ACFE
Association of Certified Fraud Examiners
New York Chapter #14

SUMMER 2021 / ISSUE 6

TABLE OF CONTENTS

Letter from the President
Dora Gomez 1

About the NYCFE 2

Nine Questions with...
James Tunkey 3

Forensic Linguistics and the Telephone Interview
Jenna Goldin 6

FCC FACT SHEET: Ten Cybersecurity Tips for Small Businesses 9

IBM Cost of a Data Breach Report Infographic 10

Comprehensive Credit Act of 2020
Bruce Hulme 11

Covid-19 Related Fraud Update 13

Identity Theft and Credit Freezes
Laura Hynes-Keller 14

IC3 2020 Elder Fraud Report
Infographic 16

The Changing Face of Hospital Security
Anthony Luizzo, Bernard J. Scaglione 17

Submission Guidelines 21



Letter from the President

Dear Chapter Members and Friends,

As chapter President of the NYCFE I would like to thank you all for your support during the last 15 months as we pivoted to change our chapter meetings to webinars at the height of the pandemic which we have continued since April 2020.

The support of this chapter has increased and continues to do so from a diverse group of chapter members and friends: CFEs, Auditors, CPAs, CIAs, law enforcement, and experts in Compliance, IT Security, CyberCrime, FinCrime, Forensics, Ethics, Governance, Risk Management, etc. We are thankful to have such a variety of professionals join us regularly!

Our Spring Fraud Conference half-day events in April and May were well attended and featured fantastic speakers including a session that included participation from several attendees who were excited to participate virtually.

The feedback we received was extremely positive, and we hope to have another interactive session in our training plans!

It is now the Summer of 2021 and things are moving in the direction of some normalcy. Many of you have asked us when we will once again host in-person events.



President Dora Gomez

Our Fall Fraud Conference will be the start of our chapter making its way back to our gatherings and networking events in NYC!

Fordham University will host our full-day conference on October 22nd offering 8 CPEs, including Ethics credits. You can expect a very unique agenda with new speakers we have not yet invited to our podium - details will be announced as soon as we have confirmed the speakers.

Our next fraud webinar will be July 21st as we welcome the FBI NYC office who will present on a few subjects: the 2021 IC3 Report and a case study on how the financial industry can be impacted by Art fraud. September 15th we will be back from the Summer break and host a fraud webinar on Financial Statement fraud. Both evening sessions offer attendees 2CPEs. We follow strict guidelines from NASBA, so please be sure to join our webinars using the Webinar App and preferrably on a laptop with reliable connection to the internet so you can answer the required poll questions.

This past June I had the pleasure of moderating a panel at the ACFE Global Conference on elder abuse

Copyright © 2021 NYCFE www.nycfe.org

and financial exploitation with some experts, both in the financial and medical field. We plan to bring this topic back again at our chapter this year, given the rise in elder fraud.

We have been fortunate to have several experts present at our chapter and as we expand more and more, we welcome chapter members that would like to volunteer on any one of our committees: Program, Training and Events, Membership, Website, Student and CFE initiative, and others.

NYCFE relies on volunteers that are empowered by our mission in bringing fraud training and awareness to CFEs and other professionals seeking the same. If you feel you have the same passion and time to commit, please reach out to me at President@nycfe.org.

This is a great way to expand your professional development, networking and be part of the success in this chapter.

Once again, NYCFE is proud to be a Double Platinum Donor to the ACFE Foundation's Ritchie-Jennings Memorial Scholarship which supports the education of students who have an interest in pursuing a career in fraud examination.

The scholarship provides an opportunity for students to advance their education and anti-fraud career paths. Many of these outstanding and deserving students go on to become Certified Fraud Examiners. Each year the ACFE Foundation reviews student applications to grant scholarships to. This year, the grand prize $10,000 scholarship winner was from New York along with a few others!

Congratulations to all 22 winners and their pursuit in becoming future CFEs!

Thank you for all you do as anti-fraud professionals and supporting the fraud fighting community!

Stay well, stay safe and we look forward to you joining us at our next fraud webinar and at our in-person event in October and seeing your smiling faces! ☺

Have a wonderful Summer Season!

With much appreciation and gratitude,

Dora Gomez, MS, CFE, CRMA
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 Dora M. Gomez: President@nycfe.org
For General Questions: Info@nycfe.org
For Newsletter Questions, Comments and Submissions: Newsletter@nycfe.org
For Training, Events, Speaker and Sponsor proposals: Training@nycfe.org
Connect with NYCFE on LinkedIn

ACFE NEW YORK CHAPTER BOARD OF DIRECTORS

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

NINE QUESTIONS WITH...JAMES TUNKEY, I-ONASIA



James Tunkey, MBA, CFE, has nearly three decades' experience as a fraud fighter, mostly focused on Asia white collar crimes. Since 2004 he has handled more than 5,000 assignments in critical and complex areas including Due Diligence, Crisis Management, Security Services, Corporate Investigations, and Litigation Support. James's fraud investigation work builds upon his international experience and skills as an analyst of large and complex data sets.

James holds an MBA jointly conferred by NYU Stern, the London School of Economics and HEC Paris. He is a proud member of the National Committee on US-China Relations, the International Organization of Asian Crime Investigators & Specialists, and OSAC's Pan Asia Regional Council, among other groups. A regular speaker at ACFE chapter events worldwide, in 2020 James presented to the NYCFE on the topic of investigations involving physical evidence. Recently, he has been presenting new material to ACFE chapters to consider problems stemming from the dramatic growth in cyber fraud, while identifying opportunities for fraud fighters in the private sector.

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

I have worked as an investigator of bribery, corruption, money laundering, and sanctions busting for my entire career. Many of my earliest cases involved major headline issues. Perhaps I was picked to be a part of the investigative teams because I was willing to travel to some risky places. (When I was working one particular project in Indonesia in the late 1990s, for example, I spent weeks working out of a hotel that was surrounded by tanks and rioting protesters.) Perhaps I was picked to work the cases because I willing to put in extremely long hours. But I enjoy seeing the world and I've been working hard since I was 12 years old, so those things that might have been hard for someone else didn't seem to matter to me. I simply loved the analytical and problem-solving aspects of the job. Somewhere along the way I decided to become more serious about developing my skills and qualifications as a fraud fighter investigating bribery and corruption and sanctions issues. My then supervisor, a former Detective Senior Superintendent of the Hong Kong Police Force, recommended that I consider pursuing the CFE qualification to cement my skills. I trusted his recommendation and am so glad to have celebrated my 20th anniversary as a CFE last year.

Q: How has bribery and corruption and money laundering changed over these past decades?

Our team mostly focuses on Asia. In that region over the past few decades, things have been relatively stable and there have been a few instances where heads of state or senior government ministers have been deposed for fraud and corruption. When I began my career there were still aspects of the clean-up of the Marcos regime in the Philippines, which used very blunt schemes. In Indonesia in the 1980s and 1990s, there was something called "Soeharto Inc.," in which a group of families tied to the president set up corporations and received special permissions in exchange for making offshore payments globally, which was more sophisticated. Certainly, fraudsters have 'gone corporate' in the years since. For example, the Panama Papers demonstrated that there are some substantial challenges with fraudsters and corrupt officials utilizing corporate secretarial services to set up companies that help them access the world's financial network whilst hiding in the shadows. The 1MDB scandal that has recently affected Malaysia is probably the biggest headline-grabbing instance of a fraud that generated political instability. The fraud was very corporate and involved investments and a veneer of professionalism.

Lately, we've been very interested in the possibility that we are seeing a trend of fraud becoming weaponized at the national level. This kind of turns the situation on its head. Instead of a leader accepting bribes or acting corruptly to benefit his family, fraud becomes an enterprise that is sanctioned by the state. Work is farmed out to syndicate departments who specialize in critical aspects of cyber-attacks and data theft. Non-core activities are subcontracted, such as bank account opening. And specialist "gig workers" workers are utilized, for example as mules for cash movement. So, I think fraud investigation expertise is becoming more important at the strategic level than it ever has been.

