Strafford

Presenting a live 90-minute webinar with interactive Q&A

FRE 902(13) and (14): Self-Authentication of ESI, Best Practices From 2021 Sedona Commentary on Admissibility

WEDNESDAY, APRIL 21, 2021

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

David R. Cohen, Partner, **Reed Smith**, Pittsburgh

Dennis I. Wilenchik, Member, **Wilenchik & Bartness**, Phoenix

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

FRE 902(13) and (14): Self-Authentication of ESI, Best Practices From 2021 Sedona Commentary on Admissibility

April 21, 2021

Strafford

Speakers

David R. Cohen

Reed Smith, LLP
Pittsburgh, PA

- **Partner and Chair of Reed Smith's Records & E-Discovery Group**
- **30+ years of commercial litigation experience**
- **Serves as special e-discovery counsel, represents companies in complex litigation matters, counsels clients on EDRM and litigation readiness.**

Dennis I. Wilenchik

Wilenchik & Bartness, P.C.
Phoenix, AZ

- **Founder and Managing Partner**
- **Former senior litigation partner at Storey & Ross and Squire, Sanders & Dempsey, and former deputy attorney, Maricopa County, Arizona**
- **Civil litigator with more than 30 years of trial experience and his practice focuses on complex commercial litigation with an emphasis on real estate and business**

Streamlining Authentication

"This approach makes sense for hard drives, flash drives, as well as data stored in copy machines, fax machines, and other commonly used devices that register a history of activity—that data is not really subject to human manipulation, and is the type of routinely generated data where the accuracy of it is highly reliable."

Anthony J. Carriuolo, Esq.

Co-Chair of Social Media & Website Subcommittee

ABA Section of Litigation's Business and Torts and Unfair Competition Committee

Prior Federal Rule of Evidence 902

Rule 902. Evidence that is Self-Authenticating

Provides that enumerated example items of evidence are self-authenticating, not requiring oral testimony in order to be admitted, including:

- Records kept in the ordinary course of business and certified
- Official government publications or certified public records
- Sealed and/or notarized documents
- Published newspapers and periodicals

For many years, Rule 902 has been routinely relied upon by trial attorneys in civil and criminal matters


DIGITAL EVIDENCE

What is Computer-Generated Evidence?

- It is Electronically Stored Information ("ESI"), which is "information that is stored electronically on [in]numerable types of media regardless of the original format in which it was created." https://www.edrm.net/glossary/esi-electronically-stored-information/

- Under FRCP 34(a)(1)(A): "[A]ny designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."

The Digital Revolution

- 2.5 quintillion bytes of data are created every day, which is expected to accelerate greatly with the growth of the Internet of Things ("IoT").
- IOT has evolved from machine-to-machine to human-to-machine. Every person generates 1.7 megabytes in just a second.
- The big data analytics market is set to reach $103 billion by 2023
- Poor data quality costs the US economy up to $3.1 trillion yearly
- 95% of businesses cite the need to manage unstructured data as a problem for their business.
- 97.2% of organizations are investing in big data and AI.
- Google processes over 40,000 search queries every second on average, which translates to over 3.5 billion searches per day and 1.2 trillion searches per year worldwide.

Source: Petrov, C. (2021, March 18). 25+ Impressive Big Data Statistics for 2020. Tech Jury. https://techjury.net/blog/big-data-statistics/

The Internet of Things ("IoT")

