Admissibility of Evidence in Federal Court

HON. PAUL W. GRIMM, US DISTRICT COURT JUDGE, DISTRICT OF MARYLAND, AND GREGORY P. JOSEPH, JOSEPH HAGE ARONSON LLC, WITH PRACTICAL LAW LITIGATION

Is the item **relevant** under Federal Rule of Evidence (FRE) 401?

See Practice Note, Evidence in Federal Court: Basic Principles: Evidence Must Be Relevant.

**YES**

Is the item **excluded from evidence** by:

- The United States Constitution?
- A federal statute?
- The FRE, such as because the item is impermissible evidence of:
  - character or "bad acts" under FRE 404?
  - habit under FRE 406?
  - subsequent remedial measures under FRE 407?
  - a settlement agreement or negotiations under FRE 408?
  - a person or entity’s payment of another person’s medical or similar expenses under FRE 409?
  - plea negotiations under FRE 410?
  - liability insurance under FRE 411?
- Other rules prescribed by the United States Supreme Court?

(FRE 402.)

**NO**

The item is inadmissible.

Is the item **protected from disclosure** by either:

- The **attorney-client privilege**?
- The **work product doctrine**?

For more on the attorney-client privilege and the work product doctrine, see Attorney-Client Privilege and Work Product Doctrine Toolkit.

**YES**

The item is inadmissible.

**NO**

The item is inadmissible.
Is the item subject to judicial notice under FRE 201(b) or self-authenticating under FRE 902 because it is:

- A public record (FRE 902(1)-(4))?
- An official publication (FRE 902(5))?
- A newspaper, magazine, or similar publication (FRE 902(6))?
- A trade inscription (FRE 902(7))?
- A business record (FRE 902(11) and (12))? 

For more on judicial notice, see Practice Note, Evidence in Federal Court: Basic Principles: Exclusion of Relevant Evidence Under FRE 403.

A court is likely to exclude the item.

Does extrinsic evidence establish the item’s authenticity under FRE 901(b), such as:

- Testimony from a knowledgeable witness (FRE 901(b)(1))?
- Comparison to other authentic items (FRE 901(b)(3))?
- Distinctive characteristics (FRE 901(b)(4))?
- Public records or reports (FRE 901(b)(7))?
- Reliability of the process used to create the item (FRE 901(b)(9))?

For more on authentication through extrinsic evidence, see Using Documents as Evidence Checklist: Establishing Authenticity and Practice Note, E-Discovery: Authenticating Electronically Stored Information: Authenticating ESI Under FRE 901(b).

The item is inadmissible.
Does the item qualify for any of the following exceptions to the hearsay prohibition that are available regardless of the declarant's availability, such as because it is evidence of:

- A present sense impression (FRE 803(1))?
- An excited utterance (FRE 803(2))?
- A statement of then-existing mental, emotional, or physical condition (FRE 803(3))?
- A statement made for medical diagnosis or treatment (FRE 803(4))?
- A recorded recollection (FRE 803(5))?
- A record of regularly conducted activity or the absence of one (FRE 803(6), (7))?
- A public record or the absence of one (FRE 803(8)-(10))?
- Certain religious, personal, family, and history records and information (FRE 803(11)-(13), (19), and (23))?
- Certain property records and information (FRE 803(14)-(15), (20), (23))?
- A statement from an ancient document (FRE 803(16))?
- A market report or similar commercial publication (FRE 803(17))?
- A statement from a learned treatise, periodical, or pamphlet (FRE 803(18))?
- The reputation about a person's character (FRE 803(21))?
- A final judgment of conviction (FRE 803(22))?

For more on these exceptions, see Practice Note, Evidence in Federal Court: Basic Principles: Statement Regardless of Whether the Declarant is Unavailable (FRE 803) and Using Documents as Evidence Checklist: Overcoming Hearsay.
Admissibility of Evidence in Federal Court

Is the declarant unavailable to testify under FRE 804(a) and, if so, does the item qualify for any of the following additional exceptions to the hearsay prohibition, such as because it is evidence of:

- Prior testimony under oath (FRE 804(b)(1))? 
- A statement made under the belief of imminent death (FRE 804(b)(2))? 
- A statement against the declarant’s interest (FRE 804(b)(3))? 
- A statement of personal or family history (FRE 804(b)(4))? 
- A statement offered against a party that wrongfully caused the declarant’s unavailability (FRE 804(b)(6))? 

For more on these exceptions, see Practice Note, Evidence in Federal Court: Basic Principles: Hearsay Statements Requiring the Declarant to Be Unavailable (FRE 804) and Using Documents as Evidence Checklist: Overcoming Hearsay.

Does the item qualify for the residual hearsay exception under FRE 807?

For a more detailed discussion of this exception, see Practice Note, Evidence in Federal Court: Basic Principles: Residual Hearsay Exception Under FRE 807 and Using Documents as Evidence Checklist: Overcoming Hearsay.

The item is inadmissible.

Is the item a writing (including electronically stored information (ESI) under FRE 101(b)(6)), recording, or photograph offered to prove its contents under FRE 1002?

For more on the best evidence rule, see Practice Note, Evidence in Federal Court: Basic Principles: Best Evidence Rule and Using Documents as Evidence Checklist: Using the Best Evidence.

