AUTHENTICATION OF ELECTRONIC EVIDENCE

RAIFORD D. PALMER, AAML
SULLIVAN TAYLOR, GUMINA & PALMER, P.C.
raif@stglaw.com

1. Electronic evidence is admissible in Illinois. Not fundamentally different than paper correspondence, diagrams, photos, etc. Process – same as authenticating paper documents.

2. Illinois Supreme Court Rule 201(b)(1): *The word 'documents' as used in these rules, includes, but is not limited to, papers, photographs, films…communications and all retrievable information in computer storage.*

3. IRE 901(a) *General Provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied be evidence sufficient to support a finding that the matter in question is what its proponent claims*. – Or, Is the "stuff" what you say it is? When in doubt, show the Judge why the electronic document should be believed. Rule 901 also provides other methods of authentication that have parallels for electronic evidence.

4. Authentication of a document may be by direct or circumstantial evidence, which is routinely the testimony of a witness who has sufficient personal knowledge to satisfy the trial court that the item is, in fact, what the proponent claims it to be. *Piser v. State Farm Mutual Automobile Insurance Co.*, 405 Ill.App.3d 341, 349.

5. **Email:** Illinois does not have an "authentication by production" rule as in other states. Email and other electronic evidence are not be authenticated at trial and summary judgment just because they are produced in discovery. Emails need to be authenticated like traditional written documents. As with paper documents, per Rule 901(a), show the document is what it purports to be. *Complete Conference Coordinators, Inc. v. Kumon North America*, 394 Ill.App.3d 105 (2nd Dist. 2009).

   Direct and circumstantial evidence can be used to authenticate emails. In a criminal sexual abuse case, the state intended to admit emails that demonstrated the defendant admitted to a sexual relationship with the victim. The victim testified that she met the defendant via the internet; that she communicated with defendant via email and used a specific email address for defendant for all her email communications in the past. When she worked with police, she emailed the defendant from the police department using the same email address that she had used before and received a response to the same email she had used in the past to contact the defendant. Finally, the reply email

contained unique information only she and the defendant would know. The defendant challenged the admission of the emails via an expert witness, claiming that the state needed to link his email address with a specific IP address. The Court stated: "Prima facie authorship of a document may include a showing that the writing contains knowledge of a matter sufficiently obscure so as to be known to only a small group of individuals." *People v. Downin*, 357 Ill.App.3d 193, 203 (3rd Dist. 2005).

Key email authentication avenues:

a. Self-identification by the parties. Identify the email address, frequent usage of the email address to send a receive email messages from a known person. Have the other party admit they sent/received the messages.
b. Ongoing exchange of email between the parties
c. Witness identifies email addresses used.
d. Unique and personal nature of the contents.
e. Device in possession of a witness contains email matching those offered into evidence.
f. Acts by witnesses or parties in conformity with an email message.
g. Chain of evidence – how did messages transfer from computer or mobile device to printed form in court? (Printing a forwarded message from a party to an attorney is a poor method).

6. **Text Messages**. Like email, texts are treated like other paper documents in terms of foundation. Texts must be authenticated by direct or circumstantial evidence. The contents of text messages may be used to authenticate them if shown to be known by the sender of the text, or at least by one person or small group of people including the claimed sender. *People v. Ziemba*. 2018 IL App (2d) 170048. In *Ziemba*, an undercover police officer used a police system to send and receive texts with the defendant in a sex trafficking sting operation. The prosecution wanted to admit the chain of text messages between them and the defendant. The texts were admitted. First, the state offered direct evidence of authenticity. The undercover officer who was involved in the text communications testified that the transcript was an accurate recording of the entire text conversation. The state also offered circumstantial evidence of authenticity. Testimony was given matching the defendant's phone number to the number the undercover officer used in the text message exchange. Also, the content of the text messages on the police computer matched with the defendant's phone text messages exactly.

   In *IRMO LaRocque*, 2018 IL App (2d) 160973, a divorce matter, the trial court admitted printouts of text messages between the parties. Admission of the messages was affirmed on appeal. The husband offered a transcript of thousands of text messages into evidence for a two-year period. As his foundation, he testified to the following: First, he found an iPhone backup file when accessing the family's shared iCloud account. He

downloaded that file onto another iPhone. Upon reviewing that file in the iPhone, he discovered that it contained text messages between himself and the wife. He then gave the phone to his attorneys, who were able to print out the text message chains. He also testified that he recalled many of the messages, and that some of phrases used in the messages were things only he and his wife would know. The appellate court affirmed, holding that the husband demonstrated that the documents were what he claimed them to be. The court also noted that the wife did not object to the authenticity of the communications, she only testified that there were "things missing from there."

