O'CONNOR DAVIES

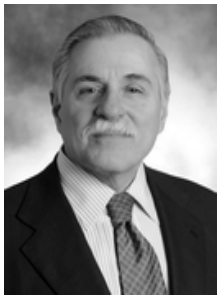
AUDIT | TAX | CONSULTING

PKF

Viewpoint on Value Newsletter

Keys to ESI Authentication

Edited by Ciro V. Cuono, Partner, CPA/ABV/CFF, CVA, CGMA



Ciro V. Cuono
CPA/ABV/CFF
CVA, GCMA
Partner
ccuono@odpkf.com
914.381.8900

Electronically stored information (ESI) has assumed a prominent role in commercial and other types of litigation. Like any evidence, it must satisfy the rules for authentication.

Unfortunately, ESI faces some unusual authentication hurdles. Unlike static paper financial statements and other documents, ESI is typically a collection of information produced by computer systems and can easily be edited without leaving any record of prior versions. Authentication, therefore, requires sufficient evidence to establish that the ESI has not been changed since its creation or a particular relevant date. Qualified experts must use several methods to ensure this type of evidence is admissible at trial.

Technological Avenues

The federal and state rules of evidence generally allow a proponent of evidence to authenticate it through its "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." These rules could cover several types of ESI authentication, including:

Hashing **-** Every electronic file is assigned a "hash value," or unique numerical identifier. One judge has described hashing as "a digital equivalent of the Bates stamp used in paper document production." A new hash value is created each time a file is modified, so hashing can be used to guarantee the authenticity of an original data set and, in turn, establish that another file is an exact duplicate.

Metadata **-** System metadata is created by the operating systems that run computers, servers and other devices. All electronic files include metadata that conveys information, such as the dates a file was created, last modified and last accessed. Metadata, however, is vulnerable to undetectable manipulation and can be deleted with access to the file. Metadata also changes each time a file is opened, which can compromise the usefulness of the information for authentication.

Digital signatures **-** A digital signature requires the signer to have a certificate-based digital ID. Digital certificates, which are issued by a "trusted authority" or "certificate authority," are the critical component in Public Key Infrastructure (PKI) and are used in the digital signature process in a way that can provide authentication.

But the presence of a digital signature indicates only that *someone* with access to the ID has signed the document. The proponent of the ESI must link it to the specific individual. What's more, it is impossible to establish when the digital

signature was created. For these reasons, digital signatures are best used in conjunction with other authentication methods.

Self-Authenticating Methods

The rules of evidence generally recognize several methods of self-authentication. Trusted time stamping may allow for the self-authentication of ESI if it can verifiably establish an accurate and nonalterable time for the evidence.

According to the rules of evidence, another permissible method of self-authentication for ESI is by "inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin." For example, corporate e-mails frequently identify the origin of the transmission and the company.

Expert Witness Testimony

Experts with relevant knowledge can offer testimony that establishes the integrity of ESI by showing that it has not been modified since its creation. Experts don't need to have personal knowledge of a particular piece of ESI as long as they can testify to applicable safeguards and the process by which it was created and preserved.

Experts also can authenticate ESI on the stand. For example, an expert witness might compare it with other pieces of ESI that have already been authenticated.

Planning Ahead

Each type of ESI comes with specific challenges. Work with your expert to determine the relevant authentication requirements and to anticipate your opponent's likely attacks on the evidence.

***

If you have any questions regarding business valuation, forensic accounting or litigation support services, please contact Ciro V. Cuono, CPA/ABV/CFF, CVA, CGMA, at ccuono@odpkf.com or 914.421.5671.

Contact:

New York, NY
212.286.2600
212.867.8000

Harrison, NY
914.381.8900

Stamford, CT
203.323.2400

Paramus, NJ
201.712.9800

Cranford, NJ
908.272.6200

New Windsor, NY
845.220.2400

Wethersfield, CT
860.257.1870

IRS CIRCULAR 230 DISCLOSURE: To comply with IRS regulations, we are required to inform you that unless expressly stated otherwise, any discussion of U.S. federal tax issues in this correspondence (including any attachments) is not intended or written to be used, and cannot be used, (i) to avoid any penalties imposed under the Internal Revenue Code, or (ii) to promote, market, or recommend to another party any transaction or matter addressed herein.