JUDICIAL CONFERENCE OF THE UNITED STATES

WASHINGTON, D.C. 20544

THE CHIEF JUSTICE
OF THE UNITED STATES
Presiding

JAMES C. DUFF
Secretary

September 28, 2016

MEMORANDUM

To: The Chief Justice of the United States and
Associate Justices of the Supreme Court

From: James C. Duff James C. Duff

RE: Transmittal of Proposed Amendments to the Federal Rules of Evidence

By direction of the Judicial Conference of the United States, pursuant to the authority conferred by 28 U.S.C. § 331, I transmit herewith for consideration of the Court proposed amendments to Rules 803(16) and 902 of the Federal Rules of Evidence, which were approved by the Judicial Conference at its September 2016 session. The Judicial Conference recommends that the amendments be approved by the Court and transmitted to the Congress pursuant to law.

For your assistance in considering the proposed amendments, I am transmitting: (i) a "clean" copy of the affected rules incorporating the proposed amendments and accompanying Committee Notes; (ii) a redline version of the same; (iii) an excerpt from the September 2016 Report of the Committee on Rules of Practice and Procedure to the Judicial Conference; and (iv) an excerpt from the May 2016 Report of the Advisory Committee on Evidence Rules.

Attachments

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

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.

REPORT OF THE JUDICIAL CONFERENCE

COMMITTEE ON RULES OF PRACTICE AND PROCEDURE

TO THE CHIEF JUSTICE OF THE UNITED STATES AND MEMBERS OF THE JUDICIAL CONFERENCE OF THE UNITED STATES:

*****

FEDERAL RULES OF EVIDENCE

Rules Recommended for Approval and Transmission

The Advisory Committee on Evidence Rules submitted proposed amendments to Rules 803(16) and 902, with a recommendation that they be approved and transmitted to the Judicial Conference. The proposed amendments were circulated to the bench, bar, and public for comment in August 2015.

Rule 803(16)

Evidence Rule 803(16) provides a hearsay exception for "ancient documents"; that is, if a document is more than 20 years old and appears authentic, it is admissible for the truth of its contents. Over the years, the rationale for the exception has been criticized because it assumes that just because the document itself is authentic, all of the statements in the document are reliable enough to be admissible despite the fact they are hearsay. The Advisory Committee has long concurred with this criticism, but has not felt the need to address it because the exception is used infrequently. However, because electronically stored information can be retained for more than 20 years, a strong likelihood exists that the ancient documents exception will be used much more frequently going forward. Accordingly, the Advisory Committee determined that the time had come to address the ancient documents exception.

The decision to address the exception was based on a concern that, with its increased use, the exception could become a receptacle for *unreliable* hearsay—that is, if the hearsay is in fact

reliable it will probably be admissible under other reliability-based exceptions, such as the business records exception or the residual exception. Moreover, the need for an ancient documents exception is questionable as applied to electronically stored information, for the very reason that there may well be a great deal of *reliable* electronic data available to prove any dispute of fact.

The proposed amendment that was issued for public comment would have abrogated the ancient documents exception. While some commentators supported elimination of the exception, most did not. Lawyers in several specific areas—*e.g.*, product liability litigation involving latent diseases, land-use disputes, environmental clean-up disputes—said they had come to rely on the exception. After considering several alternatives, the Advisory Committee decided to amend the rule to limit the ancient documents exception to documents prepared before 1998. The year was chosen for two reasons: (1) going backward, it addressed the reliance-interest concerns of many commentators; and (2) going forward, reliable electronically stored information is likely to be preserved that can be used to prove the facts that are currently proved by scarce hardcopy. If the electronically stored information is generated by a business, then it is likely to be easier to find a qualified witness who is familiar with the electronic recordkeeping than it is under current practice to find a records custodian familiar with hardcopy practices from the 1960's and earlier. Moreover, the Committee Note emphasizes that the residual exception remains available to qualify old documents that are reliable, and makes clear the expectation that the residual exception not only can, but *should*, be used by courts to admit reliable documents prepared after January 1, 1998, that would have previously been offered under the ancient documents exception. The Advisory Committee unanimously approved the modification.