When you dig down into the weeds of money laundering investigations, we also spend a lot of time investigating money laundering through the region's casinos. It used to be that we'd focus on the abuse of the mud-chip system in Macau, which is a special kind of chip for high rollers that can used to move money around. There's been an enforcement crackdown on this system. Certainly, fraudsters never stop evolving, and a few years ago we began to see a rise in the use

Copyright © 2021 NYCFE www.nycfe.org

of Bitcoin ATMs. But the old ways of moving money around remain very much still in use. For example, hawala networks used within various South Asian communities.

Q: When many people think about Asia, they worry about the theft of trade secrets. What are your views?

I've been working this issue of intellectual property (IP) rights protection for so very long. I remember the flap caused by a senior US Trade official when she brought home knock-off Beanie Babies from a trip to Asia in the 1990s…

And before I go on… Thinking about this solely as a problem with an Asian face would lead to many bad results. There are plenty of home-grown Americans that steal from their compatriots. Beyond tech, I am thinking of a recent story of a well-regarded garment company executive whose child had a side hustle that involved IP infringement.

In the 2000s, many corporations thought that the best way to protect against IP theft was to be more like Coca-Cola: expand globally and let the vast majority of employees have access to most of the business, but furiously guard the formula close to home. American tech companies also boldly claimed they could innovate faster than foreign copycats could steal their ideas. But IP thieves, including foreign copycats, responded by coming to America and infiltrating companies as employees and contractors.

Our team is very active in this arena, which is really a form of fraud and misappropriation of intangible assets. So, I'm a big advocate for more CFEs playing a key role in fighting IP theft. Despite all of the hype and headlines--and IP theft is very much at the top of the corporate and diplomatic agenda--it has been my experience that CFEs have not been playing prominent roles in the fight against IP theft. Perhaps readers have some feedback on whether the community would benefit from more training materials and case studies on this topic.

Q: What is FCPA Due Diligence?

Over the past 27 years I have worked literally thousands of due diligence cases, mostly for corporations and venture capital investors that want to buy a new business, or on behalf of companies pursuing an IPO or SPAC. As a CFE, I bring an insight into the different ways in which fraud can kill a business' future, which I apply by performing background checks into senior managers and even third parties, such as key customers or suppliers.

FCPA Due Diligence involves looking at potential business deals to make sure there is limited risk of corruption, often by taking a careful look at the compliance program. It is an increasingly important practice area, and one where a CFE can make a big impact, particularly for companies listed in the United States or headquartered in Europe. Shareholders will reward cleanly run companies, and regulators penalize businesses that engage in corrupt practices.

A CFE should be able to look at a business from a unique perspective, testing for risks and making recommendations for improvements. CFEs have the skills to dig deep to search for corruption in procurement or look for problems with bid rigging. Our teams perform a lot of this type of due diligence in Asia, working hand in glove with white collar legal counsel.

Once the work of FCPA Due Diligence is complete and there has been a needs assessment, in many cases a new compliance program might be recommended. CFEs can play key role as implementers of these new programs.

Q: What would you tell someone just starting their career as a CFE?

First, congratulations! Thank you for joining our guild of specialists dedicated to solving one of the world's biggest business challenges. Criminologists understand that there are significant gaps in our understanding of the true losses caused by fraud and related white-collar crimes such as bribery, corruption, money laundering, and sanctions busting. The problem is bigger than what may be recorded, and so much of the case knowledge and experience is kept private and confidential at the individual or corporate level. One of the things I like about my job is my firm sees a substantial volume of cases, which gives me better fraud fighting insights. I'd encourage any new CFE to follow my lead.

I see my job as having the potential to help a lot of people in times of need. The private sector has been investing heavily to fight fraud in new ways, using tech that was only a dream even a decade ago. The pace of change is rapid. Today there are a handful of fraud-tech companies with billion-dollar valuations. These "unicorns" hold the promise of delivering fraud fighting solutions to the biggest consumer, finance, and other businesses with digital strategies. Models are only as good as the specialists who build them, and predictive analytics are only useful to practitioners who know their strengths and weaknesses. Programmers and information security specialists are going to need experienced CFEs to connect to internal and external customers swamped with fraud losses, increasingly originating in data breaches and international in scope, and bridge key knowledge gaps.

Copyright © 2021 NYCFE www.nycfe.org

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

Recently our team had a fraud come in that involved Letters of Credit. I saw my first fraud involving this instrument 25 years ago. My historic experience made it easier for me to assist the victim understand how the fraud occurred and identify how the problem could be solved. Insights come from experience. There are no short-cuts. Insights and techniques come from hard work and time.

But I love new technology and am ALWAYS open to new tools and techniques that work. Lately, for example, our company I-OnAsia invested in a technology that ingests data from a variety of sources, applies fraud fighting analytics, and generates visualizations in a workflow that is far beyond anything we might have expected possible decades ago. Our team is using this tool now on nearly every case, to reduce the cost and time taken to generate leads and to create insights. It is exciting.

Q: What do you do for fun or relaxation?

I love to cook for my family and friends. Recently we had a friend come over for lunch who doesn't cook much. Her mother died when she was young. It was a very simple piece of chicken I made, with some dill and set over a salad. "This is home cooking," she said. It meant a lot because I know she had very little of it. Food has the power to make people happy and feel comfortable. When I am really relaxed, I'll make something that can be stuck in the freezer. Recently I bought a second freezer, which I've only stocked with ice cream. It's been so much fun for the family having 20 different flavors at hand.

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

I like to read and have pretty varied tastes. Right now, I am reading "The Death of Expertise" by Tom Nichols. I am very interested in the rising distrust of experts. The book is useful for anyone like me who has spent a lifetime becoming truly knowledgeable about an issue. For me, its China. I'm an Old China Hand with a clear record of the right calls on key aspects of the US-China relationship. I'm an American who has spoken and read Chinese for nearly 30 years. I have spent a lifetime studying Chinese culture. I've lived in China and am very familiar with many Chinese business activities.

Separately, in my NYCFE presentation last year entitled "Finding That Needle in The Haystack" I spent some time talking about the importance of asking good questions in fraud fighting. I quote from the book *Hound of the Baskervilles* by Sir Arthur Conan Doyle. The idea that there are clues in unseen things that may observed to be missing, is a profound insight.

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

I have truly enjoyed providing training to fellow CFEs around the world. I think I have spoken to nearly 20 chapters in the past two years. I learn so much from the audience feedback and questions. ♦

James Tunkey is NYC Head & Chief Operating Officer of I-OnAsia, a global risk management consultancy. Email: james@ionasia.com.hk



Copyright © 2021 NYCFE www.nycfe.org

FORENSIC LINGUISTICS AND THE TELEPHONE INTERVIEW

Jenna Goldin, CFE



Imagine you are tasked with overseeing a fraud investigation into a large company. As part of your investigation, you must conduct interviews with current and former employees of the organization, but because of COVID-19, everyone has been working from home. You now must schedule remote interviews in order to move forward with the investigation.

Due to the technology limitations of people's home computers, many of the interviews must happen over the telephone. You are concerned by the limitations of telephone interviews because you are used to conducting interviews in person. Telephone interviews lack the helpful visual feedback such as body language that fraud examiners might typically use as part of their investigation skills to either build rapport or communicate effectively.

Even beyond the situation presented by the pandemic, as technology has advanced, the need for in-person communication has begun to diminish. Whether it be business meetings through Zoom, catching up with family on FaceTime, or conferences via telephone, individuals and fraud examiners alike are shifting away from in-person and towards distanced communication. These various means of communication present a new set of challenges for the fraud examiner. Linguistics, the scientific study of language, can be quite useful to the fraud examiner in helping to better understand how language is used to communicate more effectively. Linguistics can provide insights into how we communicate, which can help the fraud examiner to better prepare for and overcome issues relating to an interview over the telephone.

