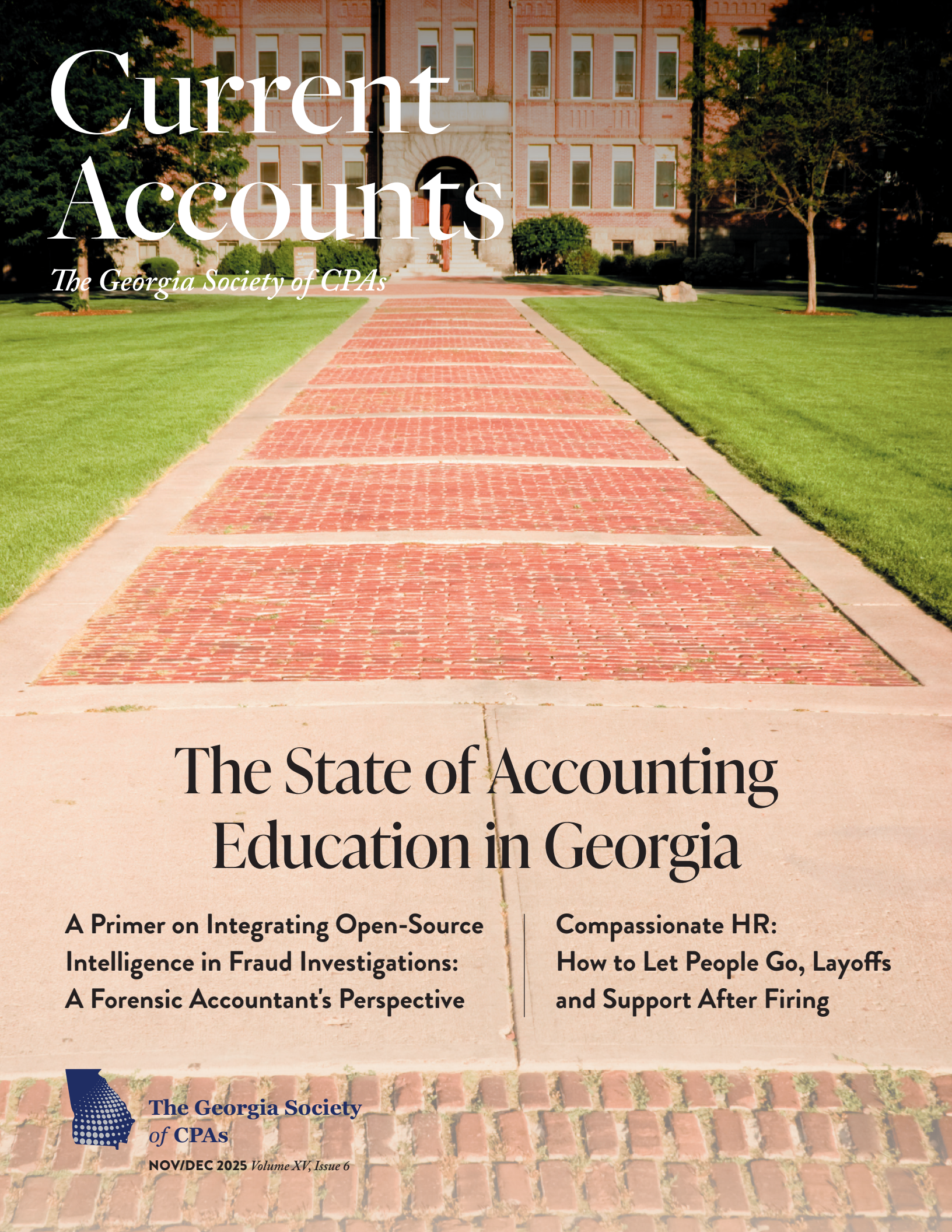


Current Accounts

The Georgia Society of CPAs

The State of Accounting Education in Georgia

A Primer on Integrating Open-Source Intelligence in Fraud Investigations: A Forensic Accountant's Perspective

Compassionate HR: How to Let People Go, Layoffs and Support After Firing

The Georgia Society of CPAs

NOV/DEC 2025 *Volume XV, Issue 6*

A Primer on Integrating Open-Source Intelligence in Fraud Investigations: A Forensic Accountant's Perspective

by **NATALIE LEWIS, CPA/CFF, CFE**

According to the Central Intelligence Agency (CIA), "information does not have to be secret to be valuable." This holds true when a forensic accountant is investigating an alleged fraud scheme. Throughout the investigation, the accountant may obtain information through a variety of sources, including financial records, emails and messages through eDiscovery, statements from key witnesses, and even publicly available information through open-source intelligence.