Interestingly, in *People v. Chromik*, 408 Ill.App.3d 1028, 1046-48 (3rd Dist. 2011): an incomplete transcript of text messages sent from defendant to victim was admitted into evidence. The messages were transcribed by the victim, a high school student, by reading the text messages with dates and times aloud to her high school principal, who typed the transcript. The transcript was held to be properly authenticated (even though not 100% accurate) where dates and times of messages in transcript mirrored those in phone company records, the high school student victim testified to the content of the messages, and the defendant acknowledged the accuracy of several of the messages.

In contrast, see *People v. Watkins*, 2015 IL App (3d) 120882 (3rd Dist. 2015), where admission of text messages for a limited purpose was reversed on appeal. In that case, the state wanted to show that defendant used a cell phone found in a drawer, where drugs were also found by police, to help prove a constructive drug possession case. The only evidence offered to authenticate the text messages by the state was that the phone was found in the same house as defendant, in a drawer in a common area, and the fact that some of the messages referred to or were directed at a person named "Charles." Court held that there were missing items important to authentication of the messages: no cell phone records to show the phone belonged to or was used by defendant, no identifying marks on the phone or the screen to indicate a connection to defendant (other than the references to "Charles" in the texts) The fact that the investigating officer testified that photos taken of the phone's screen were "true and accurate" depictions of the text messages did not change the Court's opinion. The officer had no personal knowledge of the text messages and had no idea who was the owner or user of the cell phone.

Key Text Message Authentication Avenues:

a. Sender/recipient admits authorship/receipt.
b. Witness identifies phone number used for text exchange.
c. History of text message exchanges.
d. Acts in conformity with text messages.
e. Photos sent in texts of sender/recipient or otherwise unique to the parties to the communication.

f. Actual phone itself contains the messages matching those intended to be offered, and has other identifying information (name, phone number, address listed in the phone).
g. Messages contain information only known to the parties to the communication or to a small group.
h. Phone provider records have matching phone numbers and dates and times matching messages.
i. Chain of evidence – how did the messages get from the cell phone to the courtroom? (see, e.g., *Chromik*)

7. **Social Media Posts**. In *People v. Kent*, 2017 IL App (2d) 140917 (2nd Dist. 2017), a Facebook post was not admitted into evidence. However, the court was helpful to show the ways such posts may be authenticated. In the case, Kent was charged with first degree murder. The victim was shot and killed in his driveway. The state wanted to admit a post on Facebook by a "Lorenzo Luckii Santos" showing a photo of a person resembling Defendant in an undated post stating "its my way or the highway…leave em dead in his driveway." [sic] "Lorenzo" was defendant's first name, "Luckii" was his nickname, and "Santos" was claimed to the the last name of defendant's mother (but no evidence offered at trial to this fact). In a preliminary hearing, the state made a representation that the post was sourced from an IP address linked to a woman with whom both the defendant and victim were involved, but no Facebook or IP records were offered at trial. The court noted that it is very easy to create fictional Facebook posts, and the State failed to show that it was not public knowledge that the victim was not killed in his own driveway. The court held that IRE 901 requires some basis for the trier of fact to determine that the post was in fact created by the defendant. The court stated that the type and amount of authentication will vary depending on context. The Court was helpful about what kinds of authentication would be useful.

   Key Social Media Authentication Avenues:
   a. Sender admits authorship;
   b. Poster is seen writing the post;
   c. Business records of ISP or phone company show the post originated from the claimed sender's device;
   d. Communication contains only information that the sender would know;
   e. The poster responds to an exchange in a way indicating that he was in fact the author of the post;
   f. Other circumstances unique to the case may be offered to make a *prima facie* showing of authenticity. For example, other witnesses may testify that the know the poster has a certain screen name, has used it for a length of time, and may have communicated with the person via social media using that screen name multiple times.

8. **Electronic data from computers, phones, etc.** Occasionally, a party may use a forensic expert to image hard drives on a computer taken from an opponent in a family law case, to copy them in their entirety and preserve the data. As an aside, a TRO may be useful at the outset of a case, where you have reason to believe a party will alter or destroy electronic records (like a second set of electronic books for a restaurant, or emails). In that case, you need the expert to testify as to the method used to extract the data, that the data copied is unaltered from the original, and to establish the chain of evidence establishing how the expert obtained the source data and then copied into its final form. That expert must testify as to the reliability of the system used to copy the data and any self-tests used to confirm a proper copy. Note the amendments to IRE 902 may help with these forms of data (authentication by affidavit for electronic data). See *People v. Shinohara*, 375 Ill.App.3d 85 (1st Dist. 2007).

9. **Self-Authenticating Electronic Records - Amendments to IRE 902.** Effective 9/28/18. (See below). Comment to the amendments: Certification under Rules 902(12) and (13) must contain information sufficient to establish authenticity were that information provided by a foundation witness at trial. Certification satisfies only admission requirements for authenticity. The opposing party is free to object to admissibility on other grounds, including but not limited to relevancy, hearsay, or (in criminal cases) the right to confrontation.

Rule 901.