Is the item an original under FRE 1001(d) and 1002?

Is the item a duplicate under FRE 1001(e) and 1003?
Admissibility of Evidence in Federal Court

Do the circumstances make it unfair to admit a duplicate, or is there a genuine question about the original document's authenticity under FRE 1003?

Is the item "other evidence" of the writing, recording, or photograph's content (that is, neither an original nor a duplicate of the writing, recording, or photograph), and, if so, is one or more of the following true?

- All originals were lost or destroyed, but not due to the proponent's bad faith (FRE 1004(a)).
- An original is not available through any judicial process (FRE 1004(b)).
- The party against whom the item is offered had control of the original (or equally admissible duplicate) when the party knew of its evidentiary value, yet failed to produce it (FRE 1004(c)).
- The item is not closely related to a controlling issue (FRE 1004(d)).

The item is inadmissible.

The item is admissible and may be offered through a competent witness (FRE, Article VI).

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.
E-Discovery: Authenticating Common Types of ESI Chart

While all authentication methods recognized by the Federal Rules of Evidence (FRE) are available to authenticate electronically stored information (ESI), some methods apply to ESI more easily than others. This Chart provides a snapshot of the methods that counsel most often use to authenticate common types of ESI.

<table>
<thead>
<tr>
<th>FRE Rule</th>
<th>Emails and Text Messages</th>
<th>Chat Room or Instant Messages</th>
<th>Social Media Postings</th>
<th>Websites</th>
<th>YouTube, Voice-mail, and Other Audio and Video Recordings</th>
<th>Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRE 901(b)(1)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td>See Establish That a Recording is Unaltered</td>
<td>See Authenticate Databases</td>
</tr>
<tr>
<td>FRE 901(b)(3)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td>See Authenticate YouTube, Voicemail, and Other Audio and Video Recordings</td>
<td>See Authenticate Databases</td>
</tr>
<tr>
<td>FRE 901(b)(4)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td>See Authenticate YouTube, Voicemail, and Other Audio and Video Recordings</td>
<td>See Authenticate Databases</td>
</tr>
<tr>
<td>FRE 901(b)(5)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td>See Establish Speaker Identity</td>
<td>See Establish That a Recording is Unaltered</td>
</tr>
<tr>
<td>FRE 901(b)(9)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td>See Establish That a Recording is Unaltered</td>
<td>See Authenticate Databases</td>
</tr>
<tr>
<td>FRE 902(5)</td>
<td>See Authenticate Email and Text Messages</td>
<td>See Authenticate Chat Room or Instant Message (IM) Communications</td>
<td>See Authenticate Social Media Postings</td>
<td>See Authenticate Websites</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AUTHENTICATE EMAIL AND TEXT MESSAGES

To authenticate an email or text message, counsel may rely on:

- The testimony of a witness with personal knowledge that the message is what counsel claims it is (FRE 901(b)(1)). This witness may be:
  - the sender (or author) of the message; or
  - an individual who observed the sender writing the message (see United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012)).
- A comparison of the message with other authenticated evidence, such as another message that:
  - resembles the proffered message in a relevant manner; and
  - the court has found to be authentic. (FRE 901(b)(3); see United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).)
- Circumstantial evidence regarding the message’s:
  - appearance, such as the presence of the purported sender’s email address on the message;
  - content, such as information in the message known to a small group of people that includes the purported sender;
  - internal patterns, such as the use of the nicknames or other abbreviations in the message; or
  - other distinctive characteristics. (FRE 901(b)(4); see Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007).)
- The accuracy of the electronic recordation system (such as a server) to disprove a claim that a proffered message has been altered, which can be established by showing that:
  - all texts sent from the subject device are saved on a server; and
  - the server is secure, so files on the server cannot be edited or manipulated. (FRE 901(b)(9).)
- The message itself as a self-authenticating business record if a qualified person (such as the person who created the record, a person who developed and implemented the business practice that lead to its creation, or the records custodian) certifies that it was:
  - created by someone with knowledge of the subject event at or near the time of the event as part of an ordinary business activity; and
  - kept in the course of ordinary business activity. (FRE 803(6) and 902(11), (12).)

For more information on these authentication methods, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Ways to Authenticate ESI (w-002-6960).
For texts, the telephone number listed as the sender of the text is the purported sender's known telephone number or is a telephone number to which the purported sender had access at the relevant time; or

for texts, the sender's name (as stored in the recipient's phone and displayed on the face of the subject text) is the purported sender's name, initials, nickname, or moniker.

(FRE 901(b)(4).)

Details about the device on which the subject message was found, for example:

• the purported sender owned or possessed the device on which the messages were located (see United States v. Mebratuu, 543 F. App'x 137, 140-41 (3d Cir. 2013) and United States v. Lundy, 676 F.3d 444, 454 (5th Cir. 2012));

• the device contains other emails or texts that are linked to the purported sender by name, email address, phone number, or other information (see Mebratuu, 543 F. App'x at 140-41); or

• the device contains other messages for which authorship was sufficiently authenticated.

(FRE 901(b)(4).)