WHAT IS OPEN-SOURCE INTELLIGENCE?

Open-source intelligence (OSINT) refers to the collection, analysis and interpretation of information obtained from publicly available sources to gain investigative insights. For fraud investigations, OSINT involves gathering data that is legally and openly accessible without subpoenas, search warrants or special access, and using it to uncover evidence of fraud, corroborate financial findings or identify hidden connections.

ADVANTAGES AND DISADVANTAGES OF UTILIZING OSINT IN FRAUD INVESTIGATIONS

For forensic accountants conducting financial investigations, publicly available information can be instrumental in contextualizing financial records, identifying discrepancies, and corroborating or challenging statements made by subjects and/or key witnesses during the investigation. Unlike proprietary databases or subpoenaed records, OSINT relies on materials that anyone can access, legally and without special authority. Investigators can acquire this information without the need for consent from the court or the subject of the investigation.

Since the information comes from sources anyone can legally access, such as government records, company filings, websites, news media and social media, OSINT can often be accessed instantly and for a nominal cost. As long as the information is gathered ethically, it avoids any privacy violations and allows an investigator to discover new points of interest for possible collusions or avenues of the fraud scheme. The information obtained can also aid in conducting interviews to confirm or disprove information.

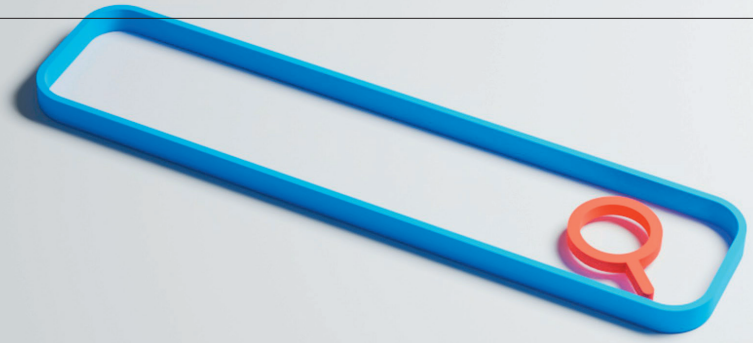
While OSINT is a powerful tool in conducting fraud investigations, it comes with its own limitations and risks. The main concern when using OSINT is its accuracy and reliability, as the information may return false positives, especially when the subject has a common name. Much like the old State Farm commercial, just because something appears on the internet doesn't mean it's true. Information on corporate websites or social media posts may contain outdated, misleading or deliberately false information. Forensic accountants should always verify the information through multiple sources and consider the type of source, such as government websites ending in .gov, which are the most reliable, such as SEC.gov.

Other risks to using OSINT include incomplete or inconsistent data, time and resource intensive, legal and ethical risks, potential bias, and risk of exposing the investigation. Not every jurisdiction provides court and property records online, which can make it more challenging to uncover certain information. With the abundance of data available through multiple sources, the process of collecting the information can be time and resource-intensive, especially as new leads are uncovered. Investigators should maintain proper organization and management to avoid going down the proverbial rabbit hole. As with any investigation, the investigator should be aware of their digital footprint for operational security to avoid exposing their search activities to the suspect.

KEY OSINT SOURCES FOR FORENSIC ACCOUNTANTS

While some helpful information can be found utilizing a simple internet search, some of the most reliable sources of information that aid in an investigation can be found through other sources. Some of those sources include:

- Corporate and Government Filings, such as regulatory filings and business registrations
- Court Records and Legal Proceedings, such as civil complaints, bankruptcy filings, and criminal indictments
- Property and Asset Records, such as property deeds and vehicle registrations
- Media and News Archives, such as press releases about a subject or company
- Social media and Blogs, such as lifestyle evidence (travel, purchases, relationships)
- Online Marketplaces and Classified Ads, such as the resale of stolen assets or evidence of any side businesses
- Geospatial Data, such as satellite images of registered business locations and geotagged photos.



