

FRAUDULENT TRAVEL  
PLEASURE P. 8

MR. OH'S  
EMBEZZLEMENT P. 14

FRAUD TRIANGLE  
ON TRIAL P. 18

FRAUD ZONE  
DEFENSE P. 24

REGENTS' CHALLENGE  
OF THE CHASE P. 38

HEROES UNITED  
P. 48

# FRAUD

A PUBLICATION OF THE ASSO

MAGAZINE®

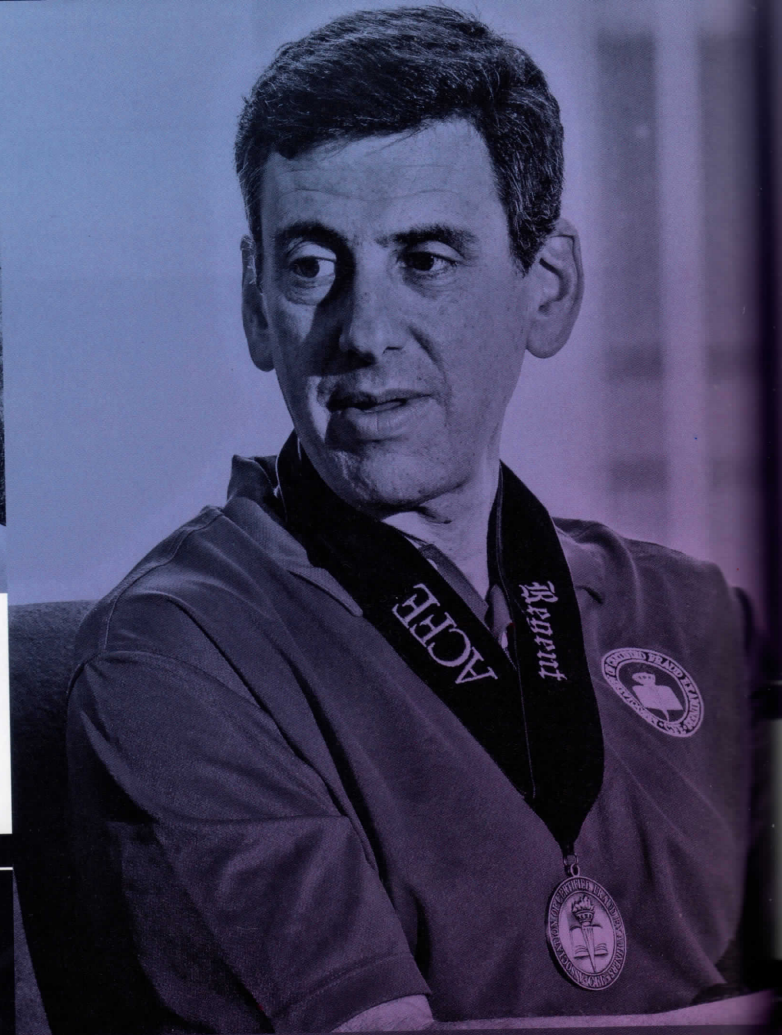
VOL. 32 | NO. 5 | SEPTEMBER/OCTOBER 2017  
[Fraud-Magazine.com](http://Fraud-Magazine.com)

## POLICING

IN HIS NEW AUTOBIOGRAPHY, ACFE PRESIDENT JAMES D. RATLEY, CFE,  
DESCRIBES HIS AUDACIOUS LIFE AND CAREER AS HE TRAVELS  
FROM BEAT COP TO GLOBAL ANTI-FRAUD LEADER P. 30

## FRAUD









## ACFE BOARD OF REGENTS OFFER BENEFICIAL ADVICE

The ACFE Board of Regents ponder the exciting, frustrating and exquisite challenges of the fraud examination profession during the 28<sup>th</sup> Annual ACFE Global Fraud Conference.

By Dick Carozza, CFE, with Emily Primeaux, CFE

# THE CHALLENGE

OF THE

*CHASE*



**Y**ou already know this: **Fraud examinations can be both basic and complex.** They're basic because you can devise them by consulting a seminal body of knowledge such as the ACFE's *Fraud Examiners Manual*. But they can also be excruciatingly complex because fraudsters can create such messy situations that you must depend on the wisdom of other fraud examiners to guide you through frustrating labyrinths.

