

1 Lisa M. Panahi, Bar No. 023421
2 General Counsel
3 State Bar of Arizona
4 4201 N. 24th Street, Suite 100
5 Phoenix, AZ 85016-6288
6 (602) 340-7236

7
8 **IN THE SUPREME COURT**
9 **STATE OF ARIZONA**

10 In the Matter of:

Supreme Court No. R-17-0003

11 **PETITION TO AMEND RULES**
12 **803(16) AND 902 OF THE**
13 **ARIZONA RULES OF EVIDENCE**

14 **COMMENT OF**
15 **THE STATE BAR OF ARIZONA**

16 The Advisory Committee on Rules of Evidence has filed a Petition to amend
17 Rules 803(16) and 902 of the Rules of Evidence to mirror impending amendments
18 to the federal rules. The State Bar of Arizona (“State Bar”) supports the Petition.
19 The State Bar believes that the recommended changes to Rule 803(16) should be
20 accepted in their entirety. The State Bar believes that the recommended additions
21 of Rules 902(13) and (14) should also be accepted in their entirety, but believes
22 language should be added to the proposed comments to Rule 902 to clarify that the
23 “record” made available to the adverse party as part of the notice procedure should
24 generally include the electronically stored information’s metadata.
25

1 **I. The Recommended Changes to the Ancient Records Exception in Rule**
2 **803(16) Should Be Adopted.**

3 Rule 803(16) sets forth the ancient records exception to the hearsay rule,
4 namely that statements contained in documents that are least 20 years old and whose
5 authenticity is established are not excluded by the rule against hearsay. Because the
6 amount of electronically stored information (“ESI”) started to explode in the late
7 1990s (approximately 20 years ago), the federal Advisory Committee on Evidence
8 Rules investigated what this meant for the ancient records exception and explored
9 potential amendments. The federal advisory committee concluded that the primary
10 justification for the exception—the necessity to rely on more dubious evidence when
11 going back more than 20 years given the likelihood that all reliable evidence will
12 have been lost or destroyed—is substantially undermined by the prevalence of ESI.
13 Namely, the federal advisory committee concluded that the chances of reliable ESI
14 still existing in some form after all those years is significantly higher than the
15 chances of hard copy documents still existing. In addition, the chances of large
16 amounts of unreliable ESI still existing after 20 years are also much greater, which
17 could cause what has been up until now a relatively little-used exception to become
18 much more widely used—potentially leading to a proliferation of unreliable hearsay
19 coming in through this exception. In light of those findings, an amendment to the
20
21
22
23
24
25

1 federal rule is scheduled to go into effect on December 1, 2017, whereby the ancient
2 records exception is limited to documents that were prepared before January 1, 1998.
3

4 The State Bar concurs with the Petition's recommendation that the Court
5 adopt this amendment to Rule 803(16). The State Bar agrees that there is a legitimate
6 risk that, without an amendment to the ancient records exception, the proliferation
7 of ESI will lead to an unwarranted expansion of the ancient records exception. The
8 State Bar further agrees that the proposed amendment to Rule 803(16) will
9 ameliorate this risk while at the same time retaining the exception for those limited
10 cases where it is reasonably needed.
11
12

13 **II. The Recommended Additions of Rules 902(13) and 902(14) Regarding**
14 **ESI Should Be Adopted, But With an Addition to the Comments**
15 **Clarifying that Metadata Should Generally Be Provided to the Adverse**
16 **Party.**

17 Rule 902 sets forth various categories of self-authenticating documents. For
18 example, Rule 902(11) permits authentication of business records through the
19 certification of a qualified person, rather than requiring a live witness at trial to lay
20 foundation for the record. Rule 902(11) was adopted in the early 2000s because the
21 presentation at trial of foundation testimony for business records was usually pro
22 forma and perfunctory and did not justify the inconvenience, time, and expense
23

1 involved. Through the certification process, the burden shifts to the adverse party
2 to come forward with some evidence calling the authenticity of the record into doubt,
3 with notice to that adverse party required in order to give them a chance to meet that
4 burden.
5

6 The federal Advisory Committee on Evidence Rules determined that the same
7 cost-benefit analysis that led to Rule 902(11) justified use of the certification
8 procedure when authenticating certain forms of ESI. The federal advisory
9 committee concluded “that the expense and inconvenience of producing a witness
10 to authenticate an item of electronic evidence is often unnecessary. It is often the
11 case that a party goes to the expense of producing an authentication witness, and
12 then the adversary either stipulates authenticity before the witness is called or fails
13 to challenge the authentication testimony once it is presented.” *See* comment to
14 impending federal rule amendment. As a result, federal rules 902(13) (for records
15 generated by an electronic process or system) and (14) (for copies of ESI
16 authenticated by digital identification) are set to go into effect on December 1, 2017.
17
18 These impending rules adopt the same certification and notice procedure currently
19 available for business records under rule 902(11).
20
21
22
23
24
25

