PROPOSED AMENDMENTS TO THE FEDERAL RULES OF EVIDENCE*

Rule 803. Exceptions to the Rule Against Hearsay—Regardless of Whether the Declarant Is Available as a Witness

The following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness:

* * * * *

(16) ***Statements in Ancient Documents.*** A statement in a document ~~that is at least 20 years old~~that was prepared before January 1, 1998, and whose authenticity is established.

* * * * *

Committee Note

The ancient documents exception to the rule against hearsay has been limited to statements in documents prepared before January 1, 1998. The Committee has

---

* New material is underlined; matter to be omitted is lined through.

determined that the ancient documents exception should be limited due to the risk that it will be used as a vehicle to admit vast amounts of unreliable electronically stored information (ESI). Given the exponential development and growth of electronic information since 1998, the hearsay exception for ancient documents has now become a possible open door for large amounts of unreliable ESI, as no showing of reliability needs to be made to qualify under the exception.

The Committee is aware that in certain cases—such as cases involving latent diseases and environmental damage—parties must rely on hardcopy documents from the past. The ancient documents exception remains available for such cases for documents prepared before 1998. Going forward, it is anticipated that any need to admit old hardcopy documents produced after January 1, 1998 will decrease, because reliable ESI is likely to be available and can be offered under a reliability-based hearsay exception. Rule 803(6) may be used for many of these ESI documents, especially given its flexible standards on which witnesses might be qualified to provide an adequate foundation. And Rule 807 can be used to admit old documents upon a showing of reliability—which will often (though not always) be found by circumstances such as that the document was prepared with no litigation motive in mind, close in time to the relevant events. The limitation of the ancient documents exception is not intended to raise an inference that 20-year-old documents are, as a class, unreliable, or that they should somehow not qualify for admissibility under Rule 807. Finally, many old documents can be admitted for the non-hearsay purpose of proving notice, or as party-opponent statements.

The limitation of the ancient documents hearsay exception is not intended to have any effect on authentication of ancient documents. The possibility of authenticating an old document under Rule 901(b)(8)—or under any ground available for any other document—remains unchanged.

The Committee carefully considered, but ultimately rejected, an amendment that would preserve the ancient documents exception for hardcopy evidence only. A party will often offer hardcopy that is derived from ESI. Moreover, a good deal of old information in hardcopy has been digitized or will be so in the future. Thus, the line between ESI and hardcopy was determined to be one that could not be drawn usefully.

The Committee understands that the choice of a cut-off date has a degree of arbitrariness. But January 1, 1998 is a rational date for treating concerns about old and unreliable ESI. And the date is no more arbitrary than the 20-year cutoff date in the original rule. *See* Committee Note to Rule 901(b)(8) ("Any time period selected is bound to be arbitrary.").

Under the amendment, a document is "prepared" when the statement proffered was recorded in that document. For example, if a hardcopy document is prepared in 1995, and a party seeks to admit a scanned copy of that document, the date of preparation is 1995 even though the scan was made long after that—the subsequent scan does not alter the document. The relevant point is the date on which the information is recorded, not when the information is prepared for trial. However, if the content of

the document is *itself* altered after the cut-off date, then the hearsay exception will not apply to statements that were added in the alteration.

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).

Committee Note

Paragraph (13). The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has

found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It 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. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(13) is solely

limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

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 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 describes 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 defendant. Similarly, a 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.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

The reference to Rule 902(12) is intended to cover certifications that are made in a foreign country.

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:

* * * * *

(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).

Committee Note

Paragraph (14). The amendment sets forth a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic

file, other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing an authenticating witness for this evidence is often unnecessary. It 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. The amendment provides a procedure in which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

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 as a sequence of characters and 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 reliably 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.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

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. For example, in a criminal case in which data copied from a hard drive is proffered, the defendant can still challenge hearsay found in the hard drive, and can still challenge whether the information on the hard drive was placed there by the defendant.

A challenge to the authenticity of electronic evidence may require technical information about the system or