NBI Seminar Litigation Start to Finish in South Carolina

I. **How to Authenticate Social Media, Email, and Text Evidence** - *2:45 - 3:30, Marcus A. Manos* Shareholder, Maynard Nexsen PC 803.253.8275 MManos@maynardnexsen.com

A. Proactively Ensuring Authenticity

> Social media messages and other content may appear to pose unique authentication problems, but these problems dissolve against the framework of Rule 901, SCRE. Social media messages and content are writings, and evidence law has always viewed the authorship of writings with a skeptical eye. 2 McCormick On Evid. § 221 (evidence law does not assume authorship of a writing, "[i]nstead it adopts the position that the purported signature of recital of authorship on the face of a writing is not sufficient proof of authenticity to secure the admission of the writing into evidence").

State v. Green, 427 S.C. 223, 830 S.E.2d 711 (Ct. App. 2019).

While social media and the modern world pose what seem to be new problems, the same basic inquiries for authenticating all writings are still relevant and important when offering into evidence.

The threshold inquiry for all evidence stems from SCRE Rules 401 and 402. Any offered evidence must be relevant and must qualify under rule 401. Generally, "[a]ll relevant evidence is admissible." Rule 402, SCRE. " 'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Rule 401, SCRE. Assuming relevancy is met, we move to Rule 901(b) which outlines the requirements for authentication.

The 2019 South Carolina Court of Appeals decision of *State v. Green* gives an in-depth analysis of the requirements for authentication in our digital world. In Green, the Appellant appealed the trial court's admission of a series of direct messages from the victim's Facebook account into evidence over Appellant's objections.

State v. Green, 427 S.C. 223, 229–30, 830 S.E.2d 711, 714 (Ct. App. 2019), aff'd as modified, 432 S.C. 97, 851 S.E.2d 440 (2020)

- All evidence must be authenticated. *State v. Brown*, 424 S.C. 479, 488, 818 S.E.2d 735, 740 (2018); 2 McCormick On Evid. § 221 (7th ed. 2016) ("[I]n all jurisdictions the requirement of authentication applies to all tangible and demonstrative exhibits."). Authentication is a subspecies of relevance, for something that cannot be connected to the case carries no probative force. The trial judge acts as the authentication gatekeeper, and a party may open the gate by laying a foundation from which a reasonable juror could find the evidence is what the party claims. Rule 901(a), SCRE ("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."). . . .
- The court decides whether a reasonable jury could find the evidence authentic; therefore, the proponent need only make "a prima facie showing that the 'true author' is who the proponent claims it to be." United States v. Davis, 918 F.3d 397, 402 (4th Cir. 2019). Once the trial court determines the prima facie showing has been met, the evidence is admitted, and the jury decides whether to accept the evidence as genuine and, if so, what weight it carries. Rule 104(b), SCRE; see United States v. Branch, 970 F.2d 1368, 1370–72 (4th Cir. 1992); 5 Weinstein et al., Weinstein's Federal Evidence § 901.02[3] (2d ed. 2019).
- The requirement of authentication cannot be met by merely offering the writing on its own. See Williams v. Milling-Nelson Motors, Inc., 209 S.C. 407, 410, 40 S.E.2d 633, 634 (1946). Something more must be set forth connecting the writing to the person the proponent claims the author to be. Rule 901, SCRE, does not care what form the writing takes, be it a letter, a telegram, a postcard, a fax, an email, a text, graffiti, a billboard, or a Facebook message. All that matters is whether it can be authenticated, for the rule was put in place to deter fraud. 2 McCormick On Evidence § 221.
- "We recognize some cases may require more technical methods to authenticate social media. Some courts have held, for example, that tracking a defendant's Facebook page and account to his email address by internet protocol (IP) evidence can satisfy authentication. . . . We understand social media could also be authenticated by evidence related to hash values and metadata. We express no opinion in these methods of proof. We are aware of the debates over the "Maryland Rule" and the "Texas Rule" concerning social media authentication, but these labels seem to complicate the simple

concept embodied in Rule 901, SCRE, and by which writings have long been authenticated."