On Sunday, June 18, at the beginning of the 28<sup>th</sup> *Annual ACFE Global Fraud Conference*, in Nashville, Tennessee, *Fraud Magazine* invited the members of the ACFE Board of Regents to provide advice to members. As Regent Chair Leah D. Lane, CFE, said at the end of the interview, the great motivation for many fraud examiners is **"the challenge of the chase."**

## THE PARTICIPANTS



**LEAH D. LANE, CFE,  
CHAIR**

LANE IS THE DIRECTOR OF GLOBAL INVESTIGATIONS FOR TEXAS INSTRUMENTS, AT WHICH SHE MANAGES A GROUP OF INVESTIGATORS IN THE U.S. AND ASIA WITH GLOBAL RESPONSIBILITY.



**SIDNEY P. BLUM, CFE,  
CPA, CFF, VICE CHAIR**

BLUM, AN INTELLECTUAL PROPERTY AND FRAUD EXPERT WITH MORE THAN 30 YEARS OF EXPERIENCE, HAS TESTIFIED AS AN EXPERT WITNESS DOZENS OF TIMES, HAS WRITTEN TWO BOOKS FOR LAWYERS ON IP AND HAD BEEN AN INTERNAL AUDITOR FOR SEVERAL FORTUNE 50 COMPANIES.



**ALEXIS C. BELL, M.S.,  
CFE, PI, TREASURER**

BELL IS THE CEO AND FOUNDER OF FRAUD DOCTOR LLC, WHICH PROVIDES PROPRIETARY ANTI-FRAUD PRODUCTS AND SERVICES. SHE'S THE AUTHOR OF TWO BOOKS, "DATA ANALYSIS FOR CORPORATE FRAUD RISK" AND "MORTGAGE FRAUD & THE ILLEGAL PROPERTY FLIPPING SCHEME."



**VIDYA RAJARAO,  
CFE, CA, ASSISTANT  
TREASURER**

RAJARAO IS A PARTNER AT GRANT THORNTON INDIA. SHE'S A NATIONAL LEADER FOR FORENSIC AND INVESTIGATION SERVICES IN INDIA AND THE SUB-CONTINENT AND A MEMBER OF THE FIRM'S GLOBAL FORENSIC STEERING COMMITTEE.



**NANCY E. RICH, CFE,  
MPA, SECRETARY**

RICH IS A SUPERVISORY SPECIAL AGENT WITH THE U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE IN NORFOLK, VIRGINIA.



**FM:** Are there some areas in which you believe fraud examiners are not keeping current regardless of what field they're in?

**LANE:** Fraud examiners need to be aware of technology and how it's used and how it's changing. And they need to be aware of local laws around the globe: What can I legally gain access to during our examinations? It's very easy to get behind if you're not paying attention.

**BLUM:** Historically, many frauds have been complex, but now with the high pace of changing technology, new frauds are vastly more complex requiring a response team of subject-matter specialists. When I started fraud examinations three decades ago, we generally could follow domestic paper trails, and common sense took us to our resolutions. You could learn on the fly. Now you really must know how to put the right team together because there's so much expertise that's required in the new complexities of computer-based and international fraud. For example, we need to know about different databases, search tools and forensic software. Fraud examiners need to be aware of their limitations and also need to know how to reach out to the fraud community and through the ACFE to find those who have particular expertise to make sure the work they perform is within their scope and skills.

**RICH:** We put together teams all the time because investigations are so highly specialized now. One person or agency will be in charge of data search, while another will handle the analytics together. All team members usually participate in the interviewing of targets and witnesses. Once you put that whole functional team together cases run a lot smoother.