Forensic information that supports a finding that the purported sender sent the subject message, such as:

• an email's hash values (Lorraine, 241 F.R.D. at 546-47); or

• testimony from a forensic expert that the email or text metadata reveals that it was sent from a particular device when the purported sender possessed the device.

(FRE 901(b)(4).)

Information beyond the message itself, including that the purported sender:

• told the recipient to expect a message before its arrival;

• orally repeated the contents to the recipient soon after the message was sent;

• discussed the contents of the message with a third party; or

• acted according to (or in response to) the message.

(FRE 901(b)(4).)
• the purported sender discussed the same subject matter elsewhere.

(FRE 901(b)(4); see United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998).) The communication itself as a self-authenticating business record if a qualified person (such as the person who created the communication, a person who developed and implemented the business practice that lead to its creation, or the records custodian) certifies that it was:
• created by someone with knowledge of the subject event at or near the time of the event as part of an ordinary business activity; and
• kept in the course of ordinary business activity.

(FRE 803(6) and 902(11), (12).) Testimony from the recipient of the message, if the recipient can testify that she:
• knows that the purported sender uses the platform used to send the message;
• recognizes the account from which the message was sent and associates it with the purported sender; and
• finds the manner of communication consistent with prior communications from the purported sender.

(United States v. Barnes, 803 F.3d 209, 217 (5th Cir. 2015).) For more information on authentication under FRE 901(b) and 902, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Ways to Authenticate ESI (w-002-6960).

**AUTHENTICATE SOCIAL MEDIA POSTINGS**

To authenticate social media postings, counsel may rely on:

- Testimony from a witness with personal knowledge of the posting, such as testimony from:
  - the purported creator of the social network account and related postings; or
  - an individual who observed the purported creator establish or post to the page.

(FRE 901(b)(1).) Circumstantial evidence of authenticity, such as evidence that:
- the posting includes non-public details of the purported creator’s life, like biographical information or nicknames that are not generally known or accessible;
- the posting includes references or links to the purported creator’s loved ones, relatives, or co-workers;
- the posting includes content that only the purported creator (or a small group that includes the purported creator) knows;
- the posting includes photos, videos, or other content that the purported creator would likely post;
- the posting includes comments in the purported creator’s style or structure;
- the purported creator acted according to the contents of the post;

- the purported creator previously used the social media account to communicate with others;
- the purported creator knows the password to the account;
- the purported creator had exclusive access to the social media account (or the computer on which it was created) at the relevant time;
- the social media account is connected to the purported creator’s email account (see Brinson, 772 F.3d at 1320-21 and United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014));
- based on a forensic evaluation of the purported creator’s computer hard drive, the social media account was created or accessed on that computer; or
- the posting was made from a computer or device with an internet protocol address (IP address) associated with the purported creator.

(FRE 901(b)(4).) Evidence that the social media platform reliably and accurately tracks the account holder’s activity, such as:
- expert testimony on how a person accesses that type of social network account and what methods account holders may use to prevent unauthorized access; or
- evidence from the social networking website that connects the purported creator with the account.

(FRE 901(b)(9).) An argument that the posting is self-authenticating as a business record under FRE 902(11) or (12). Although establishing that a posting is a self-authenticating business record may support a finding that it is unaltered, it likely will not authenticate the post regarding the particular author (see Hassan, 742 F.3d at 134). For more information on how select courts evaluate the authenticity of social media posts, see Practice Note, Social Media: What Every Litigator Needs to Know: Authenticating Social Media (w-568-4085). For more information on authentication under FRE 901(b) and 902, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Ways to Authenticate ESI (w-002-6960).

**AUTHENTICATE WEBSITES**

To authenticate a website, counsel may:

- Request judicial notice, if the version depicted in the exhibit is identical to the current version of the website (FRE 201(b); and see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Judicial Notice (w-002-6960)).
- Rely on the website as self-authenticating, if it is:
  - a government website (FRE 902(5));
  - a newspaper or other periodical website (FRE 101(b)(6) and 902(6)); or
  - a website certified as business record by a qualified person (FRE 803(6) and 902(11), (12)).

For more information, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Self-Authenticating ESI Under FRE 902 (w-002-6960).
ESTABLISH DYNAMIC WEBSITE INFORMATION

When an exhibit depicting a website is not identical to the current version of the website, counsel must establish that the exhibit accurately depicts the website as it existed at the relevant time. Counsel may rely on:

- Testimony from the individual who created or was in charge of maintaining the website that the exhibit accurately reflects the webpage content at the relevant time (FRE 901(b)(1); St. Luke’s Cataract & Laser Inst., P.A. v. Sanderson, 2006 WL 1320242 (M.D. Fla. May 12, 2006)).
- Testimony from a witness who:
  - typed in the web address on the exhibit on the relevant date and time;
  - viewed the webpage’s contents; and
  - contends that the exhibit fairly and accurately reflects what she saw at that time.
(FRE 901(b)(1); Buzz Off Insect Shield, LLC v. S.C. Johnson & Son, Inc., 606 F. Supp. 2d 571, 594 (M.D.N.C. 2009).)