- Honorable Paul W. Grimm et. al., Authentication of Social Media Evidence, 36 Am. J. Trial Advoc. 433, 441 (2013) – "At present, the cases that address the authentication and admissibility of social media evidence--typically photographs and postings on MySpace and Facebook pages--unfortunately arrive at widely disparate outcomes.
  - Maryland Rule - One line of cases sets an unnecessarily high bar for the admissibility of social media evidence by not admitting the exhibit unless the court definitively determines that the evidence is authentic.
  - Texas Rule - Another line of cases takes a different tact, determining the admissibility of social media evidence based on whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic."

- "We do not downplay the fraud risk surrounding social media. The internet flattened the speed of and access to the flow of written information; documents that once sat in dusty file cabinets crammed into office corners now float in the "cloud" making them susceptible to a wider range of mischief. We are persuaded the risk is one Rule 901, SCRE, contemplates and can contain.

Authenticating an email, text, or instant message can be simple depending on the purpose for which it is offered. A witness can authenticate such material as having been sent by the witness himself by identifying it as such. Similarly, one who receives an email, text, or instant message, can authenticate it as having been received simply by testifying, but it is another matter to prove the identity of the author of such an email, text or message.

Authenticity can be established in many ways:

- Established in pretrial discovery, including identification at a deposition or answers to discovery requests. These mechanisms can often establish not only the receipt of material, but authorship.
- Testimony by a person who saw the purported author write and send the material.
- Having the computer or cellphone from which the material was sent seized from a person's possession.
- If it is a shared computer, or one to which others have access, additional evidence linking the purported author to the email is essential.

  - This would include proof that a person in question was the one using the computer when the message was sent or having technical witnesses perform a trace such as relying on coded Internet Protocol Addresses appearing in an email header or using metadata stored in documents or encrypted data.
- The most common method of authenticating involves showing circumstantial evidence.

B. Proving Electronic Documents Have Not Been Modified

Linda Greene, Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois, 68 DePaul L. Rev. 103, 125 (2018) –

- Metadata provides contextual information as to the origins of a document, such as the date and time of its creation. Rather than rely on a witness whose recollection or credibility may be called into doubt, metadata can definitively establish the date and time a screenshot was captured.
- This is not to say that metadata is immune to manipulation. Even absent bad faith, metadata is highly susceptible to inadvertent alteration.
- But with special software, digital forensic experts can access and preserve a file without affecting the metadata and are often able to detect when metadata has been fabricated.
- Because metadata is highly volatile by nature, it inherently provides a record of if and when the electronic document has been modified.

C. Identifying Who Made the Post and Linking to the Purported Author

§ 9:9 Email, social media, web pages, text messages, instant messages electronic signatures, 5 Federal Evidence § 9:9 (4th ed.)
Social Media –

- Modern cases have increasingly faced the question whether evidence from social media (Facebook, MySpace, Twitter, and others) should be admitted.
- Authentication issues resemble those found with other forms of electronic communication, but one distinguishing factor is that social media often involve postings that are accessible to large numbers of people, and sometimes to the entire world.
- It is uncertain whether social media accounts are more easily hacked than email accounts, but obvious concerns about security of social media arise, and it may well be that more people have both motive and access to social

media, which heightens concerns over security and possibly malicious and fraudulent postings.

- The Maryland Supreme Court observed that "authentication concerns attendant to emails, instant messaging, and text messages differ significantly from those involving a MySpace profile and posting printout, because such correspondence is sent directly from one party to an intended recipient or recipients, rather than published for all to see."
- As with other forms of electronic communication, the challenge is usually not in proving that a particular communication was received or posted, and the concern is rather in learning the identity of the sender or maker.
    - A mere showing that the message was sent from a particular account or posted on a particular web page is not necessarily sufficient to authenticate the message as being from the owner of that account or web page, and more should be shown to establish the identity of the person posting the message, such as evidence that the originating site has security features that tend to assure the identity of the source.
- The authentication method most commonly used by proponents of social media evidence is to demonstrate its distinctive characteristics.
    - Under Rule 902(4) the proponent must show that the circumstantial evidence of the case combined with the "appearance, contents, substance, internal patterns, or other distinctive characteristics" of the exhibit are sufficient to prove that the proffered evidence is what it is purported to be.
    - A distinctive characteristic particularly likely to persuade a court that the authentication requirement is satisfied is the use of code words known only to the parties.
- Circumstantial evidence varies significantly from case to case, and courts apply different levels of scrutiny when determining whether the authentication threshold has been satisfied. Some courts have applied a strict standard and others a more lenient one.
- If the proponent calls an authenticating witness to testify how a particular electronic communication is made, such as an expert from the company sponsoring the social media site, that person must be able to "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."
- Courts have held, however, that it is not essential to call such an expert, at least in cases where there are other forms of authenticating evidence available