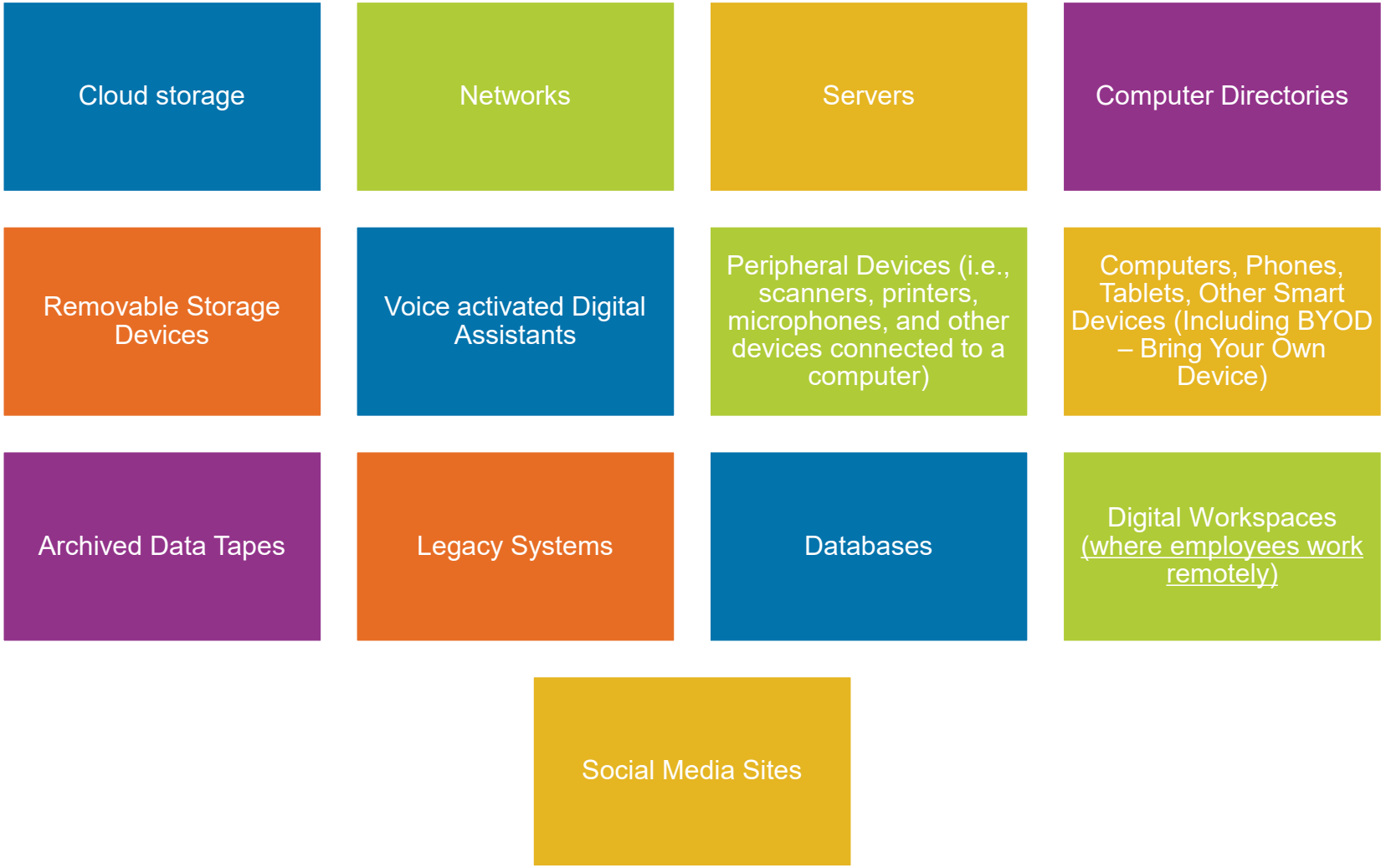
- IoT is a system of interrelated computing devices which transfer data over a network without requiring human-to-human interaction.
- According to a Juniper Research report, the number of IoT devices in 2021 will reach 46 billion. For comparison, this is a 200% increase compared to 2016.
- The thing could be a human with a heart monitor implant or a man-made object like an automobile with built-in sensors; coffee makers; washing machines; printers.
- Devices operate in the background and transmit your personal data, which has led to an entirely new area of evidence-gathering and will require you to know how to gather that information to ensure that it is admissible in court.

Multiple Forms of ESI

ESI Includes:

- ✓ Emails
- ✓ Word processing documents
- ✓ Spreadsheets
- ✓ Digital photos
- ✓ Videos
- ✓ Voicemails and audio files
- ✓ Text messages
- ✓ Call logs & calendar entries
- ✓ Database contents
- ✓ Internet activity/research
- ✓ Collaboration platform messages (Teams, Slack, etc.)
- ✓ Video call recordings (e.g. Zoom)

ESI Sources


Cloud storage
Networks
Servers
Computer Directories
Removable Storage Devices
Voice activated Digital Assistants
Peripheral Devices (i.e., scanners, printers, microphones, and other devices connected to a computer)
Computers, Phones, Tablets, Other Smart Devices (Including BYOD – Bring Your Own Device)
Archived Data Tapes
Legacy Systems
Databases
Digital Workspaces (where employees work remotely)
Social Media Sites

Amendments to Rules 902(13) and (14), Federal Rules of Evidence, Effective Dec. 1, 2017

Replaces in-person testimony to establish authenticity.