- Circumstantial evidence that:
  - the exhibit contains distinctive website design, logos, photos, or other images associated with the website or its owner;
  - the contents of the webpage are of a type ordinarily posted on that website or websites of similar people or entities;
  - the owner of the webpage has published some or all of the same contents elsewhere;
  - the contents of the webpage have been republished elsewhere and attributed to the website; or
  - the exhibit displays on its face the website address and a date and time stamp (Foreword Magazine, Inc. v. OverDrive Inc., 2011 WL 5169384, at *8-11 (W.D. Mich. Oct. 31, 2011)).
(FRE 901(b)(4).)

A printout from the Wayback Machine or similar website archival service that depicts how the website appeared on a particular date. Some courts require that counsel present a witness from the archival service to establish that it employs a process that produces accurate results (FRE 901(b)(9)). However, other courts take judicial notice of these sites (FRE 201(b)). For more information, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Archival Websites (w-002-6960).

For more information on authentication under FRE 901(b), see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Authenticating ESI Under FRE 901(b) (w-002-6960).

ESTABLISH THE CREATION DATE FOR WEBSITE CONTENT

If counsel must establish the date on which website content first appeared or when content was created, (rather than that the content was present on a site at a certain date or time), counsel may rely on:

- Testimony from a witness with knowledge of when the content (such as a video) was created (FRE 901(b)(1); see Sublime v. Sublime Remembered, 2013 WL 3863960 (C.D. Cal. July 22, 2013)).
- Circumstantial evidence related to the date on which the content was uploaded or created (FRE 901(b)(4); see United States v. Bloomfield, 591 F. App’x 847, 848-49 (11th Cir. 2014)).

For more information on authentication under FRE 901(b), see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Authenticating ESI Under FRE 901(b) (w-002-6960).

AUTHENTICATE YOUTUBE, VOICEMAIL, AND OTHER AUDIO AND VIDEO RECORDINGS

To authenticate YouTube, voicemail, and other audio and video recordings, counsel may rely on:

- A certification under FRE 803(6) that qualifies the recording as a self-authenticating business record, although many courts are reluctant to accept this method (FRE 902(11), (12); see Randazzo v. Cox, 2014 WL 1407378, at *4 (D. Nev. April 10, 2014) and Hassan, 742 F.3d at 133; see also Authenticate Email and Text Messages).
- A comparison of the recording with other authenticated evidence, such as another recording that:
  - resembles the proffered recording in a relevant manner; and
  - the court has found to be authentic.
(FRE 901(b)(3).)

- Circumstantial evidence (FRE 901(b)(4); see also Ciolino v. Eastman, 2016 WL 704449, at *2 (D. Mass. Jan. 6, 2016)).

- Evidence that:
  - the recording has not been altered (see Establish That a Recording is Unaltered); and
  - a particular individual is the speaker heard on the recording (see Establish Speaker Identity).

For more information on authentication under FRE 901(b) and 902, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Ways to Authenticate ESI (w-002-6960).

ESTABLISH THAT A RECORDING IS UNALTERED

To authenticate audio or video recordings and establish that the recording is unaltered, counsel may rely on:

- Witness testimony from an individual who:
  - overheard or observed the recording being made; and
  - confirms that the recording accurately reflects her observations and recollection.
(FRE 901(b)(1); see United States v. Castillo-Chavez, 555 F. App’x 389, 395-96 (5th Cir. 2014) and Leo v. L.I.R.R. Co., 307 F.R.D. 314, 321-22 (S.D.N.Y. 2015).)

- Evidence that the recording’s chain of custody is intact (FRE 901(b)(4); see McLaurin v. New Rochelle Police Officers, 439 F. App’x 38, 40 (2d Cir. 2011) and Bruins v. Osborn, 2016 WL 697109, at *1 (D. Nev. Feb. 19, 2016)).

- The reliability and accuracy of the recording device, which counsel may establish through testimony from the individual who operated the device that:
  - the recording device functioned properly;
• the individual operating the recording device was competent to do so; and
• the recording device reliably recorded audio content at the relevant time.

(FRE 901(b)(9).)

For more information on authentication under FRE 901(b), see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Authenticating ESI Under FRE 901(b) (w-002-6960).

ESTABLISH SPEAKER IDENTITY
To establish that a particular individual is the speaker in an audio or video recording, counsel may:

■ Rely on:
  • a comparison of the recording with other authenticated evidence (FRE 901(b)(3));
  • circumstantial evidence like that often used to authenticate social media postings (FRE 901(b)(4); see Authenticate Social Media Postings); or
  • testimony from a lay or expert witness familiar with the purported speaker’s voice who can identify her as the speaker in the recording (FRE 901(b)(5)).

■ Invite the judge or jury to compare the recorded voice with the purported speaker’s voice, if the judge or jury is familiar with the speaker’s voice (FRE 901(b)(5); see Ricketts v. City of Hartford, 74 F.3d 1397, 1410 (2d Cir. 1996)).

AUTHENTICATE DATABASES
Litigants often locate and produce relevant database information by running a query to locate relevant database records and then producing a report of the query result. To authenticate the report, counsel must authenticate both:

■ The contents of the report by relying on:
  • testimony from a witness with personal knowledge of the content (FRE 901(b)(1)); or
  • a certification sufficient to qualify the content as a self-authenticating business record (FRE 803 and 902(11), (12); see Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627, 632 (2d Cir. 1994)).