United States v. Recio, 884 F.3d 230 (4th Cir. 2018) – Government authenticated post by social networking account allegedly belonging to defendant in trial for being felon in possession of firearm; social networking website record containing post was made at or near time the information was transmitted by the user, user name associated with account was defendant's name, one of the four email addresses associated with account contained defendant's name, and more than 100 photographs of defendant were posted to account. Fed. R. Evid. 901.

U.S. v. Hassan, 742 F.3d 104 (4th Cir. 2014). – District court did not abuse its discretion in determining that government had adequately authenticated screenshots of defendants' user profiles and postings on social media website and videos posted on video sharing website, where government presented records custodians' certifications, verifying that web pages and videos had been maintained as business records in course of regularly conducted business activities, and tracked social media accounts to defendants' mailing and e-mail addresses via internet protocol addresses. Fed.Rules Evid.Rules 901, 902(11), 28 U.S.C.A.

D. Authenticating Through Witness Testimony

§ 9:9 Email, social media, web pages, text messages, instant messages electronic signatures, 5 Federal Evidence § 9:9 (4th ed.)
Authenticating an email, text, or instant message can be simple depending on the purpose for which it is offered. A witness can authenticate such material as having been sent by the witness himself by identifying it as such. Similarly, one who receives an email, text, or instant message, can authenticate it as having been received simply by testifying, but it is another matter to prove the identity of the author of such an email, text or message.

- Pre-trial –
    - Authenticity can be established in pretrial discovery, including identification at a deposition, in an answer to an interrogatory or in response to a request for admission.
    - These mechanisms can establish the receipt of material, but authorship as well.

- A witness can authenticate such material as having been sent by the witness himself by identifying it as such.
- One who receives an message can authenticate it has having been received simply by testifying

- It is more difficult to prove the identify of the author of such a message.

State v. Green, 427 S.C. 223, 231, 830 S.E.2d 711, 715 (Ct. App. 2019), aff'd as modified, 432 S.C. 97, 851 S.E.2d 440 (2020)

- Rule 901(b), SCRE, lists ten non-exclusive methods of authentication. The first method is the easiest and most direct way to authenticate a writing: having someone with personal knowledge about the writing testify the matter is what it is claimed to be. Rule 901(b)(1), SCRE. This method may be accomplished by testimony from a person who sent or received the writing. Because it is the easiest method, it is also uncommon, for the sender and the recipient are often unavailable, as here. One who witnessed the creation or signing of the writing also has the personal knowledge Rule 901(b)(1), SCRE, demands.

State v. Hall, 437 S.C. 107, 120, 876 S.E.2d 328, 335 (Ct. App. 2022) (finding the trial court erred to admit Snapchat video messages into evidence because Jackson received the messages from Elmore and could have authenticated the messages with personal knowledge under Rule 901(b)(1), SCRE. While there is a risk the video messages were not contemporaneously recorded at the time they were sent, a reasonable jury could find the messages were what Jackson said they were – videos of Elmore playing with their daughter at their home while the shootings occurred).

State v. Gray, 438 S.C. 130, 143, 882 S.E.2d 469, 476 (Ct. App. 2022), reh'g denied (Jan. 23, 2023), cert. denied (Oct. 3, 2023) (finding the State properly authenticated a video with the personal knowledge of the owner and operated of the security system which recorded the video).

United States v. Walker, 32 F.4th 377, 393 (4th Cir.), cert. denied sub nom. Anthony Walker v. United States, 143 S. Ct. 450, 214 L. Ed. 2d 256 (2022) (finding the Government adequately established that the screenshots of photographs depicted letters from Appellant through personal knowledge about the report and the comparison of two images).