Permits authentication of ESI by an affidavit by a "qualified person."

The affidavit must certify that the record also falls within the requirements of Rules 902(11) and (12).

Amendment to Federal Rule of Evidence 902(13)

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).

Self-Authenticating Evidence Under the New Amendments

Rule 902(13):

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).

Rule 902(14):

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 must also meet the notice requirements of Rule 902(11).

Amendment to Federal Rule of Evidence 902(14)

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 must also meet the notice requirements of Rule 902(11).

Federal Rule of Evidence 902(13) and (14) – "Qualified Person" Definition

Certification Requirements

- Written affidavit by "qualified person"

Committee Note:

"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 certificate provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule."

“Qualified Witness,” 803(6), FRCP

Bank of America v. Aliante Master Association, 2019 WL 1441604, at *5 (D. Nev. Mar. 31, 2019): On summary judgment, Court found that an affidavit submitted by an employee of B of A’s counsel personally confirmed the computerized documents’ accuracy. The court found that counsel’s employee qualified as “someone with knowledge” and it was not necessary that the affiant be an employee or someone with knowledge about how computerized records were made or maintained. Documents attached to the affidavit were sufficiently authenticated. Citing *ABS Entm't, Inc. v. CBS Corp.,* 908 F.3d 405, 426 (9th Cir. 2018).

Amendment to Federal Rule of Evidence 902(13)

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).**

Amendment to Federal Rule of Evidence 902(14)

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 must also meet the notice requirements of Rule 902(11).**

Certification Requirements Referenced in New Amendments – Domestic Records

Rule 902. Evidence that is Self-Authenticating

* * *

(11) Certified Domestic Records of a Regularly Conducted Activity. The original or a copy of a domestic record that meets the requirements of **Rule 803(6)(A)-(C)**, as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them.

Certification Requirements Referenced in New Amendments – Hearsay Exceptions

Rule 803. Exceptions to the Rule Against Hearsay

* * *

(6) Records of a Regularly Conducted Activity. A record of an act, event, condition, opinion, or diagnosis if:

(A) the record was made at or near the time by — or from information transmitted by — someone with knowledge;

(B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;

(C) making the record was a regular practice of that activity

Certification Requirements Referenced in New Amendments – Foreign Records

Rule 902. Evidence that is Self-Authenticating

* * *

(12) Certified Foreign Records of a Regularly Conducted Activity. In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification, rather than complying with a federal statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11).

Certification Requirements Referenced in New Amendments – Case Law

United States v. Adams, No. 15-0580, (E.D. Pa. Jan. 16, 2019)

- Defendant contended that the Government improperly relied on 902(13) to introduce evidence of text messages recovered from Defendants' cell phone "without calling a qualifying witness"
- Defendant argued that certification under Rule (13) requires the moving party to comply with the certification requirements under Rules 902(11) and 902(12) as they "relate respectively to certified domestic records of a regularly conducted activity and certified foreign records of regularly conducted activity, which the subject text messages clearly are not."

Certification Requirements Referenced in New Amendments – Case Law

United States v. Adams, No. 15-0580, (E.D. Pa. Jan. 16, 2019)

- The Court noted that, “Rule 902(13) only requires certification comply with the certification requirements of Rule 902(11) and 902(12) and not the business or foreign record requirements of those rules.”
- Rule 902(13) advisory notes state: 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.

Retrieval from Computer Files

- The ESI retrieved from computer files must be the same one as originally had been entered into its computer.
  - "In the case of a paper record, the inquiry is into the procedures under which the file is maintained, including custody, access, and procedures for assuring that the records in the files are not tampered with. The foundation is well understood and usually is easily established. *See* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[1] (5th ed. 2002); 5 WEINSTEIN § 900.07[1] [b] [i]; American Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee), 336 B.R. 437, 444-445, 2005 Bankr. LEXIS 2602, *13-14.
- The same is true for ESI: the entity's policies and procedures for the use of the equipment, database, and programs, how the database is controlled and how the original program was accessed are important questions. Changes to the database, was it backed up, logged, recorded, audited, all become important in determining the originality of the ESI.