REQUIREMENT OF AUTHENTICATION OR IDENTIFICATION

(a) General Provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) Testimony of Witness With Knowledge. Testimony that a matter is what it is claimed to be.

(2) Nonexpert Opinion on Handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.

(3) Comparison by Trier or Expert Witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.

(4) Distinctive Characteristics and the Like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) Voice Identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) Telephone Conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) Public Records or Reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) Ancient Documents or Data Compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) Process or System. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) Methods Provided by Statute or Rule. Any method of authentication or identification provided by statute or by other rules prescribed by the Supreme Court.

Adopted September 27, 2010, eff. January 1, 2011.

Rule 902.

SELF-AUTHENTICATION

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

(1) Domestic Public Documents Under Seal. A document bearing a seal purporting to be that of the United States, or of any State, district, Commonwealth, territory, or insular possession thereof, or the Panama Canal Zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation or execution.

(2) Domestic Public Documents Not Under Seal. A document purporting to bear the signature in the official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

(3) Foreign Public Documents. A document purporting to be executed or attested in an official capacity by a person authorized by the laws of a foreign country to make the execution or attestation, and accompanied by a final certification as to the genuineness of the signature and official position (A) of the executing or attesting person, or (B) of any foreign official whose certificate of genuineness of signature and official position relates to the execution or attestation or is in a chain of certificates of genuineness of signature and official position relating to the execution or attestation. A final certification may be made by a secretary of an embassy or legation, consul general, consul, vice consul, or consular agent of the United States, or a diplomatic or consular official of the foreign country assigned or accredited to the United States. If reasonable opportunity has been given to all parties to investigate the authenticity and accuracy of official documents, the court may, for good cause shown, order that they be treated as presumptively authentic without final certification or permit them to be evidenced by an attested summary with or without final certification.

(4) Certified Copies of Public Records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any statute or rule prescribed by the Supreme Court.

(5) Official Publications. Books, pamphlets, or other publications purporting to be issued by public authority.

(6) Newspapers and Periodicals. Printed materials purporting to be newspapers or periodicals.

(7) Trade Inscriptions and the Like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, content, ingredients, or origin.

(8) Acknowledged Documents. Documents accompanied by a certificate of acknowledgment executed in the manner provided by law by a notary public or other officer authorized by law to take acknowledgments.

(9) Commercial Paper and Related Documents. Commercial paper, signatures thereon, and documents relating thereto to the extent provided by general commercial law.

(10) Presumptions Under Statutes. Any signature, document, or other matter declared by statutes to be presumptively or prima facie genuine or authentic.

(11) Certified Records of Regularly Conducted Activity. The original or a duplicate of a record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written certification of its custodian or other qualified person that the record

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of these matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

The word "certification" as used in this subsection means with respect to a domestic record, a written declaration under oath subject to the penalty of perjury and, with respect to a record maintained or located in a foreign country, a written declaration signed in a country which, if falsely made, would subject the maker to criminal penalty under the laws of the country. A party intending to offer a record into evidence under this paragraph must provide written notice of that

intention to all adverse parties, and must make the record and certification available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

(12) 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 procedural requirements for Rule 902(11) certification. The proponent must also meet the notice requirements of Rule 902(11).

(13) 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 procedural requirements for Rule 902(11) certification. The proponent also must meet the notice requirements of Rule 902(11).

Adopted September 27, 2010, eff. January 1, 2011; amended Sept. 28, 2018, eff. immediately.

Bibliography

Saunders, Rhys: *Admit It*. **Illinois Bar Journal**, November 2018, Vol. 106, No. 11, P. 12.

Karrison, Dustin J.: *What's Not to "Like"?* **Illinois Bar Journal**, November 2018, Vol. 106, No. 11, P. 28.

Zimmerman, John M.: *People v. Kent: The New Standard for Authenticating Social Media Evidence.* **Illinois Bar Journal**, April 2018, Vol. 106, No. 4, P.26.

Kling, Richard; Hasan, Khalid; and Gould, Martin: *Evidence: Admissibility of Social Media Evidence in Illinois*. **Illinois Bar Journal**, January 2017, Volume 105, No. 1.

Getting Access to Social Media Evidence. **Illinois Bar Journal**, December 2017, Vol. 105, No. 12, P. 24.

Finkel, Ed: *Building Your Case with Social Media Evidence*. **Illinois Bar Journal**, June 2014, Vol. 102, No. 6, P. 276.

McCann, Nicholas O.: *Tips for Authenticating Social Media Evidence*. **Illinois Bar Journal**, September 2012, Vol. 100, No. 9, P. 482.

Haddad, Hon. Wm. J.: *Authentication and Identification of E-Mail Evidence*. **Illinois Bar Journal**. May 2008. Vol. 96, No. 5, P. 252.

Koerth, Theodore J. and Paetsch, Christopher E. *How to Admit E-Mail and Web Pages into Evidence*. **Illinois Bar Journal**. December 2006, Vol. 94, No. 12, P. 674.