The applied field of forensic linguistics, or the application of the study of language in a forensic setting, can go even further in helping the fraud examiner during an interview. Forensic linguistics was first popularized by linguistics professor Dr. Roger W. Shuy. Forensic Linguistics has been successfully applied in many instances including trademark infringement, product liability, authorship cases, and more. Forensic Linguistics has even been used to study ways to clarify jury instructions, determine issues of power between attorneys and witnesses in the courtroom, and help to better the use of interpreters in a legal setting. More information on forensic linguistics and its uses can be found on Dr. Shuy's website.

An investigative interview can be considered a forensic setting, and by applying linguistic concepts to conducting telephone interviews, we can add to our skill set and continue to successfully achieve our investigative goals. By understanding the definitions of the linguistics concepts of schema, medium, and phatic expression, the fraud examiner can hone their skills and develop new tools that will help combat the challenges presented by remote telephone interviews.

Schema: How We View the World

In any interview, avoiding miscommunication is key to extracting accurate information. To aid in actively avoiding miscommunication, it is imperative to understand the concept of schema. According to sociolinguist Janet Holmes, schema is "the set of expectations that we bring to an interaction, based on our previous experiences and our cultural norms[1]."

By understanding that each individual's communication style is directly impacted by their own experiences, including the language or languages they speak, the fraud examiner can take a more holistic approach to an interview and be even more exact when trying to interpret answers given in an interview setting. In a telephone interview, fraud examiners are limited to only hearing a person's voice. A speaker's accent, grammar, and word choice can often be subtly interpreted by a listener, triggering unconscious assumptions about both the individual and what they are trying to say.

For example, a speaker's accent may lead an investigator to believe the individual does not speak English as their first language, which could lead to problematic assumptions about their intelligence or their understanding of the interview topic. Fraud examiners should approach any interview with an open mind about the interviewee to mitigate any potential miscommunication issues.

Medium: The Means of Communication

The linguistic concept of medium, or the means through which the communication is happening, is very important to keep at the forefront of the mind when conducting a remote interview. The concept of medium is heavily explored in Barbara Johnstone's book *Discourse Analysis.*[2]

Medium shapes the discourse, no matter what it is. Examples of different mediums include email, video conferencing, or telephone. The way we communicate is directly impacted by that means.

Think about how your communication style changes from texting your friends and family versus a telephone conference with colleagues. The

[1] Janet Holmes, *An Introduction to Sociolinguistics: Third Edition* (2008), 376.

[2] Barbara Johnstone, *Discourse Analysis: Second Edition* (2008), 195.

Copyright © 2021 NYCFE www.nycfe.org

medium of the telephone creates new challenges in communication and changes the speaking style of both the investigator and the interviewee. One such difference is how speaking turns are taken in the conversation. Johnstone describes turns as the unit of conversation when one person starts to speak and then stops speaking.[3]

This could be because their utterance came to a stop naturally or because they were interrupted. When in-person, individuals can employ body language and other subtle visual cues to know when their turn is over or when they can start their turn. Over the telephone, this visual feedback is no longer available. Verbal feedback is the only available indicator to let a speaker know when they can take their turn. It is very easy to inadvertently speak over an interviewee, which may make for uncomfortable conversation or cause the fraud examiner to miss something important the interviewee has said.

The verbal feedback that indicates it is another speaker's turn could be the end of a sentence or thought, a long pause, or when their speech starts to slow down. It can be an adjustment when trying to move from in-person communication to telephone interview, so take your time and adjust to the pace of the interviewee. This will allow you to control the flow of the conversation more easily while simultaneously building a rapport with the individual.

Phatic Expression: When 'Yes' Doesn't Mean 'Yes'

The final concept discussed here that can assist in conducting remote interviews is phatic expression. According to The British Council's Teaching English website, phatic communication is defined as "verbal or non-verbal communication that has a social function… rather than an informative function.[4]"

Linguist, Janet Holmes describes phatic utterances as being used to express empathy in conversation, making these utterances social markers rather than referential information.[5] Have you ever been in a conversation where someone replies with utterances such as, "right, uh huh, and…" and then goes on to create a contradictory or unrelated point? This is a great example of the use of the seemingly affirmative words "right" and the verbal "uh huh" in a way where they might not actually be in verbal agreement of a question, but rather a social filler. In these instances, it is important for the fraud examiner to go back and ensure that any verbal agreement is solid and not just a speech function used out of social politeness.

Making Linguistics Your Own: *Best Practices*

Over my career in investigations, I have been able to incorporate these and other linguistic concepts into conducting successful telephonic interviews. In fact, most of my investigative work has been done over the telephone, even prior to the pandemic. There have been instances where I have had to interview individuals over the phone in other countries where language barriers have caused issues in communication. Keeping in mind the cultural differences that might be impacting the interviewee's schema, I was careful not to make assumptions about what they might be trying to convey and conduct successful interviews that have helped in my cases.

Phatic expressions can also vary greatly depending on a speaker's native language, so as fraud examiners, we should take extra care to ensure we receive firm responses to our questions, and not confuse filler words for affirmative replies.

With all this in mind, we can come up with a few best practices when conducting an interview over the telephone:

1. When interviewing over the phone, allow the person to come to a complete stop in their sentence or phrase before beginning your next statement or question. This will allow the individual to fully get their point across and give you time to ensure you understand their answer. Do not speak over an interviewee as this might make them uncomfortable and cause you to miss vital information.

2. Listen closely to the language the interviewee uses. Do they say, "yeah, but" or "yeah, and" when answering your question? Do they say "right" or "uh huh" while you're talking, as if they are agreeing with you? This might be phatic expression, rather than affirmative responses. If you believe the individual is simply using "yes" to carry on with the conversation, go back and double check on their answer. The difference could be a key factor in your investigation.

3. Understand that each individual has their own unique perspective and background which could influence the way in which they communicate. A person's native language, culture, and background will impact their word choice, and their chosen words might mean different things to you than it does to them.

Although we focused heavily on the telephone interview here, these ideas are not just limited to that medium. Many of us have had to conduct business on Zoom or other web-based video platforms. The concepts still apply to that medium, with the additional benefit of being able to see the individual, make eye contact, and use visual cues to help form rapport.

While COVID-19 has quickly changed the landscape for some of us in our work, the challenges it has presented will not disappear as quickly as they have arisen. The pandemic has made it clear the **increasing need to rely**

[3] Johnstone, *Discourse Analysis*, 102.
[4] "Phatic Communication," British Council Teaching English, February 23, 2021, https://www.teachingenglish.org.uk/article/phatic-communication
[5] Holmes, *An Introduction to Sociolinguistics*, 271.

Copyright © 2021 NYCFE www.nycfe.org

on technology in almost every field. Language is one of the most powerful tools of the fraud examiner and being able to understand linguistic concepts can only be beneficial moving forward into whatever comes next. ♦

Resources:

For more information on Forensic Linguistics, please visit the following websites and articles:

1. International Association of Forensic Linguists: https://www.iafl.org/forensic-linguistics/
2. New Yorker: Words on Trial https://www.newyorker.com/magazine/2012/07/23/words-on-trial

Jenna Goldin, CFE, holds a M.A. in Applied Linguistics – Forensic Linguistics. She is a Senior Investigator with Bernstein Litowitz Berger & Grossmann LLP. Email: Jenna.Goldin@blbglaw.com

FCC DATA SPOTLIGHT: 2020 TOP FIVE ROBOCALL COMPLAINTS

Auto warranty renewal scams were the top robocall complaint filed with the FCC by consumers in 2020, with the long-time front runner, *social security phishing scam calls*, coming in second.

So far in 2021, the number of auto-warranty complaints continues to grow, with January seeing a near 50 percent increase in consumer complaints compared to December 2020.

Auto warranty calls may include specific information about your particular car and warranty that can make the call seem more legitimate. To hear an audio sample of an auto warranty call and to learn how to avoid being scammed, visit the FCC's consumer guide on auto warranty scams.

Rounding out the top five unwanted call categories reported to the FCC in 2020 were computer tech support calls, credit repair and credit card rate reduction calls, and health insurance calls.