Retrieval from Computer Files

Courts, however, may determine that the ESI presented may more appropriately be directed to the weight a jury would give to the evidence, not its authenticity.

- Possibility of alteration does not and cannot be the basis for excluding emails as unidentified or unauthenticated as a matter of course. *United States v. Safavian,* 435 F.Supp.2d 36, 40–41 (D.D.C.2006).

- Foundation for a computer generated business record did not require the maker of the record, or custodian; a witness qualified to explain the record keeping system of organization is enough. *United States v. Kassimu*, 2006 WL 1880335 (5th Cir.2006).

- Computerized check-in and reservation records admissible as business records; data reflected in the printouts was kept in the ordinary course of the business. *United States v. Fujii*, 301 F.3d 535 (7th Cir.2002).

Notice Requirements Referenced in New Amendments

Notice Requirement of Rule 902(11)

"Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them."

Committee Note on Challenge to Authenticity:

"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 at trial."

Impact of Rules 902(13) and (14)

Purpose of New Rules

- Allow easier authentication of electronic evidence
  - Eliminates need for a separate authentication witness
  - Shifts burden for raising authenticity issues
- Rule only addresses authentication of the evidence
  - Does not establish accuracy (of underlying facts)
  - Does not establish relevance
  - Does not establish ownership or control
  - Does not overcome other hearsay objections

Benefits and Limitations of Certifications Under 902(13) and (14)

Example: A party wishes to introduce an internet web page into evidence.

- The certification **will be** sufficient to establish (absent advance objections by the opposing party) that the web page is what the proponent says – a particular web page that was posted at a particular time.
- The certification **will not be** sufficient to establish that the substance of the message on the web page is accurate.

Judicial Conference Illustrative Hypothetical to FRE 902(14)

Fact Scenario

Forensic technician Smith made forensic copy of mobile phone in the field. Smith verified that the forensic copy was identical to the original phone's text logs using an industry standard methodology (e.g. hash value or other means). Smith gave the copy to forensic technician Jones, who performed his examination at his lab. Jones used the copy to conduct his entire forensic examination so that he would not inadvertently alter the data on the phone. Jones found the text messages. The government wants to offer the copy into evidence as part of the basis of Jones's testimony about the text messages he found.

Judicial Conference Illustrative Hypothetical to FRE 902(14)

Without Rule 902(14):

The government would have to call two witnesses: (1) Forensic technician Smith to testify about making the forensic copy of information from the phone, and about the methodology used to verify that the copy was exact; and (2) Jones to testify about the message he found.

With Rule 902(14):

The proponent could obtain Smith's certification of the facts establishing how he copied the phone's information and then verified the copy was true and accurate. If the proper 902(14) notice procedure is followed, then the proponent need only call one witness, Jones.

Committee Note to FRE 902(14) – Process of Identification

- "Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value'."
- "[I]dentical 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 she checked the hash value of the proffered item and that it was identical to the original."
- Accounts for future technology "other than comparison of hash value" that could provide "other reliable means of identification."

Hash Value

- A digital fingerprint for files. The hash value is produced and identifies the contents of the file -- If they are modified, the hash tag value will change; a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.
- Two algorithms commonly used:
  - MD5: Message Digest algorithm 5; and
  - SHA-1 algorithm.

Prior Law on Admissibility of Electronic Evidence

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. May 4, 2007)

- In dispute about insurance claim for yacht damage from lightning, both sides' summary judgment motions were dismissed because each side attached emails without authentication.
- Magistrate Judge Grimm's 100+ page opinion analyzed admissibility of ESI.

Prior Law on Admissibility of Electronic Evidence

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. May 4, 2007)

- FRE 901(a) requires proponent of evidence to show it is what it is claimed to be.
- FRE 1003 provides that "[a] duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity…"
- FRE 1006 allows use of summaries, charts, or calculations "to prove the content of voluminous writings, recordings or photographs that cannot be conveniently examined in court."