■ The query and report process by relying on either:
  • testimony from a witness with knowledge of the database system, such as how information is uploaded to the database or how queries are run to find information residing in the database; or
  • evidence that the company relied on the database in conducting its business, which indicates that the database was sufficiently accurate.


For more information on authentication under FRE 901(b) and 902, see Practice Note, E-Discovery: Authenticating Electronically Stored Information: Ways to Authenticate ESI (w-002-6960).
Electronically stored information (ESI) poses unique authentication challenges for counsel, given the varying approaches courts have taken when authenticating different forms of digital evidence. To avoid this uncertainty, counsel often try to authenticate ESI through proactive, cooperative methods. However, because these methods are not always available, counsel must understand how digital evidence can be formally authenticated in federal court.
Judge Grimm was appointed to the District Court in 2012, and previously served as Chief Magistrate Judge for the District of Maryland. In 2009, Judge Grimm became a member of the Advisory Committee for the Federal Rules of Civil Procedure where he served as Chair of the Discovery Subcommittee until September 2015. He is a member of the American Law Institute, and has been an adjunct professor of law at the University of Baltimore School of Law and the University of Maryland School of Law, teaching courses on evidence and discovery, and he has written extensively on both topics.

Gregory previously served as President of the American College of Trial Lawyers, Chair of the Section of Litigation of the American Bar Association, and a member of the Advisory Committee on the Federal Rules of Evidence. He has tried cases involving disputes over securities fraud, takeovers, intellectual property, corporate governance, fiduciary duty, federal taxation, tort, and contract.
Under the Federal Rules of Evidence (FRE), a court may not admit an item into evidence for purposes of trial or summary judgment unless the evidence is authenticated and satisfies certain additional criteria. Digital evidence derived from ESI presents complex authentication challenges because, unlike paper records and other tangible evidence, ESI can be easily replicated and tampered with in numerous ways. Although the same authentication and admissibility standards govern traditional evidence and ESI, technological evolution has led courts to adopt varying approaches to authenticating different forms of digital evidence. In short, there is no “one-size-fits-all” authentication method for ESI. Like traditional evidence, courts and juries ultimately will consider a variety of factors in their analyses.

To minimize risk, counsel often try to authenticate ESI before a hearing or trial through requests for admission or by seeking a stipulation from opposing parties as to authenticity. However, because these proactive, cooperative methods are not always available, counsel should be well-versed on the formal methods for authenticating various types of ESI.

THE AUTHENTICATION STANDARD

FRE 901(a) generally requires a party proffering evidence (a proponent) to authenticate it by providing enough supplemental evidence to establish that the proffered evidence is what the proponent claims it is (see, for example, Hutchens v. Hutchens-Collins, 2006 WL 3490999, at *2 (D. Or. Nov. 30, 2006)). The same authentication standard applies to both ESI and traditional forms of evidence (see Lebewohl v. Heart Attack Grill LLC, 890 F. Supp. 2d 278, 298 (S.D.N.Y. 2012); Foreword Magazine, Inc. v. OverDrive, Inc., 2011 WL 5169384, at *3 (W.D. Mich. Oct. 31, 2011)).

The FRE 901(a) authentication standard is not particularly rigorous. A court need only find that there is sufficient evidence for a reasonable jury to conclude that the proffered evidence is what the proponent claims it is. The rule does not require a court to conclude that the proffered evidence actually is what the proponent claims it is. For example, if an opponent challenges the authenticity of ESI evidence by raising the possibility that a party or non-party altered the ESI, FRE 901(a) does not require the proponent to disprove that possibility before the ESI may be deemed authentic. (See Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287, 337 (E.D.N.Y. 2015).)

AUTHORITY TO MAKE AUTHENTICATION DECISIONS

FRE 104 dictates when the judge decides admissibility and when that issue is passed on to the jury. Because authenticity is a required element of admissibility, the rule likewise governs whether the judge or jury determines if a proponent sufficiently authenticated the ESI.

JUDICIAL DETERMINATIONS UNDER FRE 104(a)

A judge must admit ESI under FRE 104(a) when:

- After considering all non-privileged evidence related to the ESI’s authenticity, the judge either:
  - finds enough evidence that a reasonable jury could find that the ESI is what the proponent claims it is; or
  - does not find sufficient evidence to support a finding that the ESI is something other than what the proponent claims it is.

- The ESI satisfies all other admissibility requirements.

Once admitted into evidence, the jurors may give the ESI whatever weight they think it deserves.

Conclusory or hypothetical objections, such as speculation that the ESI could possibly be something other than what the proponent claims it is, are not evidence and therefore do not factor in to the judge’s authentication analysis. For example, if opposing counsel object to ESI as improperly or insufficiently authenticated, that objection has no bearing on the judge’s authentication analysis unless opposing counsel offer actual evidence that either:

- Disputes the proponent’s authentication evidence.
- Otherwise supports a finding that the ESI is something other than what the proponent claims it is.

In practice, judges unilaterally make the majority of admissibility decisions (including authentication determinations) under FRE 104(a), including through decisions on motions in limine.