“  
A LOT OF FRAUD  
EXAMINATION  
BY ITS NATURE  
IS REACTIONARY.  
FRAUDS OC-  
CUR AND WE'RE  
ALWAYS CHAS-  
ING THEM DOWN.  
WE'RE FOCUSED  
ON DETECTION  
AND REACTION,  
BUT WE SHOULD  
ALSO HAVE GOOD  
KNOWLEDGE ON  
PREVENTION — TO  
KEEP IT FROM  
HAPPENING IN  
THE FIRST PLACE.  
WE'RE SPENDING  
SO MUCH TIME  
CHASING THE LAST  
CRIME WE'RE NOT  
SPENDING ENOUGH  
TIME ON THE PRE-  
VENTION SIDE.  
”

**FM:** So, humility is a good character trait if you're a fraud examiner.

**RICH:** Everyone on the team needs to recognize their strengths and weaknesses. I deal with several different federal agencies such as the Defense Criminal Investigative Service and the FBI. The agencies all bring different skill sets and resources, which makes the investigation run smoother. Without those organizations we would not be able to do what we do.

**FM:** How have cyberfraud — and the issues and the educational requirements surrounding it — affected your practice? How do you think it will affect future fraud examiners?

**BELL:** In North Carolina, if you conduct digital forensics or any type of cyber investigation you're required to have a private investigator [P.I.] license. Each person in our company's digital forensics lab has to have a P.I. license and an additional electronic countermeasures designation before they can be part of the lab.

We used to spend a lot of time examining desktops and laptops for digital forensics. But now it's shifting to small devices, such as smart phones and PDAs — those are really the treasure troves of data.

**BLUM:** We're seeing an explosion of cyberfraud that is a challenge to keep up with. You're asking about what the future holds? Right now, we can't tell you other than the technology increases quickly, so by the time we catch up to it the cybercrooks are on to the next level looking to exploit system weaknesses. The challenge is how do we share fraud combating technology without showing our hand to the fraudsters and also implement fraud protection to the billions who have access to the internet. Right now, I don't see how that's possible.



**RAJARAO:** Fraud examiners need to take back control. Control the messaging of how cybercriminals are investigated. Nobody really knows what's happening. Technologists are giving advice, but they don't understand behavioral aspects of fraud, and they don't know how to investigate it. They're just peddling tools. We're always playing catch-up.

**FM:** So, what do fraud examiners do then?

**RAJARAO:** We have a roadblock. We're not technologically savvy. Members of the audit committee of the board must deal with cybercrime. We get presentations by technology evangelists who really can't explain why cybercrime is happening. How does a business protect itself? To reclaim the leadership we must redefine the message because this is a business problem.

We're never going backwards in our use of technology. Businesses use the internet for sales or supply or distribution. We risk misusing information or stealing of confidential data plus malware insertions that create havoc with our data. So, I think we should reframe it as more of a business question.

And then we answer the next set of questions: What's motivating someone to do it? Is it an insider? A vendor? An outsider? Is it a combination of these parties? All questions that fraud examiners can answer because that's what we do. But what we have are technologists who try to do fraud examiners' jobs without having the fraud examination techniques.

**BLUM:** I think we as fraud examiners need to redefine our roles. A lot of fraud examination by its nature is reactionary. Frauds occur, and we're chasing them down. We're focused on detection and reaction, but we should also have good

knowledge on prevention — to keep it from happening in the first place. We're spending so much time chasing the last crime we're not spending enough time on prevention.

**LANE:** In my company, when we have a fraud examination we do a root-cause analysis so we discover the vulnerability that allowed that fraud to occur and the business devises new controls to try to lessen the risk of that vulnerability.

One of the reasons we have more and more fraud is that fraudsters are coming up with new ways to get around those controls. As we get smarter and identify those vulnerabilities, other ones pop up. That's the nature of what we do. There's always going to be a way to get around the controls. Internally, somebody in the company has the keys to the kingdom.

**FM:** So, when you do an analysis do you find patterns?

**LANE:** Do we go back and see if that fraud has happened again?

**FM:** Yes.

**LANE:** Sometimes we do, sometimes we don't. It depends on each case.

**FM:** What do you do at that point?

**LANE:** Investigate each fraud that is raised to us. So, if we identify more we're going to investigate those as well. But we concentrate on the root causes, and the business is going to own the fix for that vulnerability. My team as an investigative unit is tasked with not only investigating the fraud but determining what allowed that fraud to occur. But then we give that vulnerability — that reason — to the business.