E. <u>Authenticating via Distinctive Characteristics and Circumstantial Evidence</u>

§ 9:9 Email, social media, web pages, text messages, instant messages electronic signatures, 5 Federal Evidence § 9:9 (4th ed.)
The most common method of authenticating involves showing "appearance, contents, substance, internal patterns, or other distinctive characteristics …, taken together with all circumstances," which can suffice Rule 901(b)(4).

- Included in the relevant circumstances are indications in the message itself of its source, connections between statements in the communication itself and known facts about the sender, behavior by the sender and the recipient that point towards the two as being sender and recipient, a course of conduct or dealing between two people that regularly employs emails, texts, or instant messages and showing that the material in question fits into that course of dealing, and connections between the person in question and the phone in question, coupled with other information about behavior as it relates to content.
- The fact that a person's name appears in the header as a sender should not be enough to authenticate the email as being from that person, just as self-identification by a telephone caller is insufficient to authenticate the call as being from that person.
- However, self-identification can complement other authenticating factors such as circumstances, content, internal patterns and extrinsic evidence.
- Stronger circumstantial evidence would be a showing that the actual email address matches an account in that person's name with the indicated internet service provider, although it is not necessarily sufficient by itself because it is not technically difficult to send an email using another's email address.
- In most modern cases, courts have relied primarily on the content of the message as a basis for authenticating emails. If an email contains particularized information that only the purported sender is likely to know, this will authenticate the email to the same extent that such knowledge would authenticate a written message.
    - Particularized content may include information about serial numbers, credit card numbers, ordering information, personal transactions, private communications, particular relationships, coded communications, and other types of private information that is now known to the general public.
    - A common type of content used to authenticate is content given in a reply to an earlier message. An email purporting to be a reply to an earlier message sent to a particular person is likely to be authored by that person.
    - Other circumstances that can be used to help authenticate an email include the fact that the purported sender promised to send an email to

the recipient and the one was later received by the fact the previous message sent to a particular email address reached the purported sender of the email in question, or the fact that actions were taken by the purported sender in response to emails sent to the purported sender's address, such as the shipping of merchandise.

- Emails can also be authenticated under Rule 901(b)(3) which authorizes "comparison with an authenticated specimen by an expert witness or the trier of fact.
- Business Records – emails, even if made in the course of business, do not necessarily qualify as a business record.
    - While emailed billing statements and similar records may qualify, routine personal and professional email communications often fail to satisfy the exception because they lack the regularity and systematic checking of information that justifies making business records an exception to the hearsay rule.
- The procedures for authenticating printouts of online chatrooms and conversations are essentially the same as those for authenticating emails.

State v. Green, 427 S.C. 223, 232–33, 830 S.E.2d 711, 715 (Ct. App. 2019), aff'd as modified, 432 S.C. 97, 851 S.E.2d 440 (2020)

- Most writings meet the authenticity test through Rule 901(b)(4), SCRE, which enables authentication to be proven by: "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Courts lag behind technology for good reason. As society adapts to the digital age, courts are growing more comfortable with using circumstantial evidence to authenticate social media content. 2 McCormick On Evidence § 227; 5 Mueller & Kirkpatrick, Federal Evidence § 9.9 (4th ed. 2018) (noting most common way to authenticate social media is by evidence of distinctive characteristics); see also Grimm, et al., Authentication of Social Media Evidence, 36 Am. J. Trial Advoc. 433, 469 (2013) (Rule 901(b)(4) is "one of the most successful methods used to authenticate all evidence, including social media evidence").
- Rule 901(b)(4), SCRE, meshes with prior South Carolina law, which has long endorsed authentication by circumstantial proof. See Kershaw Cty. Bd. of Educ. v. U.S. Gypsum Co., 302 S.C. 390, 398, 396 S.E.2d 369, 373–74 (1990). As our supreme court explained in State v. Hightower, 221 S.C. 91, 105, 69 S.E.2d 363, 370 (1952):
    - Like any other material fact, the genuineness of a letter may be established by circumstantial evidence if its tenor, subject-matter, and

> the parties between whom it purports to have passed make it fairly fit into an approved course of conduct, and manifests the probability that the subject-matter of its contents was known only to the apparent writer and the person to whom it was written ....

