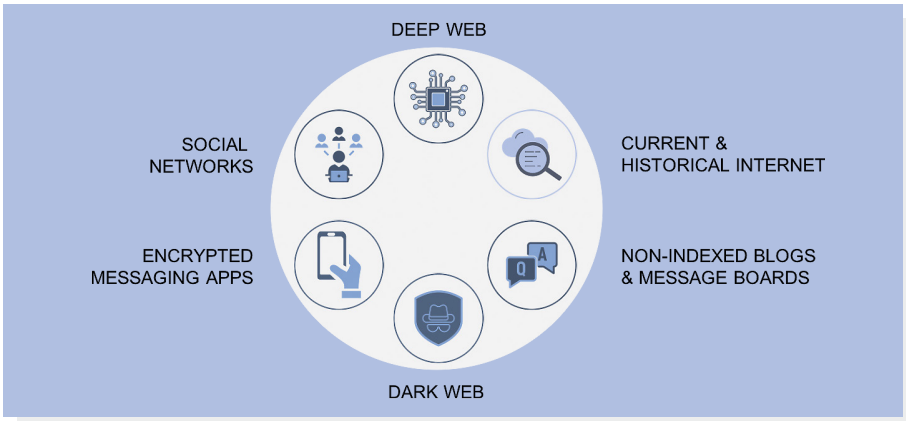
GAME-CHANGING DIGITAL BACKGROUND CHECKS AND ASSET SEARCHES

Fraud examiners understand the importance of knowing whom you're doing business with. From compliance and due diligence to investigative asset tracing, solid background-checking skills are key tools for CFEs. But beyond traditional methods, new techniques are emerging to greatly enhance business transparency — and some may surprise you.

Proficiency in conducting background checks and asset tracing is a critical skill set for fraud examiners. Some of the traditional ways to obtain information on subjects include searching public records, reference checks, adverse media scans, checking sanctions and watchlist databases, report writing, case management and the occasional "dumpster diving." But it's important that CFEs remain aware of the latest capabilities and technologies.

Recent advancements in technology have allowed anti-fraud professionals to conduct deeper, more advanced and efficient due diligence research, incorporating the banking, email, geospatial and hidden-web activities of a person or corporation of interest.

In a recent podcast, I interviewed Ernie Brod, a legend in the due diligence field with over 30 years of experience providing business intelligence services. I was fascinated as Brod described the capabilities now available to anti-fraud professionals to enhance their digital background checks and asset searches. Brod put it best when he said, "These new approaches are a heck of a lot faster, and cleaner, than traditional dumpster diving." (See "Digital Dumpster Diving: Four Key Innovations to Enhancing Your Digital Background Checks or Asset Searches with Ernest Brod," The Walden Pond, March 4, tinyurl.com/w75jv3nn.) In this column, I'll summarize my conversation with Brod and these new innovations in bank, web, contact (email) and geospatial intelligence.



Before we begin, however, I'd be remiss to not bring up the importance of data privacy and ensuring that the techniques I'm describing below are conducted ethically and legally. Understanding the rules of the game yourself, and working with legal counsel or a recognized, reputable law firm, is often the safest way to conduct these advanced due-diligence techniques. As always, consult with your privacy counsel before conducting these types of searches.

Bank intelligence

When an investigator is performing an asset trace, one of the first questions should be, "Did the person of interest (POI) interact with any banks or financial institutions?"

In the context of global asset searches, bankruptcy trustee recoveries, fraud investigations or high-profile divorce contests, leveraging the power of banking intelligence can be a real game changer for your case. It's almost impossible these days to set up a bank account without interacting with a bank through email. By tracking email contacts between the subject and the databases of all registered banks,

branches or financial institutions around the globe (over 250,000 in total), investigators can safely and anonymously identify connections between the subject and any bank or financial institution they interacted with. While the technology can't tell the investigator whether an account was set up or reveal any privacy details about deposit amounts or banking information (and providing such information would run afoul of most ethical standards), it's certainly enough to help narrow the focus of which banks to subpoena or contact.

