MAYER·BROWN

2017 Proposed Amendment to Federal Rule of Evidence 902

July 2017

Scenario

A multinational company is a defendant in a lawsuit that is expected to go to trial in 2018. The company believes that it will likely introduce evidence of web pages posted at various times, and wants to avoid the inconvenience of calling a live witness at trial to authenticate the web pages.

Authenticating Evidence at Trial

Generally, a party must produce sufficient evidence "to support a finding that the item is what the proponent claims it is" prior to introducing evidence into the record at trial. Fed. R. Evid. 901(a). Federal Rule of Evidence 902 provides that certain types of documents, such as government documents, certified copies of public records and newspapers, are self-authenticating and do not require extrinsic evidence of authenticity to be admitted at trial. Rules 902(11) and (12) also allow a party to rely on certification by a foundation witness to establish the authenticity of business records so long as the opponent is given a fair opportunity to challenge both the certificate and the underlying record.

Amendments to Federal Rule of Evidence Expand the Categories of Self-Authenticating Evidence

Proposed amendments to Rule 902 that are expected to take effect on December 1, 2017, will add two new paragraphs permitting a party to self-authenticate certain types of electronic evidence. The first, paragraph 13, will allow for self-authentication of a "record generated by an electronic process or system that produces an accurate result," such as a system registry report showing that an external device was connected to a computer. The second, paragraph 14, will allow for self-authentication of "[d]ata copied from an electronic device, storage medium, or file if authenticated by a process of digital identification," which will, among other things, permit self-authentication, using industry standard methodology, that a copy of an email is identical to the original email or that a forensic copy of cell phone text messages is identical to the original text messages. For evidence introduced under paragraph 13 or 14, a party will be required to provide certification by a foundation witness to establish the authenticity of the evidence, and the opposing party will have to be provided a fair opportunity to challenge both the certificate and the underlying record.

The intent of these amendments is to avoid the expense and inconvenience of calling on a witness at trial to certify the authenticity of electronic documents pursuant to Federal Rule of Evidence 901. The Advisory Committee found that "[i]t 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." Thus, proposed Federal

Rules of Evidence 902(13) and 902(14) will permit a party to avoid calling a live witness by providing, instead, a certificate by a qualified person certifying the authenticity of the electronic evidence.

Adopt Electronic Collection Best Practices to Benefit from the Amendments to Federal Rule of Evidence 902

Parties wishing to follow the new self-authentication rules should ensure that their electronic collections are conducted in a forensically sound manner. In most cases, this will mean either bringing in a forensics specialist to conduct the collection or appropriately supervising self-collections, including, for example, designing the collection protocol, using forensic copying tools and documenting the collection.

Collection best practices performed by a person qualified to attest to the accuracy or reliability of the process that produced an exhibit or to the facts establishing that the exhibit is an accurate copy can eliminate the need to call an authentication witness at trial. Adopting this approach can save time, expense and inconvenience at trial.

For inquiries related to this Tip of the Month, please contact Kristina Portner at kportner@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.