November 15, 2023 Training

Live In-Person & Also Virtual-Online

ACFE
Association of Certified Fraud Examiners
MARYLAND CHAPTER #21
Maryland's Anti-fraud Resource

MARTIN'S WEST - WEDNESDAY, NOV. 15TH

WHO SHOULD ATTEND?

- **Internal and Independent Auditors and Investigators**
- **Accountants**
- **Educators and Students**
- **Legal Professionals**
- **Certified Fraud Examiners**
- **Anti-Fraud Specialists**
- **Criminal Investigators**
- **Prosecutors**
- **Defense Attorneys**
- **Local, State and Federal Law Enforcement Officers**
- **Compliance Professionals**
- **Regulators**
- **Financial and Risk Professionals**
- **Chief Financial Officers**

CONTINUING PROFESSIONAL EDUCATION

At total of 4 hours of CPE will be granted on a 50-minute hour. **NASBA Sponsor Number 125190**. ACFE Maryland Chapter #21 is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

Delivery Method: Group Live

Prerequisites: Knowledge of Fraud and Fraud Schemes

Advanced Preparation: None

Program Level: Intermediate

NATIONAL REGISTRY OF CPE SPONSORS
www.nasbaregistry.org

Derek Ellington, CFE, ACE, CEDS, PI

Derek Ellington is a nationally recognized Certified Fraud Examiner (CFE), Certified E-Discovery Specialist and a licensed PI with over twenty-five years of IT experience and over 20 years of Digital Forensics experience. He is a court-recognized expert witness and regularly testifies in all manners of courts and jurisdictions including Federal Court. Ellington conducts seminars and CLEs for attorneys, paralegals, CPAs and Fraud Investigators. He is also an instructor for law enforcement Computer Crime First Responders, and a contributor to family law and legal publications on the subject of Digital Forensics.

*ACFE and NASBA-approved Continuing Professional Education (CPE), 4 hours of Specialized Knowledge.

*For those of you who will be **attending in-person**, our speaker will be traveling from Raleigh, NC to Baltimore, and will be presenting live, from **Martins' West**, at the scheduled times, in real-time.

*For those of you who will be **attending virtually**, we will be endeavoring to present a training event as close to a live, in-person experience for you as possible. We want to bring our speaker's enthusiasm and energy to you.

*We have arranged for a professional video company to travel to Baltimore and to broadcast the presentation live, **not** via Zoom, or ON24, etc.; but rather in-person in real-time. You will be able to enjoy the look and feel of the training in its entirety from the comforts of your home or office.

***Mr. Ellington introduced this training at the recent **34th Annual Global Fraud Conference**, held in Seattle, WA. We are pleased to offer this training at a substantially reduced cost. If you are considering attending, please take a look at what we are offering. You won't be disappointed.

NOTE: We do not sell or share your registration or personal information.

We are pleased to offer 4 Hours of ACFE & NASBA-Approved CPE
Attend for only $25 per person (just $6.25 per CPE hour)

INVESTIGATING CYBERCRIME AND DATA BREACHES:

INCIDENT RESPONSE FOR THE FRAUD INVESTIGATOR

There is a problem somewhere; you may not know what it is, but suddenly it is your job to figure it out. Is it fraud, embezzlement, intrusion, hacking, another crime or maybe nothing at all? How do we figure it out? In this session, we will learn what an incident actually is, look at common incident scenarios and explore the steps needed to understand and deal with the situation, whatever it may be. When do you rush in and when do you sit back and give the suspect more rope? What is an incident response team, and do you need one? We will look at real-world cases and the investigative process behind each. Along the way we will learn problem-solving strategies that can be applied to not just professional challenges, but to everyday life as well.

Where to Begin: Incident Assessment and First Steps

First, using real-world cases, we will learn what constitutes an incident. We will also discuss when to go alone and when to assemble a team, as well as how to assess next steps. If it is an active, ongoing incident, do we pull the plug and shut the bad actors out or do we monitor and record? What are the law enforcement or government oversight reporting requirements and when do those kick in? We will use real-world examples to allow you to formulate your own theories as to the possible crimes and motivations and then see how your hunches play out..