Most of the reports received by the FCC mention that the unwanted call begins with an automated or pre-recorded message that may instruct you to press a certain number or stay on the line. To avoid robocall scams follow these top tips:

Do not answer calls from unknown numbers. If you do so by mistake, hang up immediately. If you answer the phone and the caller – or a recording – asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.

Visit the FCC website to learn more about robocalls and visit the FCC Scam Glossary at fcc.gov/scams. Also check out the consumer guide on call blocking tools and resources. To file a consumer complaint with the FCC, visit fcc.gov/complaints.

Copyright © 2021 NYCFE www.nycfe.org

FCC FACT SHEET: *Ten Cybersecurity Tips for Small Businesses*

Broadband and information technology are powerful tools for small businesses to reach new markets and increase sales and productivity. However, cybersecurity threats are real, and businesses must implement the best tools and tactics to protect themselves, their customers, and their data. Visit www.fcc.gov/cyberplanner to create a free customized *Cyber Security Planning* guide for your small business and visit www.dhs.gov/stopthinkconnect to download resources on cyber security awareness for your business.

Here are ten key cybersecurity tips to protect your small business:

1.**Train employees in security principles**. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. **Protect information, computers, and networks from cyberattacks**. Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. **Provide firewall security for your Internet connection**. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. **Create a mobile device action plan**. Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. **Make backup copies of important business data and information**. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6. **Control physical access to your computers and create user accounts for each employee**. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. **Secure your Wi-Fi networks**. If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. **Employ best practices on payment cards**. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

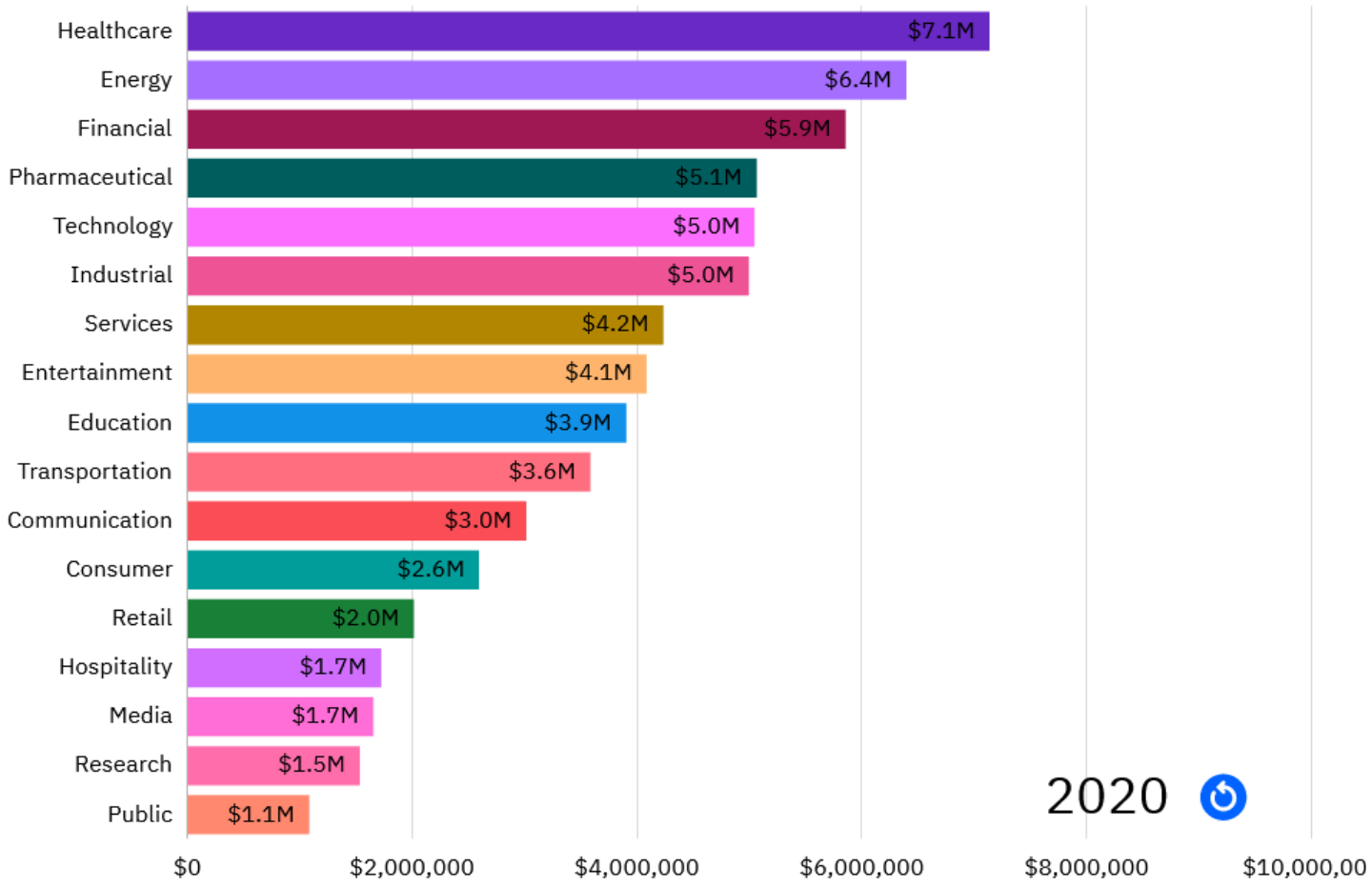
9. **Limit employee access to data and information, and limit authority to install software**. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs and should not be able to install any software without permission.

10. **Passwords and authentication. Require employees to use unique passwords and change passwords every three months**. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account. The FCC's Cybersecurity Hub at http://www.fcc.gov/cyberforsmallbiz has more information, including links to free and low-cost security tools. Create your free small business cyber security planning guide at www.fcc.gov/cyberplanner.To learn more about the Stop. Think. Connect. Campaign, visit www.dhs.gov/stopthinkconnect

Copyright © 2021 NYCFE www.nycfe.org

SPOTLIGHT

IBM COST OF A DATA BREACH REPORT 2020



Copyright © 2021 NYCFE www.nycfe.org

COMPREHENSIVE CREDIT ACT OF 2020

Bruce H. Hulme, CFE, BAI



H.R. 3621 — 116th Congress: Comprehensive CREDIT Act of 2020, which passed the U.S. House of Representatives on January 29, 2020, provides for additional consumer credit protections, sets forth requirements for credit reporting agencies, and prohibits the inclusion of specified information on credit reports.

TITLE I—IMPROVEMENTS TO THE DISPUTE PROCESS

The dispute process for consumers challenging information contained on their credit report is revised for challenges (1) through the credit reporting agency, and (2) through the furnisher of credit information. Credit reporting agencies must disclose to consumers how to dispute this information. If a credit report is revised as a result of a dispute, the credit reporting agency must provide the consumer a free copy of the revised report and credit score. Furnishers of credit information must maintain all records to substantiate the credit information provides to credit reporting agencies. Consumers must be notified when a furnisher provides specific negative credit information within five business days of it being reported to a credit reporting agency.

The bill also establishes an appeals process for disputed credit information and sets forth procedures for the credit reporting agencies and furnishers of this information. Credit reporting agencies must identify disputed information on a credit report and ensure accuracy and completeness in credit reports. The bill also establishes the right for courts to award injunctive relief to require compliance with consumer credit laws.

TITLE II—FREE CREDIT SCORES FOR CONSUMERS

The bill requires credit reporting agencies to provide free credit scores to consumers along with their free annual credit reports. The bill also provides for

- additional free credit scores and credit reports when a consumer is disputing information contained on their credit report or has had previously removed information reinserted into their report, and
- automatic free credit scores and credit reports to consumers who have obtained a fraud alert or security freeze.

Credit reporting agencies must provide consumers with additional information regarding the calculation of their credit score, including factors that adversely effected the score, and specific actions a consumer may take to improve the score.

The bill establishes educational credit scores to be used by a consumer in understanding how a lender or creditor may use the information contained in a consumer's credit report if a current credit score is not available.