JURY DETERMINATIONS UNDER FRE 104(b)

FRE 104(b) speaks to admissibility broadly, but it applies equally to authentication as an element of the admissibility analysis. In some circumstances, analyzing authenticity (and ultimately admissibility) is complicated because both:

- The proponent offers evidence that is sufficient to support a finding that the ESI is what the proponent claims it is.
- Another party offers evidence sufficient to support a finding that the ESI is not what the proponent claims it is.

In other words, the identity or nature of the ESI might be a disputed fact. In this situation, the judge may not simply find that the proponent satisfied FRE 901(a) and, assuming the ESI satisfies...
all other admissibility requirements, unilaterally admit the ESI for the jury’s consideration under FRE 104(a). Rather, the judge may only conditionally admit the ESI into evidence under FRE 104(b).

When a judge conditionally admits ESI because the parties offer conflicting evidence on the ESI’s authenticity, the judge also must:

- Allow the jury to review the ESI.
- Allow the jury to hear all evidence supporting and disputing the ESI’s authenticity.
- Instruct the jurors that if they find by a preponderance of the evidence that the ESI is:
  - what the proponent claims it is, they should deem the ESI admitted and consider it during their deliberations; and
  - something other than what the proponent claims it is, the ESI is irrelevant and inadmissible, and they may not consider it during their deliberations.

**ESI AUTHENTICATION METHODS**

As discussed above, the same authentication rules and standards apply to both traditional forms of evidence, such as hard-copy documents, and ESI. However, certain authentication methods work better for ESI than others (see Box, Authenticating Common Types of ESI). These include:

- Providing supplemental authentication evidence under FRE 901(b).
- Establishing that the evidence is self-authenticating under FRE 902.
- Requesting judicial notice under FRE 201(b).
- Seeking a ruling from the court that the opposing party conceded the ESI’s authenticity by producing it in discovery.

**PROVIDING SUPPLEMENTAL EVIDENCE UNDER FRE 901(b)**

FRE 901(b) provides a non-exhaustive list of evidence that a proponent can use to authenticate ESI (see Bury v. Marietta Dodge, 692 F.2d 1335, 1338 (11th Cir. 1982); Fin. Co. of Am. v. BankAmerica Corp., 493 F. Supp. 895, 900 (D. Md. 1980)).

A proponent also does not need to simultaneously proffer all of the evidence identified in FRE 901(b) to establish the authenticity of any particular ESI.

Under FRE 104(a), the judge may consider the proffered evidence as part of the authentication analysis even if the evidence is inadmissible, so long as it is not subject to privilege. Of the examples noted in FRE 901(b), to authenticate ESI, proponents most commonly use evidence based on:

- Testimony from a witness with personal knowledge.
- Testimony describing the process or system used to generate the ESI.
- Comparisons to previously authenticated evidence.
- Other circumstantial evidence showing the ESI’s authenticity.

**Personal Knowledge Evidence**

Testimony from a witness with personal knowledge that the proffered ESI is what the proponent claims is a common form of authentication evidence (FRE 901(b)(1)). For example, a proponent can authenticate:

- An email, through the author’s testimony that she sent the email (see Anderson v. United States, 2014 WL 6792129, at *4-5 (N.D. Ga. Dec. 2, 2014)).
- A chat room transcript, through a participant’s testimony that the transcript accurately represents the exchange (see United States v. Browne, 834 F.3d 403, 413-15 (3d Cir. 2016)).
- A social media posting, through the testimony of a witness who observed the purported author writing and posting the subject content.
- Database content, through testimony from the employee who entered the subject content.

Similarly, a proponent can authenticate an audio recording by offering testimony from a witness who is familiar with and can identify the speaker’s voice (FRE 901(b)(5); see United States v. Hemmings, 482 F. App’x 640, 643 (2d Cir. 2012)).
Process or System Evidence

Testimony describing the process or system used to generate ESI and establishing that the process or system produces an accurate result can authenticate the generated ESI (FRE 901(b)(9)). For example, a proponent can authenticate:

- A text message, through testimony from an information technology professional who knows that the subject message was collected from a server that is inaccessible to users and renders the stored messages unalterable (see United States v. Kilpatrick, 2012 WL 3236727, at *3 (E.D. Mich. Aug. 7, 2012)).
- A social media posting, through expert testimony about how the social media platform reliably and accurately tracks account access and activity.
- A previous version of a website, by proffering both:
  - a printout from an archival website (see below Archival Websites); and
  - a witness from the archival website who can testify on the accuracy and reliability of their archival and retrieval practices.
  
- An audio or a video recording, through testimony from the recording device operator that she is competent to operate the device and the device reliably recorded the content at the relevant time (see Leo v. Long Island R.R. Co., 307 F.R.D. 314, 316 (S.D.N.Y. 2014)).

Comparison Evidence

A comparison of the proffered ESI with an authenticated specimen by an expert witness or the fact finder can serve to authenticate the ESI (FRE 901(b)(3)). For example, a proponent can authenticate a text message by asking the judge to compare the proffered text with a text that the court previously recognized as authentic under FRE 901(a).

