legally obligated to preserve. Investigators must ensure that the scope and retention period of data collected during an investigation do not conflict with GDPR requirements, once the investigation has concluded. Much like the collection of any evidence, fraud investigators should work with their legal departments and Data Privacy Officer to ensure that data is not only collected in an appropriate manner, but destroyed when it is no longer needed, in accordance with appropriate laws.

Personal Data Must Be Processed in a Manner That is Secure: Appropriate controls must be in place to maintain the confidentiality, integrity, and availability of personal data. This principle must be communicated throughout the organization using existing security training and awareness programs. Privacy and security should be considered early in the design and building of systems to save time and enhance effectiveness.

In Conclusion

GDPR is complex, and all its implications have not surfaced for entities that collect and analyze personal data for the purpose of detecting fraud. But for now, it is important for anti-fraud practitioners to be aware that these laws are coming and to have those discussions with their Data Protection Officer to ensure that they have the right policies and procedures in place. ♦

Brett Fisher, CFE leads Satori Consulting's Cybersecurity practice in New York. Email: bjfisher@satoriconsulting.com

References:

General Data Protection Regulation, full text: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Web-based reference of the General Data Protection Regulation: http://gdpr-info.eu/

Satori Consulting Cybersecurity GDPR Readiness: http://www.satoriconsulting.com/gdpr-readiness.html

❖

The Case of Undue Influence: *Contested Proceedings*

By Bruce Hulme, CFE, BAI



As the director of government affairs for Investigative and Security Professionals for Legislative Action (ISPLA), a professional association concerned with legislative and regulatory issues, I am often asked to speak or write about potential pitfalls affecting private sector investigations. These pitfalls can also affect certified fraud investigators. For example: recent hot topics have included the use of drones and GPS tracking to conduct surveillance. Longstanding issues include the avoidance of Gramm-Leach-Bliley Act (GBLA) violations while locating assets or recovering ill-gotten gains and stolen property, compliance with the Fair Credit Reporting Act (FCRA) when conducting pre-employment and third-party workplace investigations, avoiding potential invasion-of-privacy lawsuits when conducting surreptitious surveillance or open-source intelligence and social media investigations, and the use of pretense, a recognized investigative tool when conducting interviews of witnesses and targets of investigations. All of the foregoing topics have been part of legislative or regulatory oversight of the professional investigator that I have addressed before members of Congress for ISPLA. Following is a case study illustrating some of these issues:

Undue Influence: A judicially created defense to transactions that have been imposed upon weak and vulnerable persons that allows the transactions to be set aside.

This case involved a contested will and undue influence litigated at Kings County Surrogate's Court in Brooklyn, New York. I was asked to investigate the validity of an unknown will that had surfaced shortly before the death of a very elderly widow with no children. A niece of the deceased who had moved in to assist with her health care was named the sole legatee. (I will not identify the parties involved as the deceased happened to have the same name as a famous female Broadway stage celebrity, also now deceased.) She was widowed when her husband, an American serviceman, had been killed in action in France during WWI. She never remarried and had been receiving a "Widow's pension" all those years. The "new will" knocked out all of the other nieces and nephews named as beneficiaries under the original will. Over the years she purchased almost every private house on the block in a lower middle-class residential neighborhood in Brooklyn. Her real estate holdings were in the millions.

I initiated my investigation working with the retained forensic questioned document firm of Osborn & Sons, a four-generation family firm of sons. I worked with Paul A. Osborn, the son of Albert D. Osborn, on this case. In subsequent investigations I've worked cases with Paul's son, John Paul Osborn. The firm's most notable case (and they had many) was the Lindbergh child kidnapping trial, State of New Jersey v. Bruno Hauptmann in 1935, when Albert S. Osborn and his son, Albert D. Osborn, testified on behalf of the prosecution. My hope in the matter I was investigating was that the signature of the deceased could be shown to be a forgery. To prove such is the case, one must secure many signatures; and although I found many exemplars, there were not enough to question the veracity of what was purported to be the signature of the deceased. I next conducted background checks of the niece, her boyfriend and another individual who had been a coworker where the boyfriend had worked as a butcher. The most information I could develop was that the boyfriend had a criminal conviction record for assault.

I then conducted an extensive canvass of the multi-family private houses that had been owned by the deceased and which she had rented over the years. I also tracked down and interviewed tenants that had previously rented and then

moved away. There were two common themes. First, her tenants all paid cash; and some recalled that when they paid the deceased, she would just open a desk drawer or a closet and just throw the cash into it. Cash would just be laying about in her house. One tenant thought she had thousands of dollars in her closet. Second, she had a husky voice and a somewhat masculine appearance with several tenants stating they observed she had hair on her chest just below her neck. She would wear dungarees and men's collar shirts open buttoned at the neck. I then wondered just how much cash the niece and her boyfriend had possibly stolen when she came to assist the deceased, and I concentrated my efforts towards establishing undue influence or some type of duress.