For example, let's say a fraud examiner is conducting an asset search on a POI, such as a corporation's CFO, and all the fraud examiner has to go by is the CFO's email address. Has the CFO set up any offshore bank accounts? In how many banks might the CFO or the company have money stashed? Without firsthand knowledge or access to company records, it would be nearly impossible to identify which banks the CFO interacted with. But with bank intelligence that bounces the CFO's email address across the entire registry of global banks, the fraud examiner can quickly narrow the universe of banks to the handful that communicated by email with the CFO. That's a pretty powerful tool.

Web intelligence

Another question the investigator should ask is, "What information about the company or person of interest exists that is *not* searchable on 'widely accessible' internet sites or search engines?"

As fraud examiners, we all know how to conduct a Google search. We may even know a few good governmental and commercial websites where we can search public records. But what about the vast amount of content on the internet that isn't searchable? Web intelligence digs deeper than traditional

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
MANAGING DIRECTOR, ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS PRACTICE

internet searches to shine a light into risk areas that aren't typically indexed or searchable. From an investigator's perspective, such risk areas might include theft of trade secrets, evidence that a product or service is being knocked off (or in violation of a patent), chatter about hidden issues brewing at the company, plans for a demonstration protesting against the company, communications among activist investors pressing for board seats, tracking hidden assets … the list goes on. To help understand the scope of web intelligence and what is searchable and discoverable, here are a few definitions from dictionary.com to consider:

- Deep web: The portion of the internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites.
- Dark web: The dark web, on the other hand, is defined as the portion of the internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser. It is part (or a subset) of the deep web.
- Social networks: In the context of digital technology, a social network is an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc. These social networks can also include non-indexed blogs or message boards.

Dark web, social networks and web intelligence might also look into historical web pages (or web archives) that were once posted online but have since been taken down. (See chart on page 8.)

Contact intelligence

Another investigative question to ask is, "Given a set of suspect email addresses, can we confirm if any of them have ever communicated?"

Without the need to physically collect hard drives or network servers (often an expensive and intrusive process), a fraud examiner can conduct quick internet scans across registries to see if two email addresses of interest have ever connected with each other. The information is limited to only a yes/no answer to the question of whether a communication was made — meaning there's no metadata available, such as "to/from/cc/bcc" information; and no information about the content, subject or time the email was sent. But simply confirming that there was communication could be an important factor in your investigation. For example, let's say a whistleblower hotline call alleges that Employee A leaked sensitive trade secrets to Person B, who works for a competitor. With knowledge of their respective email addresses (ideally, both personal and business email addresses), you could conduct a contact intelligence scan to see if the two email addresses have ever connected. If so, then more investigative procedures may be warranted.

Location intelligence

Cellphone records can also provide useful data, which leads us to ask, "Using publicly available cellphone data, can we track the movements of a person of interest and determine their movement over time?"

The answer is yes. While the U.S. government's National Geospatial-Intelligence Agency is dedicated to this type of analysis, similar capabilities are also available to private citizens. In an investigative context, location intelligence uses aggregated cellphone data to pinpoint movements associated with individual phone numbers. From a privacy perspective, the name and ownership connected to a particular phone number remain private information. The phone number itself, however, is public. So, if the investigator knows the subject's cellphone number, they can perform the analysis.

Going back to our trade secret example, imagine the value from an investigator's perspective of being able to show that Employee A's cellphone arrived at the competitor's home office where Person B worked. The phone's movement is tracked regardless of whether Employee A made any phone calls, as long as the phone is turned on in cellular mode (not airplane mode, for example). This same technology was used by law enforcement and prosecutors investigating the Jan. 6 storming of the U.S. Capitol, where individual cellphone movement was shown traveling to the Capitol. (For a good explanation of the technology, see "They Stormed the Capitol. Their Apps Tracked Them," by Charlie Warzel and Stuart A. Thompson, The New York Times, Feb. 5, tinyurl.com/h4myzpkw.)

Start your digital digging

With these new techniques for asset tracing and background checks in your fraud examiner's tool belt, you're ready to uncover highly relevant information and log more successful investigations better, cheaper and faster. Remember to conform with all applicable laws and consult with privacy counsel as needed. Good luck, and happy hunting! ■ FM

Vincent M. Walden, **CFE**, **CPA**, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback. Contact Walden at vwalden@alvarezandmarsal.com. Walden thanks Ernie Brod for his contributions to this column. You can reach Brod at ebrod@alvarezandmarsal.com.