**RICH:** The Navy has an active policy for debarring vendors that are caught defrauding. People might go to jail, and companies pay huge fines. But when you can't do business with the government anymore that sends a strong message. Debarment of companies who then can no longer bid on government contracts is a huge fraud deterrent.

**FM:** Is that permanent banishment?

**RICH:** It depends on how severe the offense was. The Naval Administrative Integrity Office can debar individuals, and they can debar companies for several months or years. The burden of proof is only administrative. After due process, the Navy can decide to debar a company for a variety of reasons, including fraudulent activity. The burden is on the company or individual to say how they're going to fix the problems and become a responsible contractor.

[See the U.S. Department of Labor's Office of Federal Contract Compliance Programs' *debarred companies' list*, [tinyurl.com/yb94gp60](http://tinyurl.com/yb94gp60) plus "Reducing Vendor Fraud Risk: Using the Excluded Parties List System," by Martha Howe, Ph.D., CFE; Priscilla Burnaby, Ph.D., CPA; Brigitte Muehlmann, Ph.D., CPA/CFE, CMA, CFM, CVA, [tinyurl.com/yavwkhhx](http://tinyurl.com/yavwkhhx).]

**RAJARAO:** The World Bank, the International Monetary Fund and the Asian Development Bank all debar companies and publish those lists.

**RICH:** But there's not a central place to look for the debarred companies. In the states, if the Navy wants to contract with a certain company it must first check the list of debarred contractors prior to awarding a contract. However, overseas there is no central list for companies debarred from India or Australia, for example. So, the



“

YOU CAN HAVE A U.S. CORPORATION WITH A SUBSIDIARY IN EUROPE WITH AN AGENT IN SOUTH AFRICA BRIBING SOMEONE IN MALAYSIA WITH A LARGE CONTRACT OFF THE SOUTH CHINA SEA. HOW ARE YOU GOING TO INVESTIGATE THAT WHEN YOU NEED ALL THESE COUNTRIES TO COOPERATE?



”

Australians might debar a company for fraudulent activity, but it doesn't merge the list on which they place that company with the list of debarred companies in the United States.

**RAJARAO:** Right, if a company bids for a World Bank contract, even if they're in India, and the World Bank has debarred them then it's on the World Bank list.

**FM:** But there's no merged list.

**Shouldn't there a worldwide database like a Watson or a good Big Brother for fraud in which we learn from our mistakes and could include root causes?**

**BELL:** Part of the challenge comes from determining who's going to oversee that and the criteria for getting on the list, how to verify the inputs and the levels of grievance.

**RICH:** Implementation might be difficult.

**BLUM:** Just so you know, even if you establish that master merged list of evildoers, there will be many ways around it. How many companies have subsidiaries and divisions that don't communicate? We're not dealing with normal business people. We're dealing with fraudsters — people who have committed a crime. Once they're on that list they'll just shut down the company and use a new name to continue their fraud.

**FM:** Yes, they'll morph into something else. But the point is that some type of database can record that too. How can we move in that direction?

**BLUM:** That's where the fraud examiner needs to be engaged. Say if you're in a corporation, you reach out to the procurement department to talk about their background checks to make certain they're looking for the right things to find fraud and fraud indicators. For example, are the owners and not just companies listed for

“do not engage in business”? As fraud examiners, we have a lot of knowledge, and we need to proactively reach out to other departments to provide advice.

**RICH:** Our fraud office is proactively starting to data mine to search for various fraud indicators. We have active hotlines for people to report frauds and other crimes. We also get several referrals from other federal agencies.

**RAJARAO:** There are two ways to move in the direction of global fraud databases. Governmental regulators around the world — the U.S., Europe, the U.K., Australia, some in Brazil, India, China — are talking amongst themselves because they realize there is money to be made. They're going after the kleptocrats and their ill-gotten gains. It no longer makes sense for governments to do this individually because they won't have access. You can have a U.S. corporation with a subsidiary in Europe with an agent in South Africa



bribing someone in Malaysia with a large contract off the South China Sea. How are you going to investigate that when you need all these countries to cooperate?