Private education lenders, motor vehicle lenders, indirect auto lenders, and residential mortgage lenders must give consumers free copies of consumer reports or credit scores used for making underwriting decisions before consumers sign the respective loan agreements.

TITLE III—STUDENT BORROWER CREDIT IMPROVEMENT ACT

The bill prohibits a credit reporting agency from furnishing a credit report containing any adverse item of information relating to a delinquent or defaulted private education loan of a borrower who has a specified demonstrated history of loan repayment.

TITLE IV—CREDIT RESTORATION FOR VICTIMS OF PREDATORY ACTIVITIES AND UNFAIR CONSUMER REPORTING PRACTICES

The bill revises the information included on a credit report by

- requiring removal of adverse information that resulted from fraudulent lending activity regarding private education loans and residential mortgage loans,
- expediting the removal of debt that is no longer owed,
- prohibiting the inclusion of an arrest that did not result in conviction,
- in general, reducing the time period adverse information stays on a credit report from seven years to four years, and
- limiting the inclusion of certain medical debt.

TITLE V—CLARITY IN CREDIT SCORE FORMATION

The Consumer Financial Protection Bureau (CFPB) must regulate credit score models by establishing standards for validating the accuracy and predictive value of these models. The bill also gives the CFPB the authority to prohibit the use of certain factors in credit score models. The CFPB must report on the impact of the inclusion of nontraditional data in these models.

TITLE VI—RESTRICTIONS ON CREDIT CHECKS FOR EMPLOYMENT DECISIONS

A credit reporting agency is prohibited from providing a consumer's credit information for employment purposes, unless the information is for a national

Copyright © 2021 NYCFE www.nycfe.org

security investigation, for a background check or investigation required by regulation, or otherwise required by law.

TITLE VII—PROHIBITION ON MISLEADING AND UNFAIR CONSUMER REPORTING PRACTICES

The bill prohibits automatic renewals for promotional consumer credit products and services, allows the CFPB to set maximum fees for products and services offered by credit reporting agencies, and allows for multiple credit inquiries of the same type without penalty to a consumer's credit score.

Additionally, the bill directs the CFPB to issue rules to provide for

- access to consumer reporting information for nonnative English speakers, the visually impaired, and the hearing impaired; and
- the registration of credit reporting agencies.

The bill also establishes credit protections for consumers affected by a government shutdown.

TITLE VIII—PROTECTIONS AGAINST IDENTITY THEFT, FRAUD, OR A RELATED CRIME

The bill revises fraud alert protections to allow for an extension of these protections upon request of the consumer if the threat of fraud is ongoing. The bill also requires a credit reporting agency to provide free credit monitoring and identity theft protection services to victims of fraud, the unemployed, recipients of public assistance, active duty uniformed consumer, and those 65 years of age and older.

The bill expands to victims of fraud existing consumer protections applicable to victims of identity theft, including free credit scores, additional free credit reports, and access to records of fraudulent activity. The CFPB must develop procedures for reporting fraud and other related crime.

TITLE IX—MISCELLANEOUS

Contract provisions that violate specified consumer protections or that are against the public interest are null and void.

The Government Accountability Office (GAO) must study (1) the use of credit reports and credit scores in housing determinations, (2) the effects on future lending of credit scores impacted by defaulted or delinquent private student loans, and (3) credit reporting agency compliance with consent orders.

The bill revises consumer credit protections for service members. The bill (1) extends consumer credit protections to certain active duty uniformed consumers in a combat zone or aboard a U.S. vessel, (2) prohibits the inclusion on a credit report of adverse credit information that occurred while a uniformed consumer was engaged in that type of active duty, and (3) provides for negative credit information alerts to such consumers. The bill also adds to those groups covered by specified active duty credit protections individuals in the commissioned corps of the National Oceanic and Atmospheric Administration and the Public Health Service.

The bill allows for the reporting of certain positive consumer credit information to credit reporting agencies. Specifically, a person may report information related to a consumer's performance in making payments either under a lease agreement for a dwelling or pursuant to a contract for a utility or telecommunications service. The GAO must report on the consumer impact of such reporting.

Nationwide credit reporting agencies are subject to supervision and examination by the CFPB with respect to cybersecurity. ♦



217th Congress – *Proposed House Bills*

The following measures were before the House Judiciary Committee before Chairwoman Representative Maxine Waters (D-CA). The events of January 6th in Washington, D.C. resulted in the following proposed measures:

- H.R.____, the "Domestic Terrorism Financing Study Act."
- H.R.____, the "FinCEN Exchange Improvement Act."
- H.R.____, the "Freezing Assets of Suspected Terrorists and Enemy Recruits (FASTER) Act of 2021."
- H.R.____, the "Fraud and Terrorism Education Act."

In essence, they would:

- Require the Comptroller General of the United States to carry out a study on the financing of domestic violent extremists and terrorists, including foreign terrorist-inspired domestic extremists, and for other purposes.
- Require financial institutions to freeze the assets of individuals arrested under suspicion of participating in domestic terrorism or providing material support to terrorists, to establish a national clearinghouse for information on incidents of homegrown ''lone wolf'' terrorism, domestic terrorism, and persons providing material support to terrorists, and for other purposes.
- Require the Director of the Financial Crimes Enforcement Network to produce and distribute educational materials designed to help Federal, State, local and Tribal agencies responsible for distributing public benefits to understand, identify, and avoid fraud, particularly fraud that includes that involves terrorist financing schemes, and for other purposes.
- Amend title 31, United States Code, to require the

Copyright © 2021 NYCFE www.nycfe.org

Secretary of the Treasury to establish a program, as part of the FinCEN Exchange, to allow designated employees of financial institutions to receive access to certain classified information related to terrorism (both domestic and international), sedition, and insurrection.

No doubt significant portions of sections of the above bills would need to be amended before obtaining nonpartisan support in the Senate. ♦

Bruce H. Hulme, CFE, BAI, is a Certified Fraud Examiner, Board Accredited Investigator, and NYCFE Vice Chair. Email: specialinvestigations@att.net

Covid-19 Related Fraud Update

Earlier this year the Department of Justice announced in criminal and civil enforcement efforts to combat COVID-19 related fraud, including schemes targeting the Paycheck Protection Program (PPP), Economic Injury Disaster Loan (EIDL) program and Unemployment Insurance (UI) programs.

As of March 26, 2021, the Department of Justice had publicly charged 474 defendants with criminal offenses based on fraud schemes connected to the COVID-19 pandemic. These cases involve attempts to obtain over $569 million from the U.S. government and unsuspecting individuals through fraud and have been brought in 56 federal districts around the country.

To report suspected illicit activity, please visit:

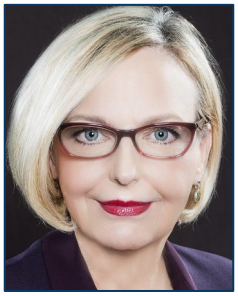
https://www.fincen.gov/coronavirus

Copyright © 2021 NYCFE www.nycfe.org

IDENTITY THEFT AND CREDIT FREEZES

What to Do When Your Information Is Lost or Exposed

By Laura Hynes-Keller, CFE



By now many people have received notifications that their personal information was exposed in a data breach or hack. Or maybe your online accounts were compromised, or your wallet was lost or stolen, any of which can result in identity theft. Depending on what information was lost, there are steps you can take to not only help protect yourself from identity theft in the first place, but also help mitigate its ongoing impact.

How to Report the Incident

If fraudsters have stolen your identity and **used** your information to open new accounts and make purchases, it's important to file an identity theft report at the FTC's IdentityTheft.gov. It's a terrific step-by-step guide that allows individuals to customize their report based on their specific circumstances.

Preventative Measures

According to the Federal Trade Commission, credit freezes and fraud alerts can protect you from identity theft or prevent further misuse of your personal information if it was stolen. In September 2018, Congress made credit freezes free; the credit bureaus offer paid subscription services with additional features.

What To Know About Credit Freezes and Fraud Alerts

- Credit Freezes

Who: Anyone can freeze their credit report, even if their identity has not been stolen.

