SUPREME COURT OF ARIZONA

In the Matter of	)	Arizona Supreme Court
	)	No. R-17-0003
RULES 803(16) AND 902,	)	
ARIZONA RULES OF EVIDENCE	)	
	)	**FILED 08/31/2017**
	)	
	)	
	)	

ORDER
AMENDING RULES 803(16) AND 902, ARIZONA RULES OF EVIDENCE

A petition having been filed proposing to amend Rules 803(16) and 902, Arizona Rules of Evidence, and comments having been received, upon consideration,

IT IS ORDERED that Rules 803(16) and 902, Arizona Rules of Evidence, be amended in accordance with the attachment hereto, effective January 1, 2018.

DATED this 31st day of August, 2017.

/s/
SCOTT BALES
Chief Justice

TO:
Rule 28 Distribution
Mark W Armstrong
Hon Samuel A Thumma
Lisa M Panahi

ATTACHMENT[1]

ARIZONA 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 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.

* * * * *

Comment to 2018 Amendment to Rule 803(16)

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

[1] Changes or additions in rule text are indicated by underscoring and deletions from text are indicated by ~~strikeouts~~.

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.

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).

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.

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).

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.