According to West Encyclopedia of American Law, virtually any act of persuasion that overcomes the free will and judgment of another may amount to undue influence. Undue influence differs from duress, which consists of the intentional use of force, or threat of force, to coerce another into a grossly unfair transaction. Blackmail, extortion, bad faith threats of criminal prosecution, and oppressive abuse of process are classic examples of duress. To establish undue influence, it must be demonstrated that the victim was susceptible to overreaching. Conditions such as mental, psychological, or physical disability or dependency may be used to show such susceptibility. There must be an opportunity for exercising undue influence. This opportunity may arise through a care-giver, a beneficiary or legatee. There must be evidence that the one was inclined to exercise undue influence over the victim. A person who aggressively initiates a transaction, insulates a relationship from outside supervision, or discourages a weaker party from seeking independent advice may be attempting to exercise undue influence. It must be an unnatural or suspicious transaction. Courts are wary of testators who make abrupt changes in their last will and testament at the behest of a beneficiary who stands to benefit from the new or revised testamentary disposition.

Courts will examine the facts closely before finding that a transaction has been tainted by undue influence. Mere suspicion, surmise, or conjecture of overreaching is insufficient. The law permits loved ones and confidants to advise and comfort those in need of their support without fear of litigation. Courts are also aware that the doctrine of undue influence can be used as a sword by the vindictive and avaricious who seek to invalidate a perfectly legal transaction for personal gain. When undue influence is found to have altered a transaction, however, courts will make every effort to return the parties to the same position they would have occupied had the overreaching not occurred.

Virtually all extortion statutes require that a threat must be made to the person or property of the victim. It is not necessary for a threat to involve physical injury. It may be sufficient to threaten to accuse another person of a crime or to expose a secret that would result in public embarrassment or ridicule. The threat does not have to relate to an unlawful act. When used in this sense, extortion is synonymous with blackmail, which is extortion by a private person.

My last phase of investigation concentrated on developing the undue influence and/or coercion possibility to attack the will that had been produced by the niece. The masculinity aspect of the deceased's appearance led me to ascertain whether an autopsy was ever conducted. I determined it was and that photographs had been taken of the body. Proof could be shown that the deceased was a hermaphrodite. The niece had found this out while tending to her nursing needs and had threatened to expose her. The deceased was fearful that if it be known to the government that she had been a hermaphrodite when she got married that her marriage would not have been recognized as being legal and that she would have to return all of the government benefits she had received. The threat of exposure and ridicule was her fear. The case was settled with the bulk of the proceeds going to the rightful heirs under the original will.♦

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

❖

Looking Forward, Looking Back

By Steven R. Levine, CFE

My Chapter, the New York



Chapter of the Association of Certified Fraud Examiners is a professional organization comprised of officers and members work diligently to provide meaningful opportunities for each other to excel in their chosen professions and thereby continue to enhance the meaning and prestige of our designation as a CFE, a Certified Fraud Examiner.

Today, our designation is not only recognized and sought by employers, in many cases it is a prerequisite for the position. As recently as ten or fifteen years ago, that was not the case.

I joined our Chapter in the beginning of the century and served as President from 2005 through 2007. It was a time when having the kind of involved membership that we have today was but a dream. Our meeting attendance was generally much less impressive than it is today.

Officer positions in the Chapter were frequently hard to fill. It was not unheard of for one person to assume the responsibilities of both Secretary and Treasurer. If there were to be a meeting, it was up to the President to find a location, time and date, identify, seek and coordinate with a speaker, get CPE approval from ACFE, publicize the meeting, prepare the sign-in sheets, print the evaluation forms and issue CPE certificates. And each one of those tasks was a job of its own.

Finding a meeting spot was a task because there was no way of estimating attendance. It's almost funny to reminisce when today our meeting pre-registration closes because of capacity issues well in advance of the meeting.

Identifying a time and date was a challenge because with such low participation, the unavailability of just a few regulars for a particular date would have a major impact on meeting attendance. Getting a meaningful speaker was a challenge either because so few "hot" speakers knew about the ACFE and our Chapter and were therefore reluctant to afford their name, or because the reason that they were willing to be the speaker was seen by them as solely a marketing opportunity, a sales meeting. When they were told that they were expected to use the opportunity to educate our membership about their area of expertise rather than to use the opportunity to pitch their firm or their product, too many of them bailed.