What: A credit freeze restricts access to your credit report, so you—or fraudsters—cannot open a **new credit account** while the freeze is in place. However, you can *temporarily* lift the credit freeze if you need to apply for new credit. Even with the freeze in place, you will still be able to apply for a job, rent an apartment, or buy insurance without lifting or removing it. Implementing a credit freeze will not impact your credit score.

Duration: A credit freeze lasts until you remove it.

Cost: Free

How: Contact **each** of the three credit bureaus — Equifax, Experian, and TransUnion.

- Fraud Alerts

Fraud alerts are available in different situations and have different benefits.

Who: Anyone who suspects fraud can place a fraud alert on their credit report.

What: A fraud alert will make it more difficult for a fraudster to open a new credit account in your name. A business is required to verify your identity before it issues new credit in your name.

When: Once you place a fraud alert on your credit report, you can obtain a free copy of your credit report from each of the three credit bureaus.

Duration: A fraud alert lasts one year. After a year, you can renew it.

Cost: Free

How: Contact any one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact first must tell the other two to place a fraud alert on your credit report.

Extended fraud alert

Who: An extended fraud alert is only available to people who have had their identity stolen and have completed an FTC identity theft report at IdentityTheft.gov or filed a police report.

What: Like a fraud alert, an extended fraud alert will make it harder for someone to open a new credit account in your name. A business must contact you before it issues new credit in your name.

When: You can place an extended fraud alert on your credit report as well as obtain a free copy of your credit report from each of the three credit bureaus **twice** within one year from when you place the alert, which means you could review your credit report six times in one year.

In addition, the credit bureaus will take you off their marketing lists for unsolicited credit and insurance offers for five years, unless you ask them not to.

Duration: An extended fraud alert lasts seven years.

Cost: Free

How: Contact any one of the three credit bureaus — Equifax, Experian, and TransUnion. It is not necessary to contact all three. The credit bureau you contact must tell the other two to place an extended fraud alert on your credit report.

Active duty alert

Who: Active duty service members can place an active duty fraud alert.

What: An active duty fraud alert will make it harder for someone to open a new credit account in your name. A business must verify your identity before it issues new credit in your name.

In addition, the credit bureaus will take you off their marketing lists for unsolicited credit and insurance offers for two years, unless you ask them not to.

Duration: An active duty fraud alert lasts one year. After a year, you can

Copyright © 2021 NYCFE www.nycfe.org

renew it for the length of your deployment.

Cost: Free

How: Contact any one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an active duty fraud alert on your credit report.

Free credit monitoring for active duty service members

Active duty service members can get free electronic credit monitoring, which can detect problems that might be the result of identity theft. To sign up, contact **each** of the three credit bureaus — Equifax, Experian, and TransUnion.

Freezing your credit and placing fraud alerts at the credit bureaus—which does not take much time--can help reduce the risk of identity theft. ♦

Laura Hynes-Keller, CFE, is founder of LHK Communications, LLC, a boutique consulting firm specializing in strategic communications and media relations. Email: info@lhkcommunications.com

The FBI's Internet Crime Complaint Center 2020 Internet Crime Report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. State-specific statistics have also been released and can be found within the 2020 Internet Crime Report and in the accompanying 2020 State Reports.

The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic.

- **Phishing**: A scam by which an Internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly.
- **Vishing**: A combination of 'voice' and 'phishing,' is a phone scam designed to get you to share personal information.
- **Smishing**: a form of phishing that involves a text message or phone number.
- **Pharming** is a form of online fraud involving malicious code and fraudulent websites.

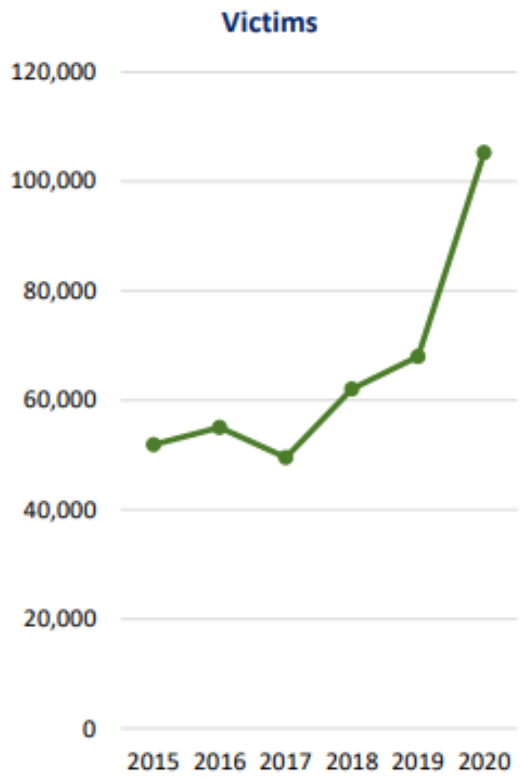
Copyright © 2021 NYCFE www.nycfe.org

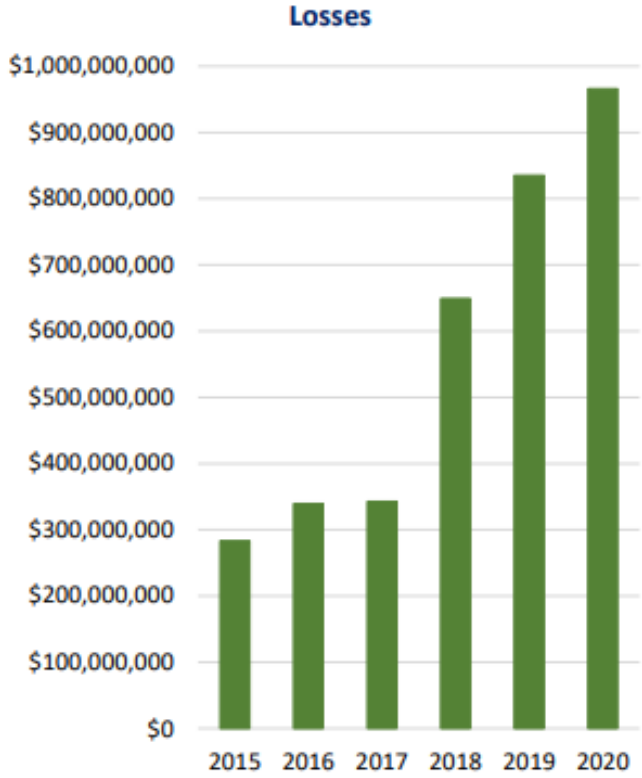
IC3 2020 ELDER FRAUD REPORT

2020 VICTIMS BY AGE GROUP

Victims		
Age Range[2]	Total Count	Total Loss
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

OVER 60 VICTIM REPORTING FOR PAST FIVE YEARS[3]





[2] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

[3] Charts describe Over 60 Victim Counts and Losses from 2015 – 2020.

Copyright © 2021 NYCFE www.nycfe.org

THE CHANGING FACE OF HOSPITAL SECURITY

Anthony J. Luizzo, Ph.D., CFE, CST, PI (Ret. NYPD)
Bernard J. Scaglione, CPP, CHPA, CHSP



Increases in workplace violence, shootings, and other crimes within the healthcare environment are a siren call to all healthcare protection professionals to devise strategies to combat these horrendous threats. Over the past few years these attacks on workers have escalated and are challenging healthcare security executives to leave the land of the familiar and begin seeking new and more innovative protection blueprints. Many hospital security executives are not sitting idle waiting for their institution to be affected, they are taking the bull by the horns and actively seeking security remedies to adequately handle all fast-coming threats.

Sundry strategies under consideration include conjoining in-house surveillance technologies with external public video systems, installing turnstiles, employing magnetometers, arming security personnel, promulgating firearms related "use of force" policies, employing metrics to showcase proficiencies and substantiate expenditures, and involving robotics and drones in standard security machinations. To effectively evaluate institutional crime risk exposure, more forward-thinking security executives turn to the security assessment for guidance. In competent hands, an assessment is analogous to a medical CT scan (computed tomography) a device used by medical experts to diagnose and treat illness. This risk assessment tool helps to diagnose and prescribe remedies for frail security programming while offering creative /corrective solutions to correct shortcomings before they wreak havoc on the institutional setting. Additional information on preparing and effectively utilizing security assessments can be found in two articles authored by the undersigned[1] and detailed further in a book by the undersigned[2].

