

15

**EFFECTIVE USE OF EVIDENCE
IN WHITE COLLAR INVESTIGATIONS
AND LITIGATION**

Edward M. Stroz

Stroz Friedberg, LLC

Effective Use of Evidence in White Collar Investigations and Litigation

Edward M. Stroz

The challenge in conducting a fair white collar investigation almost always is to gather evidence of the true intent behind the actions of the people involved. White collar offenses are usually about actions that are not violent or inherently illegal. Examples include writing a check, transferring funds, or making a representation about an investment or contract. Therefore, the bank accounts, checks, and correspondence documents typically found in white collar investigations are often no different, on their face, from those used in legitimate commerce. What makes those documents interesting, or not, will be based on evidence about how they were used, for what purpose, and to further what intentions.

As we all know from press accounts, it is email and other forms of electronic evidence that often emerge as a powerful source of intent evidence. For example, in kick-back investigations it is often possible to establish the actual payment of funds from one person to another. But, proving those funds were conveyed with the intention of paying back someone for a favor, such as in a corruption case, a procurement scandal, or the theft of trade secrets, is difficult without evidence establishing the link between the money and why it was transferred. Establishing the link between the money and the purpose for which it was paid, whether innocent or illicit, might be derived from the correspondence surrounding the transaction. In today's society, that correspondence will often be in the form of email or text messages.

In my experience, government prosecutors and investigators often find it of great value to establish a timeline of the evidence in a white collar investigation. The simple act of arranging facts in a chronological sequence clarifies the facts of the case, and helps establish "who knew what and when did they know it". Email is more often used as an alternative to conversation than to mail or letter. As a result, email is often more relaxed, open, and originates closer to key events in the timeline.

A single email may contain a fact that has huge significance in an investigation. Consequently, it's important to have a complete working set of emails relevant to an investigation. The failure to produce all emails relevant to a matter under investigation risks leading an investigation to erroneous conclusions. It can also lead to severe problems, including sanctions, if the matter goes to court. This makes the collection and review of email evidence a process that has to be executed carefully, properly, and documented with an audit trail that allows each item of evidence to be traceable to its original source (or multiple sources when copies and duplicates are involved).

Another key source of evidence that should be considered in building a chronological sequence is an internet web browser history. People often browse (or interact with) websites or conduct internet searches for topics or things that may provide important factual indicators of their states of mind. For example, a person under investigation for stealing a trade secret may have visited a website that explains how to copy data onto a CD, or how to delete and wipe data so it will not be found later. Clearly those types of actions have significance in establishing what a person may have intended just before or after a key event took place.

It is also important to distinguish "digital forensics" from "ediscovery." While there are differing views on what those terms mean, it's generally useful to think of "ediscovery" as pertaining to the "obvious" data that a general user can read and is familiar seeing on a computer screen. For example, the date and time an email is sent or received is generally evident from the face of the email. However, establishing whether an email was opened, or its attachment was opened, can require analysis of data and file attributes that cannot be accessed by a general purpose user, or cannot be accessed without the risk of altering that same information while trying to read it. Finding and interpreting latent, forensic digital evidence generally requires training, expertise, and experience.

The evidence gathered in a white collar investigation should be used in an interview of the relevant persons. The way the evidence is used will depend on the professional judgment and interview strategy of the interviewer. For example, sometimes an article of evidence is used to initiate a line of questioning by showing the evidence to the person being interviewed and asking questions about it. In other examples, the interviewer asks questions without the evidence in view, and then decides whether to display it to the person being interviewed in order to corroborate or refute what was stated. The results of an interview can also provide new information that makes it necessary to revisit certain evidence for reexamination.

In summary, white collar evidence continues to consist of traditional commercial documents such as checks (front and back), wire transfers of funds, bank account statements, ledgers, telephone records, and hard copy documents. However, these documents by themselves rarely indicate fully the intentions of the people who utilize them. Because the element of intent is often so crucial in white collar investigations, it is important to be astute about where such evidence can be found. Electronic evidence, including emails, text messages, and documents, often contain language and other attributes which indicate the state of mind of an individual at a point in time. Such electronic evidence may require special handling, a defensible chain-of-custody, and analysis of latent attributes. Arranging evidence (electronic and hard copies) in a chronological sequence can bring out and facilitate obtaining an accurate understanding of the facts, and allow for a fair and thorough interview of the parties involved.