Amendment to Federal Rule of Evidence 902(14)

FEDERAL RULES OF EVIDENCE

Rule 902(14) Amendment on Dec 1, 2017

***United States v. Dunnican*,** 961 F.3d 859 (6th Cir. 2020)

- As explained by the Advisory Committee in 2017, there are critical convenience and efficiency objectives linked to the application of Rule 902(14): 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 Committee also notes that the amendment was intended to **"provide 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."**

Social Media & Internet Collection – Challenges with Screenshot Methodology

- ***Monet v. Bank of America, N.A.***, 2015 WL 1775219, at *8 (Cal Ct. App. Apr. 16, 2015) (Facebook screenshot disallowed due to lack of authentication)
- ***Moroccanoil vs. Marc Anthony Cosmetics***, 57 F.Supp.3d 1203 (2014) (Facebook screenshots inadmissible in infringement matter without supporting circumstantial information)
- ***Linscheid v. Natus Medical Inc.***, 2015 WL 1470122, at *5-6 (N.D. Ga. Mar. 30, 2015) (LinkedIn profile page not authenticated by declaration from individual who printed the page from the Internet)
- 902(14) will only underscore flaws of the proponent where a valid "process of digital identification" is not utilized

Social Media & Internet Collection – Success with Screenshot Methodology

United States v. Bondars, No. 1_16-cr-228 (E.D. Va. Aug. 20, 2018)

- Court granted Government's motion to admit internet screenshots obtained using the Internet Archive's "Wayback Machine" in accordance with Fed. R. Evid. 902(13).
- The Court held that "the Wayback Machine screenshots introduced by the Government comport with the requirements and purpose of Rule 902(13) . They are established by a certificate of an Internet Archive Official and are not deficient in their authenticity. Further, they meet all procedural requirements under Rules 902(11) and 902(12)."

E-Discovery Collection Challenges – Custodian Self Collection

Numerous Challenges

- Defensibility/Compliance:
  - ***Nat'l Day Laborer Org. Network v. US Immigration & Customs Enforcement Agency***, (S.D.N.Y. Jul. 13, 2012)
  - ***GN Netcom, Inc. v. Plantronics, Inc.***, No. 12-1318-LPS, 2016 U.S. Dist. (D. Del. July 12, 2016)
- Lack of uniformity and transparency
- Disruptive to employees
- Matter sensitivity

E-Discovery Collection Challenges – Custodian Self Collection

EEOC v. M1 5100 Corp., No. 19-cv-81320 (S.D. Fla. July 02, 2020)

- "The relevant rules and case law establish that an attorney has a duty and obligation to have knowledge of, supervise, or counsel the client's discovery search, collection, and production"
- "It is clear to the Court that an attorney cannot abandon his professional and ethical duties imposed by the applicable rules and case law and permit an interested party or person to 'self-collect' discovery without any attorney advice, supervision, or knowledge of the process utilized"
- "There is simply no responsible way that an attorney can effectively make the representations required under Rule 26(g)(1) and yet have no involvement in, or close knowledge of, the party's search, collection and production of discovery"

Suggestions for Rule 902(14) Certifications

1. Identify the custodian and his/her qualifications.
2. Duties in conducting computer forensic investigations for litigation support and electronic discovery.
3. The number of investigations and preservation efforts related to the source (social media, emails, servers, cloud-based programs) done in the past and on similar collections.
4. How custodian was retained and the exact instructions given to carry out the preservation, maintenance, and collection.
5. When collected, how the software generated and assigned hash values based upon the evidence's content.
6. Quality control measures taken to verify the identical hash values and an attestation that the evidence has not changed or been altered.

Preparing for Authenticity Issues

- Collect your ESI in a defensible way at the onset of the case, using forensically sound methods and custodians who can provide the foundation necessary for admissibility
- Prepare the certification well in advance and provide to opposing counsel
- Make sure that the certifying party has checked the hash values for original documents and copies to ensure they are identical

Sedona Conference Commentary on ESI Evidence and Admissibility, Second Edition

- In March 2008, Sedona released its initial publication outlining a framework for authenticating and admitting ESI. On Oct. 12 2020, Sedona announced the release of its *Commentary on ESI Evidence & Admissibility*, Second Edition, 22 Sedona Conf. J. 83 (forthcoming 2021).
- The updated Commentary:
  - Addresses the impact of the 2017 and 2019 amendments to the Federal Rules of Evidence
  - Discusses the application of existing rules and case law to ESI evidence
  - Analyzes new issues related to emerging ESI derived from sources such as ephemeral data, blockchain, social media, collaboration tools, emoji's and artificial intelligence
  - Offers practical guidance on admissibility and the use of ESI in court

State Analogs to FRE 902(13)(14)

The following states have amended their rules of evidence to allow for a provision identical or nearly identical to FRE 902(13)(14):