Conjoining house surveillance with public surveillance systems

It makes good sense for healthcare security executives to reach out to local government and law enforcement officials to discuss joining the municipality's external surveillance network. Connecting to the community's surveillance network would permit the hospital security's eye in the sky surveillance system to monitor access and capture mischievous activity and/or other non-criminal emergencies at the institution's periphery. Interestingly, for the very first time this past New Year's Eve (2019), the New York City Police Department used both public surveillance and drones to monitor access control in Times Square. Obviously, joining these existing networks would be a win-win for all in the never-ending war on terrorism. There are legal and logistical questions associated with conjoining surveillance technologies, but there could be tremendous benefits derived from thinking beyond the standard way security projects are usually packaged.

Technological enhancement considerations: Turnstiles / magnetometers / arming security operatives / updating use of force policy / employing robotics / drones for patrolling and surveillance / using metrics to showcase proficiencies & substantiate expenditures.

Turnstiles:

The use of turnstiles provides a physical barrier between the entrance and the interior of the hospital. Turnstiles also provide for the screening of all persons entering the hospital. This process includes the authentication of all visitors and the issuance of an "access device" {pass/card} to provide entry into the hospital. The key to the implementation of a turnstile program is the establishment of reasonable security controls that adequately protect people, property, systems, equipment, and other assets while restricting access where appropriate. Designing a program that considers internal traffic flow and its impact on clinical operations is the desired outcome. It is important that appropriate signage be prominently posted, and security operatives be sensitized and briefed on how to keep visitors and staff moving freely without incident. The screening process should be engineered to quickly maneuver traffic through the turnstile check point as effortlessly as possible. The system should be capable of adequately handling seniors and the disabled as well. As a matter of reality, turnstiles and access control cards that require swiping to pass through the turnstile may be difficult to manage for select individuals. One example that immediately comes to mind is a child visiting a patient with a parent, oftentimes a child would not necessarily be issued an access credential; but must be able to pass through a turnstile. This is precisely why human interaction will likely be required to assist those who do not understand or have trouble navigating these barriers. Finally, some thought needs to be given to turn style jumping and illegally allowing

Copyright © 2021 NYCFE www.nycfe.org

several persons to gain access on the same card.

When using turnstiles, it is suggested that anti-pass back programing be applied. An anti-pass back system can be programmed to allow a credential to open a door or turnstile for a determined period so that an access card cannot be used by *two* different people. Once the technological issues are addressed, it's time to tackle traffic flow considerations. To get it right, it's important that a traffic study be initiated to determine 'high and low' traffic periods and wait times. Once completed, the new process should be tested to ensure it will flawlessly function under extremely stressed circumstances and that the normal ebb and flow of the facility is not severely interrupted.

For example, what happens when one or several of the turnstile portals malfunction? How will this downtime effect wait times? Will security staff be available to screen persons when turnstiles are dysfunctional? These and other eventualities; including cost considerations must be considered when selecting access technology for the turnstile. As with most technological enhancements, the higher the level of security one seeks, the costlier the system. Proximity cards are the costliest and they must be included in your cost/benefit analysis. Should a less costly security technology be used, then consideration must focus on installing two or three different types of card readers, and/or designate specific turnstiles for specific users.

Notwithstanding, most hospitals utilize proximity access cards for staff and a less costly barcode or magnetic stripe cards for visitors and vendors. Obviously, budgetary considerations almost always drive the decision. With respect to budgetary deliberations, turnstile costs vary depending on whether the turnstile project is earmarked as a new construction or retrofit undertaking. A great many institutions engineer a system that offers a lane for visitors and patients, and a separate lane for staff, as well as an additional lane for eventual breakdowns. Finally, let us not forget that an entry gate may be need for deliveries and/or disabled access.

Magnetometers / screening procedures

In healthcare today, walk-through, and handheld metal detectors are used primarily in emergency departments and in behavioral health areas. There is now interest in utilizing metal detectors at hospital entrances. Protection wisdom theorizes that metal detectors and scan bag X-ray machines help to lessen the opportunity of illegal weaponry finding its way into healthcare facilities.

Prior to considering walk-through metal detection devices, it would be wise to survey the installation site, audit the detection device placement schematic, and valuate its effect on access-related traffic flow. In the court of protection wisdom, walk-through metal detectors should be placed in areas where there is the ability to restrict access upon activation; especially when a person activates the detector or tries to by-pass the metal detector. Depending on traffic density, more than one detector may be necessary to reduce wait times. It is suggested that security operatives assigned to pilot these detection systems be armed. ***In lieu of arming security staff, many hospitals opt to install a physical barrier to obstruct entry at these strategic check points.*** With respect to screening procedures, all persons entering the hospital should be scanned. The scanning process should allow for hand-held scanners so that all medical emergencies can be immediately adjudicated. When metal detectors are used, all entrances into the hospital should be secured and monitored to make sure persons wishing to enter the hospital cannot by-pass the detection system. Finally, when metal detectors are used at emergency department entrances, a procedure must be enacted to handle individuals who arrive by ambulance; but are not seeking medical treatment. It is important to note that metal detectors are not effective if handbags, backpacks, and other carried items are not screened. These items should be sent through an x-ray machine or be physical inspected by a security operative. When inspecting bags, a table must be made available for inspection purposes. Initial inspections should *not* include a detailed review of a person's bags, but simply a quick look-see for weaponry. Security officers assigned can use a handheld scanner before conducting the full-blown inspection to determine if any metal objects are present. To effectively perform full-blown searches, a private screening room needs to be erected to effectively handle these searches. A process needs to be drafted speaking to what to do when a weapon is found? How will weaponry be safeguarded? How will legal weaponry be returned? Finally, a screening procedure is needed to handle special cases such as infants and small children walking through detectors or arriving in a stroller and wheelchair and/or physically impaired access.

Moving from patient and staff access to vendor, delivery and law enforcement admittance. Procedures need to be drafted speaking to how bags or packages are to be searched? What will the process be for emergency personnel responding to an emergent situation? Will emergency responders be allowed to bypass the security checkpoint without going through the metal detection? What will the process look like for on and off duty law enforcement personnel carrying firearms and other weapons? Finally, the trillion-dollar question,

Copyright © 2021 NYCFE www.nycfe.org

what is the policy re persons that refuse to go through the metal detector? Will service be refused, or will they be allowed to enter the hospital anyway? Questions abound!

Arming hospital security operatives

The decision to arm security personnel should not be taken lightly. This decision can have a major impact on the healthcare institution and its constituency.

Arming security staff is an administrative decision that each institution needs to carefully ponder. Before arriving at a decision, hospital administrators need to decide the purpose for arming security staff. Irrespective of the reason, the process must begin and end with getting legal advice and researching state and local ordinances, along with conducting a comprehensive risk assessment to validate the need for and impact of arming security personnel. Because of the high liability associated with arming staff, alternate approaches to having firearms on hospital property should also be pondered.

Possible alternatives might include having an off-duty police officer assigned to the healthcare institution, hiring armed contracted private security, and only arming senior security management personnel.

If arming security is the road to be traveled, then selecting weapons of choice need to be considered. When selecting a weapon of choice, there are questions galore. The type of revolver (single shot or semi-automatic) to be purchased? If the revolver selected is a semi-automatic type of firearm than how large of a clip will be allowed? What type of bullet will be used? How much ammunition will be kept on site? Will each qualifying officer purchase and carry their own weapon, or will weapons be issued to each officer during shift changes? Will the Hospital purchase the weapons or ask the officer to purchase the weapon out of their own money? What will the ammunition carry policy entail? In the court of security management opinion, a good strategy to follow is to have the institution purchase all firearms and set the policy and standards. With respect to safeguarding firearms, it is important that the institution provide an isolated and secure location for firearm storage. The room should provide a high level of security and have an ammunition cleaning area. The firearms storage room should have only one entrance and be equipped with a card reader and CCTV camera surveillance system. Access into the room should be restricted to *only qualified armed staff* who have a firearm issued to them.