When reviewing these sources, certain acquired information can be especially beneficial to a financial investigation, such as the following:

- Family relationships or affiliations
- Physical assets, including the purchase of real estate, vehicles, aircraft, and boats, and possible liens
- Business records, including Secretary of State filings
- Civil, criminal, and bankruptcy records
- Professional licenses
- Photos and/or video evidence
- Locations
- Profiles and connections.

TECHNIQUES FOR USING OSINT EFFECTIVELY IN AN INVESTIGATION

Using open-source intelligence effectively in a fraud investigation requires more than just collecting information. The forensic accountant should apply structured techniques to uncover relevant, reliable, and actionable insights to incorporate into the investigation. Cross-referencing information is a primary technique for using OSINT in an investigation. For example, during the course of the investigation, a particular vendor name may be of interest and needs to be examined for a possible link to the suspected employee. Cross-check corporate registries, LinkedIn, and other sources like Chamber of Commerce listings and domain registrations to confirm ownership. Through the aid of OSINT, a forensic accountant can construct a timeline of key events (evidence of misappropriated funds, travel, purchases, acquisition of assets, and statements in emails or messages) with findings from financial records. OSINT can also shed light on possible collusion or relationships by mapping the subject's network and connections with individuals and companies. Forensic accountants can then use the acquired information to effectively prepare for key witness interviews.

BEST PRACTICES FOR FORENSIC ACCOUNTANTS

Since many investigations advance through court proceedings and/or insurance claims process, one should follow best practices to ensure the information is reliable, admissible, and ethically obtained. As a forensic accountant, you should start by defining the objective of the search to clearly understand what you are trying to prove or disprove, such as ownership of a vendor, identities of relatives, significant others, or business partners, or undisclosed assets.

As you begin the search, it's best to start with broad, general searches (subject's name, company name, email address) and then refine to specific geographic regions or databases. As you start collecting data, you should meticulously document sources of where, when, and how data was obtained, including the URLs, timestamps, screenshots, and any metadata, to preserve authenticity. In addition, one should not rely on a single OSINT source but instead verify with at least two independent sources. For example, if the subject posts photos of a luxury vehicle on social media, confirm the ownership through vehicle registration databases.

Once information has been collected, the forensic accountant can integrate it with financial analysis. For instance, if the forensic accountant has uncovered the ownership of a luxury vehicle through OSINT, the forensic accountant can verify whether the subject misappropriated company funds to purchase said vehicle. Throughout the investigation, the forensic accountant should continuously monitor and update as new public information may become available.

LEGAL AND ETHICAL CONSIDERATIONS

The use of OSINT in fraud investigations must always remain within ethical and legal boundaries. To avoid legal and ethical risks, forensic accountants should always consider jurisdiction, respect privacy laws, avoid any type of bias, and maintain admissibility. Ethical OSINT is about leveraging what is publicly available, not tricking or deceiving subjects into revealing information. Forensic accountants should be mindful of privacy and data protection laws when using OSINT. It's important to consider jurisdiction to understand privacy laws, as different regions maintain different privacy laws and regulations, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) in the European Union. As with other rules, forensic accountants should consult legal counsel, especially when dealing with cross-border cases.

Investigators should strive to avoid bias throughout the investigation, especially confirmation bias. When using OSINT, stay neutral and expand searches to those that may prove or disprove any theories. Also, consider any alternative explanations for findings and document all evidence, both supporting and contradictory.

CONCLUSION

Integrating open-source intelligence into fraud investigations is essential in our digital age as society generates vast amounts of data each day. By systematically incorporating OSINT into investigative work plans, forensic accountants can uncover hidden connections, validate suspicions, and build stronger, more defensible cases. While fraudsters may manipulate the books, they cannot easily erase the digital and public records that OSINT makes visible and available.

NATALIE LEWIS, CPA/CFF, CFE *is a senior vice president in J.S. Held's economic damages & valuations practice. As a CPA and Certified Fraud Examiner, who is also certified in financial forensics, Natalie specializes in forensic accounting and the analysis of economic damages. She provides consulting and expert services for both plaintiff and defense law firms for investigations involving embezzlement, Ponzi schemes, commercial crime insurance claims, Foreign Corrupt Practices Act (FCPA) and asset misappropriation. Natalie can be reached at natalie.lewis@jsheld.com or 470-852-4601.*