Almost without exception, those individuals who have served as officers of our Chapter who have been members in the past have really put in their time and are marveling about have far our Chapter has come. It was always a concern of mine to seek diversity on our Board. My Board had several females as officers of our Chapter. For whatever reason, most were unable to remain active enough to rise through the ranks.

For the first time our Chapter has a female as President, Dr. Chelsea Binns, and a female Vice President and Training Director, Dora Gomez. My perspective from more than fifteen years in this Chapter may explain why the willingness to assume these impossibly difficult positions

by these two amazing individuals is so exciting and meaningful to me. They are more than our current leaders; they are our future.

Although there are so many people who are eager to take leadership roles, each one of those roles is now so much more complicated and time consuming than it would have been in the past. Our membership demands and receives speaker presentations from notables who are top-notch and who themselves publicize the opportunity of addressing our membership. Computers and the World Wide Web make things easier to administer, but the job of keeping things current demands almost a daily focus. It was easier to identify membership interests when contemplating speakers when attendance and participation was small.

Membership, attendance and participation is now many times what it was, so identifying and securing topics and presenters that will appeal to the spread of our attendees is so much more difficult than it was when I and other individuals of the period served as President and did almost the whole job.

I seek to remain actively involved. If you're already active in our Chapter, I congratulate and thank you for your efforts and diligence. It really shows. If you've yet to become active, I'm eager to see the changes and improvements that you will bring to our Chapter through your own experience, leadership abilities and talent. I and so many others truly appreciate everything that you've already accomplished and everything yet to happen!♦

Steven R. Levine, CFE is President and CEO of Prolective Solutions, LLC (www.prolective.com). The consulting firm works with accounting, legal and construction firms to seek to assure government construction project labor law compliance. Steve is Past Chairman of the Board, Past President and current board member of the New York City Chapter. Email: srlevine@prolective.com

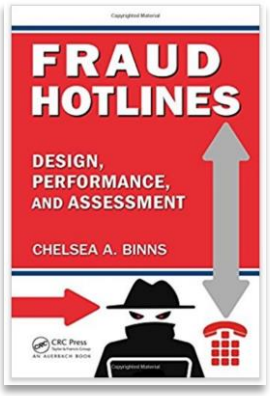
❖



NYCFE Full Day Conference on April 20th at Thomson Reuters in New York City

BOOK CORNER

Editor's Picks for Suggesting Readings

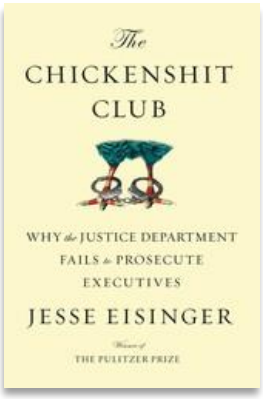


Fraud Hotlines

Design, Performance, and Assessment

Chelsea Binns, Ph.D., CFE, President, NYCFE

This book provides a complete guide on fraud hotlines. It is designed to educate readers with respect to the history, purpose, operation, use and utility of fraud hotlines. It also equips readers with the knowledge to create, analyze and assess the performance of fraud hotlines.



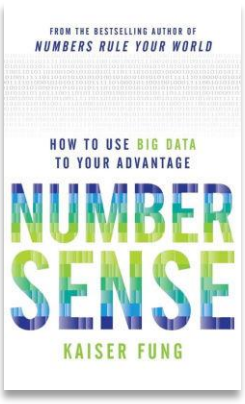
The Chickenshit Club

Why the Justice Department Fails to Prosecute Executives

By Jesse Eisinger

Winner of the 2018 Excellence in Financial Journalism Award

From Pulitzer Prize–winning journalist Jesse Eisinger, "a fast moving, fly-on-the-wall, disheartening look at the deterioration of the Justice Department and the Securities and Exchange Commission…It is a book of superheroes" (*San Francisco Review of Books*).



Numbersense: How to Use Big Data to Your Advantage

By Kaiser Fung

"We live in a world of Big Data—and it's getting bigger every day. Virtually every choice we make hinges on how someone generates data . . . and how someone else interprets it—whether we realize it or not.