Excerpt from the September 2016 Report of the Committee on Rules of Practice and Procedure

Rule 902

The proposed amendments to Rule 902 (Evidence That Is Self-Authenticating) add two new subdivisions that would allow certain electronic evidence to be authenticated by a certification of a qualified person (in lieu of that person's testimony at trial). New Rule 902(13) would allow self-authentication of machine-generated information (such as a web page) upon a submission of a certificate prepared by a qualified person. New Rule 902(14) would provide a similar certification procedure for a copy of data taken from an electronic device, media, or file. The proposed new subdivisions are analogous to Rule 902(11) and 902(12), which permit a foundation witness to establish the authenticity and admissibility of business records by way of certification, with the burden of challenging authenticity on the opponent of the evidence. The purpose of the two new subdivisions is to make authentication easier for certain kinds of electronic evidence that, under current law, would likely be authenticated under Rule 901 but only after calling a witness to testify to authenticity. The Advisory Committee has found that electronic evidence is rarely the subject of a legitimate authenticity dispute yet, under current law, a proponent must still go to the expense of producing authenticating witnesses for trial. The amendments would alleviate the unnecessary costs of this production by allowing the qualifying witness to establish authenticity by way of certification.

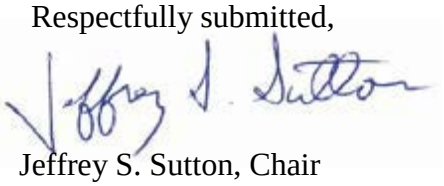
Commentators were generally supportive of the proposal. Following the public comment period, minor revisions to the Committee Notes were made in an effort to increase clarity and emphasize the importance of reasonable notice.

The Standing Committee voted unanimously to support both recommendations of the Advisory Committee on Evidence Rules.

Recommendation: That the Judicial Conference approve the proposed amendments to Evidence Rules 803(16) and 902, and transmit them to the Supreme Court for consideration with a recommendation that they be adopted by the Court and transmitted to Congress in accordance with the law.

*****

Respectfully submitted,



Jeffrey S. Sutton, Chair

Brent E. Dickson	Patrick J. Schiltz
Roy T. Englert, Jr.	Amy J. St. Eve
Gregory G. Garre	Larry D. Thompson
Daniel C. Girard	Richard C. Wesley
Neil M. Gorsuch	Sally Quillian Yates
Susan P. Graber	Jack Zouhary
William K. Kelley	

Excerpt from the May 7, 2016 Report of the Advisory Committee on Evidence Rules

COMMITTEE ON RULES OF PRACTICE AND PROCEDURE
OF THE
JUDICIAL CONFERENCE OF THE UNITED STATES
WASHINGTON, D.C. 20544

MEMORANDUM

TO: Hon. Jeffrey S. Sutton, Chair
Committee on Rules of Practice and Procedure

FROM: Hon. William K. Sessions, III, Chair
Advisory Committee on Evidence Rules

RE: Report of the Advisory Committee on Evidence Rules

DATE: May 7, 2016

I. Introduction

The Advisory Committee on Evidence Rules (the "Committee") met on April 29, 2016 in Alexandria, Virginia.

The Committee seeks final approval of two proposed amendments for submission to the Judicial Conference:

1. Amendment to Rule 803(16), the ancient documents exception to the hearsay rule, to limit its application to documents prepared before 1998; and

2. Amendment to Rule 902 to add two subdivisions that would allow authentication of certain electronic evidence by way of certification by a qualified person.

* * * * *

Excerpt from the May 7, 2016 Report of the Advisory Committee on Evidence Rules

II. Action Items

A. Amendment Limiting the Coverage of Rule 803(16)

Rule 803(16) provides a hearsay exception for "ancient documents." If a document is more than 20 years old and appears authentic, it is admissible for the truth of its contents. The Committee has considered whether Rule 803(16) should be eliminated or amended because of the development of electronically stored information. The rationale for the exception has always been questionable, because a document does not magically become reliable enough to escape the rule against hearsay on the day it turns 20. The Committee concluded that the exception has been tolerated because it has been used relatively infrequently, and usually because there is no other evidence on point. But because electronically stored information can be retained for more than 20 years, there is a strong likelihood that the ancient documents exception will be used much more frequently in the coming years. And it could be used as a receptacle for unreliable hearsay, because if the hearsay is in fact reliable it will probably be admissible under other reliability-based exceptions, such as the business records exception or the residual exception. Moreover, the need for an ancient documents exception is questionable as applied to ESI, for the very reason that there may well be a great deal of *reliable* electronic data available to prove any dispute of fact.