Circumstantial Evidence

A proponent can use circumstantial evidence, such as the appearance, contents, substance, internal patterns, or other distinctive characteristics of the ESI, for authentication purposes (FRE 901(b)(4)). The significance of these factors might differ if the authenticity dispute relates to the identity of the sender or the recipient. For example, a proponent can authenticate:

- An email, by offering evidence that:
  - the purported author is known to use the email address listed in the “From” header field;
  - the email body includes facts known to a small group of people that includes the purported author; or
  - the signature block at the end of the email contains the purported author’s name, title, and company logo.
  

- A video recording, by offering evidence that it contains non-public details of the purported creator’s life, such as nicknames that are not generally known or accessible.

A proponent also can authenticate a website under FRE 901(b)(4) by offering evidence that it contains distinctive website design, logos, photos, or other images associated with the website or its owner (see Metcalf v. Blue Cross Blue Shield of Mich., 2013 WL 4012726, at *10 (D. Or. Aug. 5, 2013); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002)).

ESTABLISHING ESI AS SELF-AUTHENTICATING UNDER FRE 902

FRE 902 identifies types of evidence that do not require supplemental, extrinsic authentication evidence, based on long-standing assumptions about the trustworthiness of certain types of documents. For example, courts have found the following types of ESI self-authenticating under FRE 902:

- Website publications, including books and pamphlets, purportedly issued by a public authority (FRE 902(5); see Williams v. Long, 585 F. Supp. 2d 679, 685-690 (D. Md. 2008) (finding that printed webpages from branches or subdivisions of the Maryland state government were self-authenticating as official publications); EEOC v. E.I. Du Pont de Nemours & Co., 2004 WL 2347559, at *2 (E.D. La. Oct. 18, 2004) (finding that printed webpages from the US Census Bureau, a government website, were self-authenticating as official publications)).
- Online publications purporting to be newspapers or periodicals (FRE 902(6); see Davis v. Hous. Auth. of Birmingham, 2015 WL 1487199, at *2 (N.D. Ala. Mar. 31, 2015) (noting that an article from an online news outlet is analogous to a traditional newspaper article and holding that the article was self-authenticating); but see Specht, 758 F. Supp. 2d at 582 (holding that an article appearing on forbes.com was not self-authenticating under FRE 902(6) because forbes.com was not a printed newspaper or periodical)).
- Online, certified copies of domestic or foreign records of regularly conducted activities, such as a company’s policies and procedures (FRE 902(11)-(12); see Intermarine, LLC v. Spliethoff Bevrachtingskantoor, B.V., 123 F. Supp. 3d 1215, 1218 (N.D. Cal. 2015) (noting that the portions of Dropbox’s website regarding its business and practices are self-authenticating under FRE 902(11))).
### Authenticating Common Types of ESI

<table>
<thead>
<tr>
<th></th>
<th>Emails and Text Messages</th>
<th>Chat Room or Instant Messages</th>
<th>Social Media Postings</th>
<th>Websites</th>
<th>YouTube, Voicemail, and Other Audio and Video Recordings</th>
<th>Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FRE 901(b)(1)</strong> (Witness with personal knowledge)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>FRE 901(b)(3)</strong> (Comparison with other authenticated evidence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>FRE 901(b)(4)</strong> (Circumstantial evidence)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>FRE 901(b)(5)</strong> (Opinion about a voice)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>FRE 901(b)(9)</strong> (Process or system evidence)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>FRE 902(5)</strong> (Self-authenticating official publications)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>FRE 902(6)</strong> (Self-authenticating newspapers and periodicals)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>FRE 902(11) and (12)</strong> (Self-authenticating certified records of regularly conducted activity)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Judicial Notice</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Production in Discovery</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
REQUESTING JUDICIAL NOTICE UNDER FRE 201(b)

When ESI’s authenticity is not subject to reasonable dispute, a court may take judicial notice and admit the ESI into evidence (FRE 201(b)). Judicial notice saves the proponent the time and expense of gathering resources and presenting evidence on the ESI’s authenticity, and may be taken at any time, including on appeal.

A proponent should consider asking a court to take judicial notice of the authenticity of ESI, particularly where the ESI involves:

- Government websites.
- Select non-governmental websites.
- Archival websites.
- GPS data.

Government Websites

Courts often take judicial notice of government website postings based on their view that this evidence is presumptively accurate and reliable (see Denius v. Dunlap, 330 F.3d 919, 926-27 (7th Cir. 2003); United States v. Head, 2013 WL 5739095, at *3 n.2 (E.D. Cal. Oct. 22, 2013)). For example, courts have taken judicial notice of evidence from:

- Court websites (see Feingold v. Graff, 516 F. App’x 223, 226 (3d Cir. 2013) (taking judicial notice of an attorney’s disciplinary record as posted on the Supreme Court of Pennsylvania website)).
- Department websites (see Flores v. City of Baldwin Park, 2015 WL 756877, at *2 (C.D. Cal. Feb. 23, 2015) (taking judicial notice of a printout showing information from a municipal police department website)).

Court cases also may extend this presumption of reliability to evidence found on:

- Foreign government websites (see United States v. Broxmeyer, 699 F.3d 265, 296 n.32 (2d Cir. 2012) (taking judicial notice of content on the Brazilian and Vietnamese government websites)).
- International or quasi-governmental organization websites (see Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351, 1367 (2013) (taking judicial notice of information on the World Bank website)).