1 The Petition recommends adopting an identical amendment adding
2 subsections (13) and (14) to Arizona Rule 902. The petition further recommends
3 adopting some, but not all, of the federal comments to the additions of Rules 902(13)
4 and (14). The State Bar agrees with the petition’s recommendation, but believes that
5 language should be added to the proposed comments to clarify the “record” that is
6 to be provided to the adverse party during the notice process.
7

8
9 Because the justification for self-authentication of ESI is to “provide[] a
10 procedure under which the parties can determine in advance of trial whether a real
11 challenge to authenticity will be made” (*see* proposed comments to Rules 902(13)
12 and (14)), the State Bar believes that the comments to the amendment should clarify
13 that information reasonably necessary to allow the adverse party to analyze
14 authenticity must be provided with the certification. The State Bar believes that, in
15 the case of ESI, such information would normally include the metadata for the record
16 at issue. *See* THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS &
17 PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, at p. 61, cmt.
18 12.a (2d ed. June 2007) (noting potential importance of metadata in authenticating
19 ESI); *see also, e.g., Robinson v. City of Arkansas City*, 896 F. Supp. 2d 1020, 1031-
20
21
22
23
24
25

1 32 (D. Kan. 2012) (observing importance of metadata in examining authenticity of
2 an electronically generated document).

3
4 Proposed Rules 902(13) and (14) state that the procedures of Rules 902(11)
5 or (12) must be followed. Those rules state that the “record” being authenticated
6 must be provided to the adverse party along with the certification. The term “record”
7 is defined in Rule 101 as “includ[ing] a memorandum, report, or data compilation.”
8

9 While the State Bar believes that these provisions, when read in light of the purpose
10 behind the additions of Rules 902(13) and (14), should logically lead to the
11 conclusion that metadata is normally to be provided to the adverse party, the
12 comments to the amendments should clarify this to be the case. Therefore, the State
13 Bar recommends adding back in language found in the comments to the proposed
14 federal amendment about the potential need for technical information, with a
15 sentence added further clarifying that metadata should generally be provided as part
16 of the “record” disclosed to the adverse party. The paragraph the State Bar
17 recommends adding to the comments to Rules 902(13) and (14) would read as
18 follows:
19
20
21

22 In order to provide the adverse party with an opportunity to properly
23 analyze the issue of authenticity, the “record” provided by the

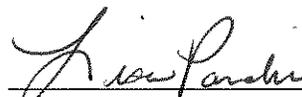
1 proponent of the ESI evidence must include the metadata for the
2 material in question if reasonably necessary to assess the material's
3 authenticity. In addition, a challenge to the authenticity of electronic
4 evidence may require technical information about the system or
5 process at issue, including 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.

6 Appendix A includes the proposed comments to Rules 902(13) and (14), with this
7 proposed additional language underlined.

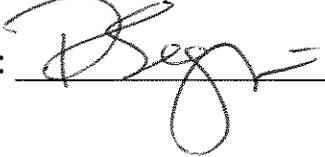
9 CONCLUSION

10 The State Bar supports the Petition filed by the Advisory Committee on Rules
11 of Evidence and believes that the Court should adopt its recommended amendments
12 to Rules 803(16) and 902. The State Bar does, however, believe that a paragraph
13 should be added to the comments to Rules 902(13) and (14) clarifying that metadata
14 and other technical information may be necessary to permit the adverse party to
15 properly analyze the authenticity of ESI. The recommended language is found in
16 Appendix A to this Comment.
17
18

19 RESPECTFULLY SUBMITTED this 22nd day of May, 2017.

20
21 
22 Lisa M. Panahi
23 General Counsel
24
25

1 Electronic copy filed with the
2 Clerk of the Arizona Supreme Court
3 this 22nd day of May, 2017.

4 by: 

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

APPENDIX A

Comment to 2018 Amendment Adding Subdivision (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 Court has determined 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.

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.

In order to provide the adverse party with an opportunity to properly analyze the issue of authenticity, the “record” provided by the proponent of the ESI evidence must include the metadata for the material in question if reasonably necessary to assess the material’s authenticity. In addition, 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.

Comment to 2018 Amendment Adding Subdivision (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 Court has determined 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 the person 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.

In order to provide the adverse party with an opportunity to properly analyze the issue of authenticity, the “record” provided by the proponent of the ESI evidence must include the metadata for the material in question if reasonably necessary to assess the material’s authenticity. In addition, 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.