The proposed amendment that was issued for public comment would have eliminated the ancient documents exception. The public comment on that proposed elimination was largely negative, however. Most of the comments asserted that without the ancient documents exception, important documents in certain specific types of litigation would no longer be admissible—or would be admissible only through expending resources that are currently not necessary under Rule 803(16). Examples of litigation cited by the public comment include cases involving latent diseases; disputes over the existence of insurance; suits against churches alleged to condone sexual abuse by their clergy; cases involving environmental cleanups; and title disputes. Many of the comments concluded that the business records exception and the residual exception are not workable alternatives for ancient documents. The comments contended that the business records exception requires a foundation witness that may be hard to find, and that the residual exception is supposed to be narrowly construed. Moreover, both these exceptions would require a statement-by-statement analysis, which is not necessary under Rule 803(16), thus leading to more costs for proponents. Much of the comment was about the amendment's leading to extra costs of qualifying old documents.

In light of the public comment, the Committee abandoned the proposal to eliminate the ancient documents exception. But it also rejected the option of doing nothing. The Committee strongly believes that the ESI problem as related to Rule 803(16) is real. Because ESI can be easily and permanently stored, there is a substantial risk that the terabytes of emails, web pages, and texts generated in the last 20 or so years could inundate the courts by way of the ancient documents exception. Computer storage costs have dropped dramatically—that greatly expands the universe of information that could be potentially offered under the ancient documents exception. Moreover, the presumption of the ancient documents exception was that a hardcopy document kept around for 20 years must have been thought to have some importance; but that presumption is no longer the case with easily stored ESI. The Committee remains convinced that

it is appropriate and necessary to get out ahead of this problem—especially because the use of the ancient documents exception is so difficult to monitor. There are few reported cases about Rule 803(16) because no objection can be made to admitting the content of the document once it has been authenticated—essentially there is nothing to report. So tracking reported cases would not be a good way to determine whether ESI is being offered under the exception. Finally, the Committee adheres to its position that Rule 803(16) is simply a flawed rule; it is based on the fallacy that because a document is old and authentic, its contents are reliable. Therefore something must be done, at least, to limit the exception as to ESI.

The Committee considered a number of alternatives for amending Rule 803(16) to limit its impact. The alternatives of adding reliability requirements, or necessity requirements, were rejected. These alternatives were likely to lead to the increased costs of qualification of old documents, and extensive motion practice, that were opposed in the public comment. Ultimately, the Committee returned to where it started—the ESI problem. The Committee determined that the best result was to limit the ancient documents exception to documents prepared before 1998. That amendment will have no effect on any of the cases raised in the public comments, because the concerns were about cases involving records prepared well before 1998. And 1998 was found to be a fair date for addressing the rise of ESI. The Committee recognizes, of course, that any cutoff date will have a degree of arbitrariness, but it also notes that the ancient documents exception itself set an arbitrary time period for its applicability.

The Committee has considered the possibility that in the future, cases involving latent diseases, CERCLA, etc. will arise. But the Committee has concluded that in such future cases, the ancient documents exception is unlikely to be necessary because, going forward from 1998, there is likely to be preserved, reliable ESI that can be used to prove the facts that are currently proved by scarce hardcopy. If the ESI is generated by a business, then it is likely to be easier to find a qualified witness who is familiar with the electronic recordkeeping than it is under current practice to find a records custodian familiar with hardcopy practices from the 1960's and earlier. Moreover, the Committee has emphasized in the Committee Note that the residual exception remains available to qualify old documents that are reliable; the Note states the Committee's expectation that the residual exception not only can, but *should* be used by courts to admit reliable documents prepared after January 1, 1998 that would have previously been offered under the ancient documents exception.

The Committee unanimously recommends that the Standing Committee approve the * * * * * amendment to Rule 803(16), and the Committee Note, for submission to the Judicial Conference[.]

* * * * *

B. Proposed Amendment to Evidence Rule 902

At its Spring 2015 meeting, the Committee unanimously approved a proposal to add two new subdivisions to Rule 902, the rule on self-authentication. The first provision would allow self-authentication of machine-generated information, upon a submission of a certification prepared by a qualified person. The second proposal would provide a similar certification

procedure for a copy of data taken from an electronic device, medium or file. These proposals are analogous to Rules 902(11) and (12) of the Federal Rules of Evidence, which permit a foundation witness to establish the authenticity of business records by way of certification.

The proposals have a common goal of making authentication easier for certain kinds of electronic evidence that are, under current law, likely to be authenticated under Rule 901 but only by calling a witness to testify to authenticity. The Committee has concluded that the types of electronic evidence covered by the two proposed rules are rarely the subject of a legitimate authenticity dispute, but it is often the case that the proponent is nonetheless forced to produce an authentication witness, incurring expense and inconvenience—and often, at the last minute, opposing counsel ends up stipulating to authenticity in any event.

