



Fraud & the Law

Law for Fraud Examiners



By Juliana Morehead, J.D., CFE, and Kelly J. Todd, CPA/ABV

ELECTRONIC DISCOVERY IN THE 21ST CENTURY

For this column, Juliana Morehead is joined by coauthor, Kelly J. Todd, CPA/ABV, shareholder at Forensic/Strategic Solution PC. – ed.

The quantity and quality of electronic information stored on computers and other electronic media have forever changed the way attorneys approach the discovery process and fraud examiners approach internal investigations. Researchers at the University of California at Berkeley estimate that 93 percent of all information is solely computer data.¹ Many businesses in a wide variety of industries – including banking, insurance, manufacturing, service, and retail sales – maintain only electronic documents in their “digital offices.”

Computer systems or other electronic media contain vital information about activities, motives, and intent of suspect individuals and businesses. Information relevant to cases can reside in a variety of locations and forms so electronic discovery can be extremely challenging. Locating, searching, and managing electronic evidence requires an understanding of technology that often goes beyond that of the average computer user. And because electronic evidence is fragile, we have to avoid corruption of data to preserve evidence admissibility in a court of law. Fraud examiners must learn about electronic evidence – how it’s stored and retrieved, what and how to ask for it, and the federal discovery rules that surround its admissibility. One thing is certain: the opposing party isn’t going to volunteer electronic information (assuming they already have the info).

Researchers at the University of California at Berkeley estimate that 93 percent of all information is solely computer data.

WHAT’S ELECTRONIC EVIDENCE?

Electronic evidence is any information residing on various storage devices or media, but it’s normally on a personal computer’s hard drive or on a server. The distinguishing legal factors between electronic evidence and traditional paper documents are vast. Moreover, because most electronic evidence is never printed to paper, the amount of information available in digital form can be staggering. For example, a 10-gigabyte computer hard drive (considered small by today’s standards), can potentially contain more than 4.5 million pages of text data.

Discovery in large cases might yield thousands and sometimes millions of pages of evidence, most of which is stored electronically. And electronic documents thought to be deleted or lost by a user can be recovered. Valuable information such as time, date, and author’s name might be embedded in an electronic version of a document. We can compare a computer backup to an existing document to show that it was altered and when it happened. Also, we can freeze casual and candid e-mail correspondence in time.

COLLECTING AND PRESERVING ELECTRONIC EVIDENCE

Courts have routinely held that information generated and stored on computers and in other electronic forms is discoverable. Collection and preservation can fall into one or two categories: evidence in the client’s possession, as in an internal investigation, and evidence that’s controlled by an external third party, as in a case of discovery for civil litigation.

The Internal Investigation

You should immediately safeguard all suspect computers and other removable devices and quickly complete the forensic investigation. In fact, before you do anything else, restrict all access to computers and digital information if a suspected

or terminated employee knows an investigation is pending or underway. A business' worst cyber-crime threat doesn't come from outside the organization but from its employees. A disgruntled employee can wreak havoc on information systems in a matter of seconds. Among several other devastating possibilities, the employee can attempt to cover his tracks by deleting incriminating evidence, stealing sensitive trade secrets, and encrypting programs that render them useless.

Opponent's Electronic Data

In every lawsuit, you have to tailor your discovery strategy according to the specific needs of the case and the client's budget. Obviously, when opposing counsel shares more electronic data, a case's scope and depth of discovery increases. And you'll substantially cut expenses if the parties agree on guidelines for producing and preserving electronic evidence. Establish one repository of all electronic material to avoid duplication of efforts and expense.

Letter of Preservation

If you have to wait weeks for the courts to give you a discovery order to access an opponent's computer systems, send a letter of preservation to the opponent to establish notice that the recipient has a legal duty to preserve electronic evidence relevant to the case. This can be a useful tactic to accelerate the case.

Interrogatories

Interrogatories are one of the easiest and least expensive methods for gathering basic information about a company's information system. Write questions so that the answers establish an overall picture of the opponent's computer system and information system processes. Questions focusing on key personnel in the information systems department are especially helpful in determining individuals to depose. You might want to ask a computer forensic specialist for precise computer terms and concepts when you write your questions.

Requests for Production

Make sure your requests for production stipulate that you're asking for both electronic and paper documents. Requests should include such items as data compilations, e-mails, various storage media, and backup tapes.

Depositions

Questions leading to depositions of key personnel within a company's information systems department will be similar to interrogatories. Focus them on the system profile, the backup and retention schedules, maintenance and access, and chain of custody and authentication. You could retain a computer forensic specialist for the deposition's planning and preparation.

FEDERAL RULES OF CIVIL PROCEDURE

Although electronic information has been introduced in courts

for many years, the rules for pre-trial discovery have traditionally been limited to the scope of physical evidence such as paper documentation, photographs, charts, and graphs. Because of the increasing management of documents in electronic format, coupled with the judicial difficulty of introducing electronic documents as evidence, the Federal Rules of Civil Procedure (FRCP) amended several discovery rules in 2006 to acknowledge electronic information as a necessary component of discoverable evidence.