Investigating Cybercrime: Collecting and Documenting Evidence

Next, we will get an understanding of evidence collection and documentation. We will brainstorm where critical evidence might be and how to get it. How do collections differ for different types of incidents? What types of data can be collected locally? What will we need to subpoena? We will also go behind the scenes in a digital forensics lab to see how computers, phones, and other evidence items are collected, processed, and reviewed. We will get a better understanding of what it means for evidence to be “deleted” and what can and cannot be recovered. We will then see how this collected evidence helps us to understand what really happened and how it will help us to build our cases against the bad actors..

Protecting Against Future Harm: Remediation and Prevention

Finally, we will look at remediation and prevention. What could have been done to protect against this type of incident? How can prevention efforts and good practices help to keep these incidents from happening again? From IT and human resources to internal accounting and outside auditors, where do the responsibilities for protecting against cybercrime lie?.

You Will Learn How To:

- Identify what constitutes an incident, understand incident response and prepare to put together or work with incident response teams
- Recognize common incident scenarios that a CFE might encounter and learn how to approach them step by step
- Examine real-world case studies to see where and how cases start, how they progress and their ultimate resolutions.
- Navigate incident response and determine internal versus external threats
- Categorize a threat as isolated or persistent
- Discern the differences between economic, intellectual property, and reputational loss versus protected customer data loss
- Determine when to assemble an incident response team, who should be on that team, and what the legal notification requirements may be

Check our website frequently
We will begin accepting registrations in early September

4 Hours of ACFE & NASBA-Approved CPE
Total Cost: $25 (just $6.25 per CPE hour)

TRAINING INFORMATION: Due to the travel requirements of our presenter, we will be strictly adhering to the training agenda. We hope that we have allowed ample time within the training for attending to professional and personal matters. **So as not to miss out on any of the action, please be ready to go when the session is about to resume.**

CERTIFICATE OF CPE ATTENDANCE: For those of you **attending in-person**, several times during the presentation, you will be required to enter a code on your attendance sheet. For those of you **attending virtually**, several times during the presentations, you will be required to acknowledge a prompt which will indicate your participation in that particular presentation. When you have entered the codes or acknowledged the prompts for a particular presentation you will have earned the designated CPE hours.

IMPORTANT CPE INFORMATION: Prior to the date of the training, specific instructions will be sent directly to you so that you understand what you will need to do to earn your CPE and how you will download your CPE Certificate.

EVALUATIONS & FEEDBACK: We are very grateful for your support over the years. You deserve nothing less than world-class presenters which we intend to provide right here in our own backyard. We sincerely hope that you will let us know if there is anything that we can do to make our meetings more enjoyable for you. We ask that you take the time to fill out the evaluation form which will be sent to you electronically, shortly after our meeting.

EVENT POLICIES —CANCELLATIONS & REFUNDS:

- If you have registered and/or paid for an event and you need to cancel, you MUST email **mdchap21@gmail.com** no later than 10 days prior to the event to request a refund and/or to cancel your registration.
- Cancellations within 10 days of the event will not be eligible for a refund, but substitutions will be accepted. Please request substitutions by emailing **mdchap21@gmail.com**
- The Chapter must confirm event registrations with the online video provider prior to the event and any changes after this time period can become a financial cost to the Chapter. The Chapter reserves the right to make the final determination on what percentage charge/refund will be returned for cancellations made after the cutoff. The default condition is that cancellations made after cutoff will be charged at 100% and/or no refunds will be permitted. In the event the Chapter determines that partial charges or refunds will be allowed, they will be made on a case by case basis. In the event an attendee does not show up to the event, the registration cost will be forfeited.

LINKS:

Maryland Chapter #21 of the Association of Certified Fraud Examiners

Martin's West—Baltimore, MD

MARYLAND CHAPTER #21 TRAINING

WEDNESDAY, NOVEMBER 15, 2023

AGENDA - Eastern Time (ET)

7:00 – 8:00 AM	**IN-PERSON (Check-in & Continental Breakfast) or VIRTUAL-ONLINE (Check-in)**
8:00 – 8:10 AM	**WELCOME AND OPENING REMARKS**
8:10 – 9:20 AM	**SESSION - 1 Where to Begin: Incident Assessment and First Steps**
9:20 – 9:35 AM	**BREAK**
9:35 – 10:45 AM	**SESSION – 2 Investigating Cybercrime: Collecting and Documenting Evidence**
10:45 – 11:00 AM	**BREAK**
11:00 – 12 NOON	**SESSION – 3 Protecting Against Future Harm: Remediation and Prevention**
12:10 PM	**TRAINING CONCLUDES**