The self-authentication proposals, by following the approach taken in Rule 902(11) and (12) regarding business records, essentially leave the burden of going forward on authenticity questions to the opponent of the evidence. Under those rules a business record is authenticated by a certificate, but the opponent is given "a fair opportunity" to challenge both the certificate and the underlying record. The proposals for new Rules 902(13) and 902(14) would have the same effect of shifting to the opponent the burden of going forward (not the burden of proof) on authenticity disputes regarding the described electronic evidence.

Applications of Rules 902(13) and (14)

At the Standing Committee meeting in Spring 2015, Committee members inquired as to what kind of information might be authenticated under these new provisions. The Committee (with the substantial assistance of John Haried, who initially proposed these amendments) has prepared the following examples to illustrate how Rules 902(13) and (14) may be used:

Examples of how Rule 902(13) can be used:

1. Proving that a USB device was connected to (i.e., plugged into) a computer: In a hypothetical civil or criminal case in Chicago, a disputed issue is whether Devera Hall used her computer to access files stored on a USB thumb drive owned by a co-worker. Ms. Hall's computer uses the Windows operating system, which automatically records information about every USB device connected to her computer in a database known as the "Windows registry." The Windows registry database is maintained on the computer by the Windows operating system in order to facilitate the computer's operations. A forensic technician, located in Dallas, Texas, has provided a printout from the Windows registry that indicates that a USB thumb drive, identified by manufacturer, model, and serial number, was last connected to Ms. Hall's computer at a specific date and time.

> **Without Rule 902(13):** Without Rule 902(13), the proponent of the evidence would need to call the forensic technician who obtained the printout as a witness, in order to establish the authenticity of the evidence. During his or her testimony, the forensic technician would typically be asked to testify about his or her background and qualifications; the process by which digital forensic examinations are conducted in general; the steps taken by the forensic technician during the examination of Ms. Hall's

computer in particular; the process by which the Windows operating system maintains information in the Windows registry, including information about USB devices connected to the computer; and the steps taken by the forensic examiner to examine the Windows registry and to produce the printout identifying the USB device.

Impact of Rule 902(13): With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer; that the process by which such information is recorded produces an accurate result; and that the printout accurately reflected information stored in the Windows registry of Ms. Hall's computer. The proponent would be required to provide reasonable written notice of its intent to offer the printout as an exhibit and to make the written certification and proposed exhibit available for inspection. If the opposing party did not dispute the accuracy or reliability of the process that produced the exhibit, the proponent would not need to call the forensic technician as a witness to establish the authenticity of the exhibit. (There are many other examples of the same types of machine-generated information on computers, for example, internet browser histories and wifi access logs.)

2. Proving that a server was used to connect to a particular webpage: Hypothetically, a malicious hacker executed a denial-of-service attack against Acme's website. Acme's server maintained an Internet Information Services (IIS) log that automatically records information about every internet connection routed to the web server to view a web page, including the IP address, webpage, user agent string and what was requested from the website. The IIS logs reflected repeated access to Acme's website from an IP address known to be used by the hacker. The proponent wants to introduce the IIS log to prove that the hacker's IP address was an instrument of the attack.

Without Rule 902(13): The proponent would have to call a website expert to testify about the mechanics of the server's operating system; his search of the IIS log; how the IIS log works; and that the exhibit is an accurate record of the IIS log.

With Rule 902(13): The proponent would obtain the website expert's certification of the facts establishing authenticity of the exhibit and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the registry key, then the proponent would not need to call the website expert to establish authenticity.

3. Proving that a person was or was not near the scene of an event: Hypothetically, Robert Jackson is a defendant in a civil (or criminal) action alleging that he was the driver in a hit-and-run collision with a U.S. Postal Service mail carrier in Atlanta at 2:15 p.m. on March 6, 2015. Mr. Jackson owns an iPhone, which has software that records machine-generated dates, times, and GPS coordinates of each picture he takes with his iPhone. Mr. Jackson's iPhone contains two pictures of his home in an Atlanta suburb at about 1 p.m. on March 6. He wants to introduce into evidence the photos together with the metadata, including

the date, time, and GPS coordinates, recovered forensically from his iPhone to corroborate his alibi that he was at home several miles from the scene at the time of the collision.

Without Rule 902(13): The proponent would have to call the forensic technician to testify about Mr. Jackson's iPhone's operating system; his search of the phone; how the metadata was created and stored with each photograph; and that the exhibit is an accurate record of the photographs.

With Rule 902(13): The proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibits and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the iPhone's logs, then the proponent would not have to call the technician to establish authenticity.