A second way is what technology companies are doing. They're not beholden to the old methods of investigation. Say you have a technology company, and it already has a globalized workforce. It really doesn't have borders. Physically they share information much more commonly. If the industry suffers — say if someone leaves and takes intellectual property and goes to a competitor — tech companies will collaborate with each to catch the fraudster. They might compete in the marketplace, but they cooperate in combating intellectual property thefts and cybercrime, including data breaches. No one has the right answer so you need that brain trust of multiple companies to come up with the solution that individually no one can think of because individually you would just have roadblocks.

**BELL:** I think it depends on the sector. I observed in the microfinance sector, as an example, where they were starting to get together to do something like that. They had a centralized database that they used collectively. What we found in practice was that because they were in competition with each other many were routinely inputting false information into the database, which meant that it became meaningless and people stopped using it. So, I suggested they appoint a third party — somebody who has incentive to maintain accurate records — to administer the database. They establish the criteria and vet the inputs.

**RAJARAO:** Here's another example of sharing fraud-related information in technology companies in India. Employees can misrepresent their credentials.

“THIEVES STEAL YOUR MONEY, BUT LIARS STEAL YOUR TIME. IT JUST ECHOED IN MY MIND THAT FOR MY ENTIRE LIFE GROWING UP IT WAS ENGRAINED INSIDE OF US, ‘LIARS AND THIEVES.’ SO, I LOOKED AT MY DAD WITH AN EPIPHANY, AND SAID, ‘IN THIS MOMENT, I THINK I JUST REALIZED, THIS IS WHY I DO WHAT I DO.’”

Companies would often just terminate an employee for that. They know they lied on their resume, so they just agreed to a mutual separation. But guess what? The employee is just going to go to another technology company and do the same thing. The second time, they got away. The third time the companies got together and said enough is enough. The fraudsters are just gaming the entire system. But now the technology industry has a skills database, so if that person has been terminated for lying on their CV they'll never get employed by the industry again if the potential employer checks their information on the National Skills Registry [[nationalskillsregistry.com](http://nationalskillsregistry.com)].

**RICH:** We see that cooperation in Virginia with the private sector, too. I am a part of the Virginia Beach Banking Association,

which actively teams with local, state and federal law enforcement agencies to discuss certain banking issues. This is a great partnership with the private sector. This association has made our job so much easier because we now have someone at the banks we can go to ask questions, and they also pass on any fraud alerts and trends they are seeing too. Cooperation is also vital when you're working in an overseas environment. You need to have the expertise from the local foreign governments you are working with. You also need to have a good working relationship with the prosecutors who will prosecute the case.

**FM:** One thing we don't like to talk about are the things that didn't go right. But we learn from those mistakes more than we learn from our



**successes. So, would you be willing to share some of the steps you made in the last year or past years that have really helped you in a particular case of how a fraud was working?**

**RAJARAO:** I think not understanding the scope of the problem is the biggest one. Initially you just have tunnel vision. You think it's a small problem. You don't realize it's the tip of the iceberg. And what you're attacking is just the tip.

**FM:** So, have you learned that there are no small problems? That you must assume this is the tip of the iceberg?

**RAJARAO:** The challenge, as a practitioner, is I must assume this is not the tip of the iceberg, but then when you talk to

clients they don't want to hear that the problem is an iceberg. They want to contain it, and they believe that it's just the tip. They want to believe it's isolated: one rogue employee, one division, that it's not a companywide problem. So, you need to balance the two. When you're doing your work you still need be mindful that even though your current mandate is to evaluate the tip of the iceberg you'd be remiss in not telling your client once you have finished there is a larger problem behind the small issue, even though the client doesn't want to hear that message.

**FM:** Can you think of an instance when you didn't do that?

**RAJARAO:** Yes, I can think of instances where I've not done that. Either because the client doesn't want to listen or to Sid's

point, you're just chasing the next fraud case. You've got five other cases, your teams are strained, so you just don't explain the bigger picture. Five months later, you realize the small fraud is emblematic of a larger organizational issue either because of lack of controls, lack of training or they've done an acquisition and haven't devoted time to transitioning everybody into one level of corporate governance. So, there's only so much you can handle, and you're always chasing.