- Alabama
- Arizona
- Illinois
- Mississippi
- North Dakota
- Ohio
- Pennsylvania
- Utah
- Vermont – *Vt. R. Evid. 902(13) relates to Blockchain records*
- Wyoming

Thank You

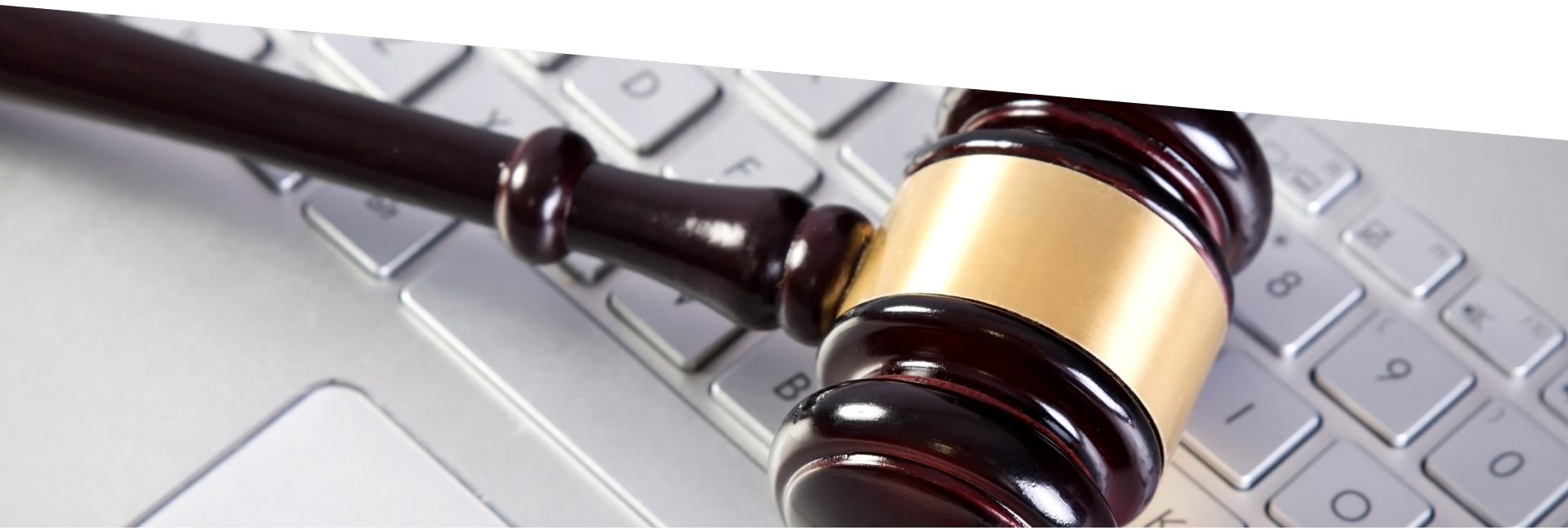
David Cohen
drcohen@reedsmith.com
412-288-1098

Dennis Wilenchik
DIW@wb-law.com
602-606-2810

Questions?

Key Questions Regarding FRE 902(14)

- Have ESI collection practitioners (service providers, in-house counsel, law enforcement) seen increased utilization?
- Have their been more written certifications, less testimony?
- Have the new rules served as a new basis for challenges if best practices not utilized?
  - "Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate."



Further Discussion Points

Further Discussion Points

How do you do collect ESI?

- Do you rely on custodians?
- Internal IT?
- Forensic experts?
- Does it depend on the case?

What tools do you use to collect ESI today?

Further Discussion Points

Has authentication of ESI been an issue for you? If so, in what context?

- Email? Other messaging data (e.g., Texts, Teams, Slack, Bloomberg, etc.)?
- Sharepoint/One Drive/Cloud Data?
- Mobile devices?
- Structured data?
- Social media or other webpages?

Further Discussion Points

How much difference has this rule change made in your discovery process?

- Prior to the rule change, did you track/match hash values of original versus produced data?
- How does hash value matching occur in practice?
- Who is a “qualified person”? Internal IT?
- Have you made changes to your discovery process to take advantage of this change?

Further Discussion Points

What issues (or benefits) have you seen in complying with the rule change?

- Opportunity for easier authentication?
- Opportunity for opposing parties to create issues about authentication?
- Other?