The problem is, the more data we have, the more difficult it is to interpret it. From world leaders to average citizens, everyone is prone to making critical decisions based on poor data interpretations." Kaiser Fung

❖

Combatting Identity Theft: *A Resource Guide*

By Laura Hynes-Keller, CFE

Identity theft, tax scams, data breaches, data losses, social engineering, phishing/vishing schemes and other fraud and cybersecurity cons and scams are all too commonplace today for both individuals and businesses. Family, friends, neighbors and business owners often turn to the community of Certified Fraud Examiners seeking answers to questions such as *"How Can I Protect Myself and Others from Getting Scammed?"* and *"What Should I Do Now that My Identity Has Been Compromised?"*

The good news is there are many useful and informative resources available to help combat and mitigate various types of identity theft. Below please find ***Combatting Identity Theft: A Resource Guide**** curated from federal and state government sources, along with industry-funded and not-for-profit entities. Designed as an "*At-A-Glance*" guide, the links provide additional tools, tips and information for more in-depth research and action guidelines in combatting and resolving both personal and business identity theft matters.

Personal Identity Theft

- The Federal Trade Commission's IdentityTheft.gov website is the federal government's one-stop resource to report and recover from identity theft, which includes a step-by-step guide in creating a personalized recovery plan based on individual circumstances. The website features a one sheet listing multiple government agency contacts including the Department of Justice and the U.S. Postal Inspection Agency, leading credit card and telecom companies, and information for key credit reporting agencies.

- The IRS Taxpayer Guide to ID Theft. For 2018, the IRS, the states and the tax industry joined together to enact new safeguards and take additional actions to combat tax-related identity theft.

  Quick IRS Tips:

  - ✓ Forward IRS-related scam emails to phishing@irs.gov.
  - ✓ Report IRS-impersonation telephone calls at tigta.gov.
  - ✓ If you are an identity theft victim whose tax account is affected, see www.irs.gov/identitytheft.

Additional IRS Resources can be found at: Publications, articles, YouTube videos and other identity theft related outreach.

The Identity Theft Resource Center (ITRC) is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cyber security, scams/fraud and privacy issues.

Medical Identity Theft

The U.S. Department of Health and Human Services Office of the Inspector General's OIG Hotline accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in Department of Health and Human Services' programs.

Social Security Identity Theft

The Social Security Administration's Office of the Inspector General website includes information about what it investigates, types of Social Security Fraud, and how to report it.

Metro Area Identity Theft Resources

- The Connecticut State Department of Consumer Protection portal contains multiple links and resources to deal with different types of identity theft.
- The New York State Department of Taxation and Finance website is available to residents of New York State to report fraud, scams, and identity theft, which includes a link to Form DTF-275, *Identity Theft Declaration*.
- The New York State Division of Consumer Protection offers additional identity theft tips and resources for when accounts have been compromised.
- The State of New Jersey Department of Law and Safety/Office of the Inspector General provides a helpful checklist of actions to take in the instance of identity theft.

❖

Business Identity Theft

- The Association of Certified Fraud Examiners offers a free Fraud Prevention Check Up as a downloadable PDF to proactively identify and manage business fraud risks.
- BusinessIDTheft.org offers a Business Identity Theft Victim Action List. Please visit the State Resources section for additional information and identity theft resources in your state or territory. See the Federal Resources section for additional information about U.S. federal government agencies and resources for further assistance.
- The National Association of Secretaries of State has been working with a wide array of industry stakeholders, including state legislators, law enforcement, business support groups, financial institutions and others to combat business identity theft.
- The National Association of State Attorneys General website lists information on how to contact your state's Attorney General.

- The U.S. Department of Justice StopFraud.gov website, run by the Financial Fraud Enforcement Task Force, offers links to multiple resources; a link can also be found on the nycfe.org website.

Employment Related Identity Theft

The IRS clarifies not every data breach will result in identity theft, and not every identity theft is tax-related identity theft.

- IRS Guide to Employment-Related Identity Theft. If you or someone you know is a victim of employment-related identity theft, review the information on your notice or visit Identity Protection or Employment Related Identity Theft for actions you can take to further protect your identity.

- The Federation of Tax Administrators created a State ID Theft Resources Guide. You can review each state's dedicated page with information on what to do if you or your employees are victims of identity theft.

**Please note: This resource guide should not be used in lieu of legal advice.*

❖

SUBMISSION GUIDELINES: We welcome submissions from current NYCFE members including news about professional achievements and milestones, original bylined articles, opinion pieces, case studies, links to pertinent research papers with an executive summary, book recommendations, resources, and additional tips and suggestions for fraud prevention, detection and deterrence. Word count limit 1500. Photos and illustrations can accompany submissions. The deadline for the Fall/Winter 2018 issue is September 30, 2018. Please contact Laura Hynes-Keller via email at laura.hyneskeller@gmail.com with submissions, questions or comments. Thank you.

Things gained through unjust fraud are never secure.

Sophocles