**RICH:** When someone makes an initial complaint to us, they usually have several issues they want us to deal with; some may not be related to fraud. One problem I see constantly is on big fraud cases, it takes time to isolate the exact fraud. Our first priority is to see if there are any criminal violations and work from there. So, we

## Law Enforcement and Government **ANTI-FRAUD SUMMIT**

**October 30, 2017 | Washington, D.C.**

Join industry experts and anti-fraud professionals as the ACFE Law Enforcement and Government Anti-Fraud Summit returns to Washington, D.C. on October 30, 2017. Hosted by the ACFE Law Enforcement and Government Alliance, this event delivers insights, techniques and tools to combat current anti-fraud threats to your agency. Plus, you'll have the opportunity to connect with peers and earn CPE credit.

Register by  
Sept. 29 to  
**Save  
\$95!**

Last year's event sold out. Register early  
to secure your spot — plus save \$95!  
**ACFE.com/FraudSummit**

 **ACFE**  
Association of Certified Fraud Examiners



hosted by the ACFE

**LAW ENFORCEMENT  
AND GOVERNMENT  
ALLIANCE**



need to investigate a case enough to secure that criminal conviction.

**LANE:** Then it's policy violations versus criminal violations.

**RICH:** We just need to keep the investigation focused so we can obtain that prosecution and then move on to the next crime.

**FM:** So, let's say you're faced with a big fraud and a smaller fraud. You might be able to get more evidence from the smaller fraud, but there's a smaller dollar return as compared to the big fraud. However, if you find evidence on the bigger fraud you'll be able to prevent tremendous amounts of money loss even though it might take three times as much time to do.

**RICH:** It's a business decision.

**FM:** But is it your decision or management's?

**RICH:** The prosecutors we work with drive the decisions on which cases will be addressed. Our goal is to help return as much money as we can to the U.S. government and prosecute the companies or individuals who have committed fraud.

**FM:** So, you don't try to prove the whole fraud?

**RICH:** We obtain all the information necessary to obtain the prosecution since we have limited resources.

**FM:** Have there been times when you have done that and you thought, "I spent too much time on it?"

**RICH:** Oh yes!

**FM:** And you didn't get the conviction?

**RICH:** We ended up getting the conviction, but we had to refocus our efforts. Once you understand the scheme, you can focus your investigation to get enough information for the prosecution.

**LANE:** And we say the other fraudsters that you can't prosecute are outliers but their behavior is not going to change. We will get them next time.

**RICH:** We just had a person prosecuted who was previously under investigation but had never been prosecuted by another federal organization. Instead of the fraudster learning his lesson, he started the same scheme again, and we finally prosecuted him.

**FM:** How do you keep from being frustrated knowing that there's a case you can't tackle right now?

**LANE:** It is quite frustrating. From an internal-investigation standpoint, we are factually based. Facts are facts, and that's all we can go on. All the evidence we've found right now does not substantiate the fraud.

**RICH:** And you must get over that. You can't take it personally.

**FM:** What motivates you to keep doing your job? What kind of encouragement do you need?

**BELL:** I'll tell you a quick story. I used to get that question and I would answer, "Integrity is a daily part of the process of what we do, and that's really important to me." I think that's why I gravitated from traditional accounting to the CFE and forensic

accounting side. Last week, I was spending some time with my dad and he was telling somebody that the two groups of people he doesn't have time for are liars and thieves. Thieves steal your money, but liars steal your time. It just echoed in my mind that for my entire life growing up it was ingrained inside of us, "liars and thieves." So, I looked at my dad with an epiphany, and said, "In this moment, I think I just realized, this is why I do what I do." I don't think I truly understood that until a few days ago, and today is Father's Day. Shout out for dad! So, I invite everybody to ask yourself why are you a fraud examiner? What is your "why"?

**RICH:** Now that I'm in a supervisory role, it's a chance for me to impart what I've learned from my mistakes. And our office has been super productive this year with several prosecutions and millions of dollars in recoveries. The people I work with see their hard work paying off and then become excited for the next case. And I'm invigorated to pass on all the information I've learned from my years working in the field.

**LANE:** For me, it's seeing the value added to the business: stopping the fraud, prosecutions, recoveries — when you see what you do is actually helping people.