Rule 26

FRCP Rule 26 sets forth the most substantial amendments affecting electronic discovery. Whereas the FRCP once used the term "data compilations" to refer to electronic evidence, the 2006 amendments replaced this term with "electronically stored information."

Rule 26 requires a discovery planning conference between parties to discuss certain issues such as the form in which the parties want electronic information to be produced. Prior to the amendment, parties *could* discuss electronic discovery issues but now they *must*. Following a discovery planning conference, the parties are to develop a discovery report (Form 35 report), which includes a description of how disclosure or discovery of electronic information should be handled. After the court receives a Form 35 report from the parties, it will enter a scheduling order.² FRCP Rule 16 provides that the order may also include "provisions for disclosure or discovery of electronically stored information." Consequently, failure to abide by a discovery report or scheduling order might result in sanctions and possible criminal charges against the parties.

The amendments also provide that, in most circumstances, parties must voluntarily turn over (that is, without awaiting a discovery request by the other party) a copy, or a description by category and location, of all electronically stored information to the other party within 14 days of the discovery planning conference. Therefore, parties (or organizations) must be prepared for the advent of electronic discovery prior to a case being filed or when litigation is foreseeable.

The most notable change to Rule 26 is the provision that "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information isn't reasonably accessible because of undue burden or cost." "Reasonably accessible" isn't defined in the statute. However, we can deduce that production of electronic information can't result from "undue burden or cost." Thus at the outset of foreseeable litigation, parties should understand the scope and sources of

the electronic information that might be related to the case and the information's location and format. Thereafter, the court will be responsible to reconcile disagreements between the parties on which electronic information is reasonably accessible.

Rule 34

Rule 34 now establishes a procedure that gives parties a means for determining the form of production for electronic information. Specifically, a requesting party "shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced." This rule also requires that when a party objects to the form for producing the electronic information or if no form is specified in a request for information, "the responding party must state the form or forms it intends to use." Furthermore, if a request doesn't specify a form for producing the electronic information, the "responding party must produce the information in a form or forms in which it is ordinarily maintained ... or that are reasonably usable." Given the specificity of Rule 34, parties should decide on the type of form(s) they want to obtain prior to requesting electronic information from the opponent.

Rule 37

The most controversial electronic discovery amendment is found in FRCP Rule 37. Rule 37 is a "safe harbor" provision, which provides "[a]bsent exceptional circumstances, a court may not impose sanctions ... on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." What defines a "good-faith operation" is left open for court interpretation. However, ignorance of how your electronic information is stored is no defense.

EXPERT WITNESSES

The complicated collection and preservation methods and the fragile nature of electronic evidence often require expert witnesses knowledgeable in computer forensics to help the judge and/or jury understand the technology. But attorneys often mistakenly employ individuals who don't have the appropriate expertise and might give inadmissible evidence. The expert not only should be proficient in handling and preserving evidence but should attempt to establish a relationship with the employer's system administrator and learn the operating and backup systems.

DILIGENT IN EVERY STEP

Electronic discovery carries a burden greater than the mere technicality of ensuring that rules are followed and evidence is correctly gathered and protected. The cost of collecting and preserving the evidence can be enormous and could push a settlement out of court. Nonetheless, fraud examiners must be diligent in every step of the process to ensure that the discoverable evidence can be set forth accurately and understandably to any layperson. 🔍

Juliana Morehead, J.D., CFE, is a staff attorney, legal writer, and editor for the ACFE. Her e-mail address is: jmorehead@ACFE.com. Kelly J. Todd, CPA/ABV, an ACFE Associate Member, is a shareholder at Forensic/Strategic Solution, PC, in Birmingham, Ala. Her e-mail address is: kelly@forensicstrategic.com.

¹ Peter Lyman and Hal R. Varian, "How Much Information?" Oct. 20, 2000. Available at www2.sims.berkeley.edu/research/projects/how-much-info/charts/charts.html.

² A scheduling order is entered by the district court judge, or a magistrate judge when authorized by a district court rule, which limits the time to: join other parties to the lawsuit, file motions, and complete discovery. In addition to setting forth a time schedule, it might also include: modifications of the times for disclosures; the extent of admissible discovery, provisions for disclosure or discovery of electronic evidence; agreements by the parties relating to asserting privilege claims or protection of trial-preparation material after production; dates of pre-trial conferences and the trial; and other matters as deemed appropriate in the circumstances of the case.

ADVERTISERS' INDEX

| | |
|--------------------|--------------------|
| CaseMap/LexisNexis | Page 1 |
| EthicsLine | Page 2 |
| IDEA | Inside front cover |
| Protiviti | Back cover |
| WizSoft | Page 15 |

This index is provided as a reader service. The publisher doesn't assume any liability for errors or omissions. For information about advertising, call Leslie Simpson at the ACFE, (800) 245-3321 or e-mail her at lsimpson@ACFE.com.

Publication of an advertisement in *Fraud Magazine*TM doesn't constitute an endorsement of the product or service by *Fraud Magazine*TM or the Association of Certified Fraud Examiners Inc.