Select Non-Governmental Websites

Courts are more likely to take judicial notice of reference websites that represent online versions of reputable, print sources that courts historically have been willing to judicially notice. For example, courts have taken judicial notice of:

- Maps and geographic data from websites like Google Maps and MapQuest (see McCormack v. Hiedeman, 694 F.3d 1004, 1008 n.1 (9th Cir. 2012) (holding that Google Maps’ accuracy could not reasonably be questioned); Cline v. City of Mansfield, 745 F. Supp. 2d 773, 801 n.23 (N.D. Ohio 2010) (taking judicial notice of the time of the sunset on a particular date as stated on timeanddate.com)).
- The publication of newspaper and periodical articles (see Ford v. Artiga, 2013 WL 3941335, at *7 n.5 (E.D. Cal. July 30, 2013) (taking judicial notice of the publication of newspaper articles but not the truth of their content); HB v. Monroe Woodbury
Online versions of textbooks, dictionaries, rules, and charters, © 2017 Thomson Reuters. All rights reserved.

F. Supp. 2d 968, 973 (W.D. Mich. 2003), aff’d, 270 United States ex rel. Dingle v. BioPort Corp. on Wikipedia); 2012) (declining to take judicial notice of information contained, 861 F. Supp. 2d 1099, 1104 n.4 (S.D. Cal. 2013); Martins v. 3PD, Inc., 2013 WL 1320454, at *16 n.8 (D. Mass. Mar. 28, 2013)). However, judicial notice typically is limited to the content that appeared on a website on a given date, as courts rarely take judicial notice of either:

- The truth of the archived website’s content, unless the website is a government website or a non-governmental website of the sort that courts consider sufficiently trustworthy (see above Select Non-Governmental Websites).
- Images or links in the archived websites, because the depiction of images and function of links are less reliable in archived versions.

Other courts have authenticated archived versions of websites only when they are accompanied by witness testimony regarding the archival service’s process and reliability (see Specht, 747 F.3d at 933 (requiring testimony from a witness with personal knowledge of the archival service’s reliability, rather than testimony from only the website creators, asserted from memory, that the archived screenshot reflected how the websites looked at the relevant time); United States v. Bansal, 663 F.3d 634, 667 (3d Cir. 2011) (finding an archived website image to be authentic based on testimony about the archival service’s reliability and testimony that compared the archived screenshot with other authenticated images of the subject website at a later time)).

GPS Data

 Courts have taken judicial notice of GPS data based on the overall reliability, frequency of use, and wide availability of GPS devices (see United States v. Brooks, 715 F.3d 1069, 1078 (8th Cir. 2013) (affirming the district court’s judicial notice of data from a GPS tracker that a teller placed in an envelope of stolen money during a bank robbery)).

SEEKING CONCESSION OF AUTHENTICITY BASED ON PRODUCTION

A proponent can proffer ESI that an opposing party produced in discovery. However, the opposing party might object to the authenticity of the ESI. Some courts have broadly held that a party that produces ESI in discovery implicitly concedes the ESI’s authenticity (see EEOC v. Fred Meyer Stores, Inc., 954 F. Supp. 2d 1104, 1117 (D. Or. 2013) (holding that ESI produced in discovery by one party is deemed authentic when the opposing party proffers
it as evidence); Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 397 (D. Conn. 2008), aff’d, 587 F.3d 132 (2d Cir. 2009) (holding that ESI was authentic by virtue of the act of production)).

Other courts have considered the fact that the objecting party produced the ESI as one of several factors in the authenticity analysis (see, for example, Gallegos v. Swift & Co., 237 F.R.D. 633, 641 (D. Colo. 2006) (the proponent established authenticity with sufficient circumstantial evidence by showing that the opposing party produced the evidence and much of it contained either corporate letterhead or the company officials’ signatures)).

However, several courts have found that production implies authenticity only for ESI produced in response to sufficiently specific requests for production. These courts are less likely to find that a producing party concedes the authenticity of ESI it produces in response to a broad request for all documents in its possession, custody, and control on a particular topic. Typically, these courts conclude that production in this context is not an endorsement that a document is what it appears to be on its face, but instead is only a representation that the ESI:
- Was in its possession, custody, or control.
- Relates to the particular topic.

Courts take this position because parties often have ESI in their possession, custody, or control that originated from other sources, such as ESI obtained from a third party in response to a subpoena. These parties typically are not in a position to verify that other entities’ ESI actually is what it appears to be on its face.

However, the opposite is true when a party produces ESI in response to a more specific request, such as a request to produce its own business records on a particular topic. In this circumstance, the producing party typically is best positioned to authenticate its own ESI because the party has firsthand knowledge of how, when, and why it created the ESI. By contrast, a party generally is less familiar with ESI that it obtained from an outside source. For these reasons, courts are more likely to find that a producing party implicitly authenticates ESI when it produces the ESI in response to a targeted request for its own records.

Several courts have found that production implies authenticity only for ESI produced in response to sufficiently specific requests for production. These courts are less likely to find that a producing party concedes the authenticity of ESI it produces in response to a broad request.