A firearms instructor / supervisor position should be developed to keep track of all firearms, ammunition distribution, and collection. The supervisor should be an individual who has passed the certification program and who possibly has prior law enforcement experience. A firearms supervisor should be assigned to each shift and/or just work alternate shifts on a regular basis. If one firearms supervisor is selected, then a backup supervisor should be considered as well.

Use of force policy

Obviously if firearm use is added to the healthcare protection envelope, it's imperative that suitable use of force guidelines is enacted. Questions to be considered include:

- state and municipal law requirements
- type and amount of force to be used
- whether aerosols or tasers will be allowed
- training curriculum requirements
- firearm type, distribution, storage, ammunition type, training requirements, instructor availability

The role of robotics and drones

In a 2016 book by Robert J. Gordon a professor in social sciences at Northwestern University[3], speaks of the possible use of robots in a wide variety of applications outside of manufacturing, and warehousing sectors including supermarkets, doctor and dentist offices and hospitals. According to 11/14/2019 article in *The Verge*: by James Vincent - *Security robots are mobile surveillance devices, not human replacements*[4] states that security robots are slowly becoming a more common sight in malls, and public spaces.

Moreover, the author goes on to mention that these *friendly* robots are collecting far more data than humans could! Obviously, robotics is becoming a bigger and bigger part of the protection landscape and most likely will play a much broader role in the years to come. It would be wise for security executives to put this new up and coming protection strategy on their radar screens. In addition to using robotics, security executives need to network with local law enforcement agencies about remote drone surveillance usages.

According to an article by Curt Fleming *Remote drone dispatch: law enforcement's future*[5] https//www.policechiefmagazine.org/remote-drone-dispatch/, 347 law enforcement agencies in 43 U.S. states are using unmanned aerial vehicle technology (drones) to assist in a wide variety of protection-related applications including search and rescue, traffic control, surveillance crowd monitoring, and active shooter investigations. Ongoing synergism is especially important herein because hospitals play an extremely active role in terrorism-related occurrences helping to treat the injured both during and after catastrophic occurrences.

Cost / benefit considerations

As with all security enhancement endeavors, cost is always a major

Copyright © 2021 NYCFE www.nycfe.org

factor. Once the security scope of work is completed, it is time to consider preparing a cost-benefit study to compare intervention value vs. enhancement costs. This analysis should consider both direct and indirect costs and benefits. Direct costs often include financial and operational costs associated with implementing proposed programmatic initiatives, and the indirect costs often involve productivity, business disruption, management-related diversion, loss of reputation and/or brand value costs.

Once the assessment is concluded, it's time for a rigorous benefit analysis. One of the most effective methods of analyzing the degree of crime-risk exposure is to sub-divide risk exposures into "low" – "medium" and "high" risk categories. It is through this analytic process that the amplitude of various risk exposures is valuated. The International Association for Healthcare Security and Safety (IAHSS) has published a set of basic guidelines you should follow. Included in these guidelines is an outline for the development and implementation of a healthcare risk assessment.

The IAHSS guidelines state: "Security Risk Assessments will be conducted on a regular and on-going basis. The objective of the Security Risk Assessment is to identify assets of the Healthcare Facilities (HCFs) primary mission and operations, threats to and vulnerabilities of those assets, and develop reasonable risk mitigation strategies to protect the assets. Moreover, the Association offers the following advice: "Establish reasonable and responsible security controls and processes that protect people, property, systems, equipment and other assets while restricting access where appropriate!

Applying metrics to validate expenditures

Metrics is a management tool for measuring performance. Using metrics is an effective method of demonstrating security-related programmatic effectiveness and expenditure justification. The authors have written a trilogy of articles[6] and a book[2] highlighting several metric applications. Utilizing metrics helps the security executive speak the language that CFOs (bean-counters) understand. Moreover, using metrics is an extremely beneficial strategy to employ when seeking additional security enhancement dollars and/or to justify programmatic expenditures.

Conclusion

One lesson to be learned from today's healthcare challenges: *"if one is afraid to take chances – one can never get answers"*. Seeing that the security-camera is watching, it is always a good thing to be the *'first to tomorrow'* and begin embracing and experimenting with new security fixes. The techniques and technologies mentioned herein are only the tip of the iceberg; but may be a good fit for your organization. Finding the right suit of armor to snugly fit your institution's wardrobe is not always an easy task, but a wise security administrator has many advisors, both internal and external, to help him or her find the right suit of protection attire for their institution's wardrobe!

Biography

Anthony Luizzo, Ph.D., CFE, CST, PI is a retired NYPD detective, and the former corporate director of security for the New York City Health and Hospital Corporation, the largest public healthcare system in the United States. He is a past president of the Society of Professional Investigators, former eastern region governor: Association of Certified Fraud Examiners and a founding member and president-emeritus of the New York Chapter: Association of Certified Fraud Examiners. He is a former editorial advisory board member: Reuters WG&L/RIA Group - Thomson Publications. Dr. Luizzo is a member of IAHSS and a frequent contributor to the *Journal of Healthcare Protection Management.*

Bernard J. Scaglione, CPP, CHPA, CHSP is the Senior Consultant directing healthcare security services at DVS Security Solutions. He has served in several capacities for the International Association for Healthcare Security and Safety (IAHSS) including 4 years as a board member and 10 years serving on several councils and committees. Ben is past Chairman of the ASIS International Healthcare Council and the Past President of the New York City Metropolitan Healthcare Safety and Security Directors Association.

References

1. Luizzo, A. (2018) March/April). The security survey: an investigative tool. *PI Magazine, issue 156, 28-30.*
   Luizzo, A. (2018) March/April). The security survey: an investigative tool – part II. *PI Magazine issue, 159, 22-25.*
2. Scaglione, B. (2019) Security management for healthcare: proactive event prevention and effective resolution. *N.Y. Rutledge, Taylor & Francis Group. Publications*
3. Robert Gordon. (2016) Rise and fall of American growth: U.S. Standard of Living Since the Civil War: *The Princeton University Press*
4. Vincent J. (2019) Security robots are mobile surveillance devices, not human replacements. *The Verge - https://www..theverge.com/2019/11/14/20964584/knightscope-security-robot-guards-surveillance-devices-facial-recognition-numberplate-mobile-phone*
5. Fleming, C. (2019) Remote drone dispatch: law enforcements future? *IACP Police Chief Magazine – https//www.policechiefmagazine.org/remote-drone-dispatch/.*
6. Luizzo, A. & Scaglione B. (2015) An alternative view in the development of security metrics. *Journal of Healthcare Protection Management. 31, 98-104.*
   Luizzo, A. & Scaglione B. (2016) Resources available for applying metrics in security and

Copyright © 2021 NYCFE www.nycfe.org

safety programming. *Journal of Healthcare Protection Management. 32, 27-33.*
Luizzo, A. & Scaglione B. (2017) Applying metrics to 21st century healthcare security. *Journal of Healthcare Protection Management. 33, 7-13.*

Suggested readings:

Luizzo, A. & Scaglione B. (2007) Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management 23, 1-9.*
Luizzo, A. & Scaglione B. (2017) Aspects of crime and violence avoidance. *Journal of Healthcare Protection Management 33, 21-30.*
Luizzo, A. & Scaglione B. (2019) Training security officers to recognize the perils of weapons of mass exposure contaminates – part II. *Journal of Healthcare Protection Management 35, 32-39.* ♦

Reprinted courtesy of the Journal of Healthcare Protection Management: (Vol. 37. No 1. - pp. 1-10 – 2021)



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

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

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

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

With Special Thanks to Bruce Hulme and Ozan Gurel

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

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

Things gained through unjust fraud are never secure.
Sophocles

Copyright © 2021 NYCFE www.nycfe.org