Featured Professionals

Timothy M. O'Shea

Related Services

E-Discovery Strategy & Advocacy

Proposed Amendments to Federal Rule of Evidence 902 Will Impact Collection of Electronically Stored Information

Legal Update
01.27.2017

By Timothy M. O'Shea

To establish that an item of evidence is authentic, a proponent must produce sufficient evidence "to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). Rule 901(b) of the Federal Rules of Evidence sets forth examples for establishing that the evidence is authentic, such as the testimony of a witness with knowledge.

Rule 902, in its current form, provides that certain documents such as certified copies of public records, government documents and newspapers are self-authenticating and do not require extrinsic evidence of authenticity to be admitted at trial. Moreover, Rules 902(11) and (12) allow a party to rely on a foundation witness to establish the authenticity of business records by way of certification, but the opponent is given "a fair opportunity" to challenge both the certificate and the underlying record.

The proposed amendments to Rule 902 would add two new subdivisions that set forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness:

Rule 902. Evidence That is Self-Authenticating

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(13) *Certified Records Generated by an Electronic Process or System*. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) *Certified Data Copied from an Electronic Device, Storage Medium, or File.* Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

In a nutshell, the first amendment (paragraph 13) would allow for self-authentication of machine-generated information (i.e., establishing that a USB device was plugged into a computer). The second amendment (paragraph 14) would allow for self-authentication for a copy of data taken from an electronic device (i.e., establishing that a copy of an email was identical to the original email or a forensic copy of mobile device containing text messages was identical to the original phone text messages using an industry standard methodology for collection (e.g.,hash value or other means).

The intent of these amendments is to alleviate the need to call a witness at trial, pursuant to Rule 901, to certify the authenticity of electronic documents. The Advisory Committee found that "[i]t is often the case that a party goes to the expense of producing an authentication witness and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented." Thus, instead of calling a live witness, the proposals for new Rules 902(13) and 902(14) allow the proponent to provide a certificate by a qualified person to certify the authenticity of the electronic evidence.

The Advisory Committee Notes make clear that "[a] certification under this Rule can only establish that the proffered item is authentic. The opponent remains free to object to admissibility of the proffered item on other grounds — including hearsay, relevance, or in criminal cases the right to confrontation."

Takeaways

The proposed amendments to Rule 902 are expected to go into effect on December 1, 2017, and highlight the importance of utilizing best practices for collection of electronic evidence. Indeed, the proposed new rules make clear that a certification must be provided by a "qualified person" that can attest to the accuracy or reliability of the process that produced that exhibit or the facts establishing how that exhibit is an accurate copy. Thus, it is important that parties to litigation not only utilize defensible collection methods and tools, but also utilize an experienced e-discovery practitioner, information technology practitioner or forensic expert when collecting electronic evidence.