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

IN THE SUPREME COURT
STATE OF ARIZONA

In the Matter of: **PETITION TO AMEND RULES 803(16) AND 902 OF THE ARIZONA RULES OF EVIDENCE**	Supreme Court No. R-17-0003 **COMMENT OF THE STATE BAR OF ARIZONA**

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

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

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

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

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

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

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

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

The federal Advisory Committee on Evidence Rules determined that the same cost-benefit analysis that led to Rule 902(11) justified use of the certification procedure when authenticating certain forms of ESI. The federal advisory committee concluded "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." *See* comment to impending federal rule amendment. As a result, federal rules 902(13) (for records generated by an electronic process or system) and (14) (for copies of ESI authenticated by digital identification) are set to go into effect on December 1, 2017. These impending rules adopt the same certification and notice procedure currently available for business records under rule 902(11).

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

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

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

Proposed Rules 902(13) and (14) state that the procedures of Rules 902(11) or (12) must be followed. Those rules state that the "record" being authenticated must be provided to the adverse party along with the certification. The term "record" is defined in Rule 101 as "includ[ing] a memorandum, report, or data compilation." While the State Bar believes that these provisions, when read in light of the purpose behind the additions of Rules 902(13) and (14), should logically lead to the conclusion that metadata is normally to be provided to the adverse party, the comments to the amendments should clarify this to be the case. Therefore, the State Bar recommends adding back in language found in the comments to the proposed federal amendment about the potential need for technical information, with a sentence added further clarifying that metadata should generally be provided as part of the "record" disclosed to the adverse party. The paragraph the State Bar recommends adding to the comments to Rules 902(13) and (14) would read as follows:

> 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.

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

CONCLUSION

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

RESPECTFULLY SUBMITTED this 22nd day of May, 2017.

Lisa M. Panahi
General Counsel

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

by: _____

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.