Amendments to the Federal Rules of Practice and Procedure: Evidence 2017—Self-Authenticating Electronic Evidence (Video Transcript)[1]

Federal Judicial Center

December 1, 2017

Federal Rules of Evidence 902(13) and 902(14), which became effective on December 1, 2017, provide for the self-authentication of electronic evidence. Under these rules, electronic evidence can be authenticated by certification instead of by testimony. Rule 902(13) applies to electronic evidence such as computer files, social media posts, smart device data, etc. Rule 902(14) applies to electronic copies.

NARRATOR: Authenticating evidence at trial simply means proving that it is what it purports to be. Self-authenticating evidence, on the other hand, is evidence deemed to answer that question without the burden of further testimony.

Federal Rule of Evidence 902 has for years listed twelve types of self-authenticating evidence. Sections 13 and 14, effective as of December 1, 2017, deal with the self-authentication of electronic evidence.

Self-authenticating evidence previously listed in Rule 902 included official publications, under Rule 902(5), and newspapers and periodicals, under 902(6). Other types of self-authenticating evidence are given that status because they are accompanied by a signature, seal, or certification.

Rules 902(13) and 902(14) provide for self-authentication of records generated by an electronic process or system and data copied from an electronic device, storage medium, or file, respectively, when the evidence is certified by a qualified person.

These new sections of Rule 902 were written to rely on already existing parts of the rule. That is, the "certification of a qualified person" under sections (13) and (14) must "compl[y] with the certification requirements of Rule 902(11) or 902(12)."

1. This is a transcript of a video available at www.fjc.gov/content/325216/rules-amendments-2017-self-authenticating-electronic-evidence.

Rule 902(11) provides for the self-authentication of certified *domestic* records of a regularly conducted activity. Rule 902(12) provides for the self-authentication of certified *foreign* records of a regularly conducted activity.

In turn, self-authentication requires that the record meets the procedural criteria of the Rule 803(6) hearsay exception for records of a regularly conducted activity. Specifically, the record must "(A) [be] made at or near the time by—or from information transmitted by—someone with knowledge; (B) [be] kept in the course of a regularly conducted activity of a business, organization, occupation, or calling whether or not for profit; [and] (C) [be made as] a regular practice of that activity."

To support the certification of the evidence of a *domestic* record, Rule 902(11) requires that "the certification of the custodian or other qualified person [comply] with a federal statute or a rule prescribed by the Supreme Court." Certification of a *foreign* record under Rule 902(12) requires that the certification "be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed."

New Rule 902(13) provides for the self-authentication of "[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 902(11) or 902(12)."

The Evidence Rules Advisory Committee explains, in a note accompanying the amendment, what authentication does and does not mean:

"A certification under this rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to the admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. For example, assume that a plaintiff in a defamation case offers what purports to be a printout of a webpage on which a defamatory statement was made. Plaintiff offers a certification under this Rule in which a qualified person described the process by which the webpage was retrieved. Even if that certification sufficiently establishes that the webpage is authentic, defendant remains free to object that the statement on the webpage was not placed there by the defendant. Similarly, certification authenticating a computer output, such as a spreadsheet, does not preclude an objection that the information produced is unreliable—the authentication establishes only that the output came from the computer."

Computer logs and metadata are other types of computer records that can be authenticated by certification under Rule 902(13).

Rule 902(14) speaks to the self-certification of "data copied from an electronic device, storage medium, or file, if authenticated by a process of digital authentication, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12)."

Rule 902(14) applies to electronic copies of electronic records. Here the Advisory Committee note explains how authentication is often established by what are called hash values:

"Today data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value.' A hash value is a number that is often represented by a sequence of characters that is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology."

New sections (13) and (14), like previously existing sections (11) and (12), require reasonable notice, before the trial or hearing, to the adverse party by the proponent of his or her intent to offer the record. That notice must be written and must make the record and certification available for inspection, so that the party has a fair opportunity to challenge them.