4. Proving association and activity between alleged co-conspirators: Hypothetically, Ian Nichols is charged with conspiracy to commit the robbery of First National Bank that occurred in San Diego on January 30, 2015. Two robbers drove away in a silver Ford Taurus. The alleged co-conspirator was Dain Miller. Dain was arrested on an outstanding warrant on February 1, 2015, and in his pocket was his Samsung Galaxy phone. The Samsung phone's software automatically maintains a log of text messages that includes the text content, date, time, and number of the other phone involved. Pursuant to a warrant, forensic technicians examined Dain's phone and located four text messages to Ian's phone from January 29: "Meet my house @9"; "Is Taurus the Bull out of shop?"; "Sheri says you have some blow"; and "see ya tomorrow." In the separate trial of Ian, the government wants to offer the four text messages to prove the conspiracy.

Without Rule 902(13): The proponent would have to call the forensic technician to testify about Dain's phone's operating system; his search of the phone's text message log; how logs are created; and that the exhibit is an accurate record of the iPhone's logs.

With Rule 902(13): The proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibit and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the iPhone's logs, then the court would make the Rule 104 threshold authenticity finding and admit the exhibits, absent other proper objection.

Hearsay Objection Retained: Under Rule 902(13), the opponent – here, criminal defendant Ian—would retain his hearsay objections to the text messages found on Dain's phone. For example, the judge would evaluate the text "Sheri says you have some blow" under F.R.E. 801(d)(2)(E) to determine whether it was a coconspirator's statement during and in furtherance of a conspiracy, and under F.R.E. 805, to assess the hearsay within hearsay. The court might exclude the text "Sheri says you have some blow" under either rule or both.

Example of how Rule 902(14) can be used

In the armed robbery hypothetical, above, forensic technician Smith made a forensic copy of Dain's Samsung Galaxy phone in the field. Smith verified that the forensic copy was identical to the original phone's text logs using an industry standard methodology (*e.g.*, hash value or other means). Smith gave the copy to forensic technician Jones, who performed his examination at his lab. Jones used the copy to conduct his entire forensic examination so that he would not inadvertently alter the data on the phone. Jones found the text messages. The government wants to offer the copy into evidence as part of the basis of Jones's testimony about the text messages he found.

> **Without Rule 902(14):** The government would have to call two witnesses. First, forensic technician Smith would need to testify about making the forensic copy of information from Dain's phone, and about the methodology that he used to verify that the copy was an exact copy of information inside the phone. Second, the government would have to call Jones to testify about his examination.
>
> **With Rule 902(14):** The proponent would obtain Smith's certification of the facts establishing how he copied the phone's information and then verified the copy was true and accurate. Before trial the government would provide the certification and exhibit to the opposing party—here defendant Ian—with reasonable notice that it intends to offer the exhibit at trial. If Ian's attorney does not timely dispute the reliability of the process that produced the Samsung Galaxy's text message logs, then the proponent would only call Jones.

The Committee has carefully considered whether the self-authentication proposals would raise a Confrontation Clause concern when the certificate of authenticity is offered against a criminal defendant. The Committee is satisfied that no constitutional issue is presented, because the Supreme Court has stated in *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 322 (2009), that even when a certificate is prepared for litigation, the admission of that certificate is consistent with the right to confrontation if it does nothing more than authenticate another document or item of evidence. That is all that these certificates would be doing under the Rule 902(13) and (14) proposals. The Committee also relied on the fact that the lower courts have uniformly held that certificates prepared under Rule 902(11) do not violate the right to confrontation; those courts have relied on the Supreme Court's statement in *Melendez-Diaz.* The Committee determined that the problem with the affidavit found testimonial in *Melendez-Diaz* was that it certified the accuracy of a drug test that was itself prepared for purposes of litigation—a certification cannot render constitutional an underlying report that itself violates the Confrontation Clause. There is of course no intention or implication from the amendment that a certification could somehow be a means of bringing otherwise testimonial reports into court. But the Committee concluded that if the underlying report is not testimonial, the certification of authenticity will not raise a constitutional issue under the current state of the law.

In this regard, the Note approved by the Committee emphasizes that the goal of the amendment is a narrow one: to allow authentication of electronic information that would

otherwise be established by a witness, instead to be established through a certification by that same witness. The Note makes clear that these are authentication-only rules and that the opponent retains all objections to the item other than authenticity --- most importantly that the item is hearsay or that admitting the item would violate a criminal defendant's right to confrontation.

The Committee unanimously recommends that the proposed amendment to Rule 902, adding new subdivisions (13) and (14), and their Committee Notes, be approved by the Standing Committee and submitted to the Judicial Conference.

* * * * *