**RAJARAO:** Everybody, obviously, will say, "I stand for integrity." But it's easier said than done. Let's say you have a sales manager who's really high performing, gets the business, customers like them, employees like them. But then they skim on expense reports. What do you do? Do you terminate them? Do you counsel them? Do you give them a letter of warning? Do you condone it as an obvious lapse in judgment? If you keep the employee and counsel them, what kind of message



does that send to others who are playing by the rules? What motivates me is helping the clients come up with a solution. I don't have all the answers. And as fraud examiners I don't think we need to have all the answers. But at least helping them figure out the conversation. Figuring out the larger picture.

**FM: What have you done to mentor young fraud examiners?**

**BLUM:** Thanks to the ACFE, I've been receiving daily emails where members ask questions through the community forums [Connect.ACFE.com]. I'm an active participant. I post probably biweekly in response to the questions. The most recent question was from a CPA concerned about a potential conflict performing a fraud examination for a company that was also a client for compilation reports. I said I would advise against it as an expert witness. I would encourage all senior CFEs to participate on the forums.

**RICH:** My daughter is here as a student representative. She previously attended the ACFE conference in Las Vegas. When she starts college in the fall at Christopher Newport University in Virginia, she wants to start her own ACFE student chapter. I have taken her to several court hearings on fraud-related matters. She now is very intrigued and wants to become a fraud examiner. She also had the opportunity to spend time with Leah, Alexis and Vidyah to get some great insight on what they do daily. No one knows exactly what a fraud examiner is until you talk with one, and my job is different from the other ladies. When my daughter talked with Alexis [Bell] she realized it wasn't just paperwork; it's exciting work.

**LANE:** It's the challenge of the chase.

## VOTING FOR NEW BOARD OF REGENTS MEMBERS BEGINS NOVEMBER 1

Certified members of the ACFE will begin to vote November 1 online at ACFE.com for their selections for three new members. Voting will close December 31. Candidate bios will appear in the ACFE News department of the November/December issue of *Fraud Magazine*.

The Board of Regents performs several integral functions. Under the current bylaws, the Board of Regents has sole authority over the admission of members including, but not limited to, examination standards.

The board is also responsible for establishing, modifying and enforcing the CFE Code of Professional Ethics, and all other necessary matters to maintain the high standards of the ACFE.

"I encourage ACFE members to vote early for their choices for the new members of the Board of Regents," said ACFE Vice President and Program Director Bruce Dorris, J.D., CFE, CPA. "It's a privilege for members to select those who'll represent them on the board. The board frames the future of the ACFE and, in many ways, the profession."

The ACFE Nomination Committee selected nine applicants to vie for three available positions. The new Regents, who will be installed in February 2018, will each serve two-year terms.

**BELL:** Solving problems is so energizing to me!

**LANE:** Each fraud examination is a challenge to find the truth. As part of me becoming the chair of the Board of Regents my company published a graphic on me as part of its online "My Career Path" series for our employees. Company interns, co-ops, young people in finance and accounting then reached out to me. I talked with eight who came to meet with me. And we talked about who a CFE was, and they asked about their own career paths. I'm passionate about what I do, and when you have those one-on-one talks it gets them excited.

**BELL:** We have an intern program at Fraud Doctor for recent graduates. In addition, I went to Cornell University for undergrad. Any student who expresses an interest in fraud or forensic accounting there is routed to me, and we have a conversation. I'm a mentor for them because when I was attending there wasn't any information at the career center about the anti-fraud field. So, they asked me to be a resource for students. I've been volunteering as a mentor at Cornell since 2004, and I do the same for Utica College in the Financial Crime and Compliance Management Master's Degree program, as well.

**RICH:** Senior CFEs can lend their personal support to student chapters to speak and visit with prospective CFEs to help them focus on what we do. ■ **FM**

**Dick Carozza, CFE**, is editor-in-chief of *Fraud Magazine*. His email address is: [dcarozza@ACFE.com](mailto:dcarozza@ACFE.com)

**Emily Primeaux, CFE**, is associate editor of *Fraud Magazine*. Her email address is: [eprimeaux@ACFE.com](mailto:eprimeaux@ACFE.com).