- See also Singleton v. Bremar, 16 S.C.L. 201, 210 (Harp. 1824) (letter authenticated by reference to unique facts relating to writer "and her situation"). A writing may also be authenticated if it is made in reply to an earlier communication from a source known to be genuine. See Kershaw Cty. Bd. of Educ., 302 S.C. at 398, 396 S.E.2d at 373–74; Leesville Mfg. Co. v. Morgan Wood & Iron Works, 75 S.C. 342, 344, 55 S.E. 768, 768–69 (1906); see also 7 Wigmore et al., Evidence in Trials at Common Law § 2153 at 753 (Chadbourn rev. ed. 1978). This *233 has been termed the "reply letter doctrine"—though today it might be better called the "reply email2 doctrine."

United States v. Walker, 32 F.4th 377, 393 (4th Cir.), cert. denied sub nom. Anthony Walker v. United States, 143 S. Ct. 450, 214 L. Ed. 2d 256 (2022) (holding a trier of fact may authenticate a document by comparing it with an authenticate specimen).

F. Self-Authentication Methods

United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (finding that Facebook pages and YouTube videos were self-authenticating under Federal Rule of Evidence 902(11) and were thus admissible as business records because the Facebook pages displayed their user profiles and posting, included photos and links to the YouTube videos, their user profiles included biographical information and listings of their interests, and the government presented certification of records custodians of Facebook and Google, verifying the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities).

United States v. Banks, 29 F.4th 168, 182 (4th Cir. 2022) (finding it was not an abuse of discretion for the district court to admit into evidence the certificate of authenticity of the Facebook records and messages associated with the Facebook account because the jury could conclude that Banks authored and received the messages based upon the username associated with the account, the account was present on a phone recovered from the vehicle at the motel which Banks was

observed exiting and entering, a 2018 message identified the sender with a nickname for Banks and his place of residence.)

DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 (D.S.C. 2004) (holding the declaration with a witness affidavit satisfied the business record exception to hearsay and simultaneously resolved plaintiff's authentication problem because the declaration satisfied Rule 803(6) and Rule 902(11) by stating that the e-mail records were kept in the normal course of business and created at or near the time of the matters involved).

Secondary Sources:

Authenticating Digital Evidence at Trial – April 2017 – American Bar Association – Michaela Battista Sozio – https://www.americanbar.org/groups/business_law/resources/business-law-today/2017-april/authenticating-digital-evidence-at-trial/

E-mails are now commonly offered as evidence at trial. After first demonstrating that the evidence is relevant pursuant to FRE 401, the attorney proffering this evidence must establish authenticity:

- Was the e-mail sent to and from the persons as indicated on the e-mail?
- Here, a witness with personal knowledge may testify as to the e-mail's authenticity, which typically is the author of the e-mail or a witness who saw the proffered e-mail drafted and/or received by the person the proponent claims drafted/received the e-mail.
- In addition, if the e-mail has been produced in response to a sufficiently descriptive document request, the production of the e-mail in response may constitute a statement of party-opponent and found to be authenticated under FRE 801(d)(2).

Texts are also becoming increasingly offered as evidence at trial.

- Typically, evidence of texts is obtained in one of two forms: (1) as screen shots; or (2) as photographs of the text messages.
- Whether a screen shot or a photograph, it is important that the screen with the text message, the name and/or phone number of the person sending the text message, and the date and time the message was sent are clearly displayed.
- Text messages can be authenticated by the testimony of a witness with knowledge or by distinctive characteristics of the item, including

circumstantial evidence such as the author's screen name or monikers, customary use of emoji or emoticons, the author's known phone number, the reference to facts that are specific to the author, or reference to facts that only the author and a small number of other individuals may know.

Social media networks such as Facebook, Linked-In, and the like are now ubiquitous; consequently, social media posts have increasingly become evidence at trial.

- However, authenticating a social media post generally is more difficult than an e-mail or a text.
- For example, it is insufficient to simply show that a post was made on a particular person's webpage; it is generally too easy to create a Facebook page or the like under someone else's name.
- In addition, an individual could have gained access to someone else's social media account.
- To properly introduce evidence of a social media post at trial, you must first have a printout (or download, if a video) of the webpage that depicts the social media post you seek to introduce as evidence, and the person who printed or downloaded the post must testify that the printouts accurately reflected what was on his or her screen when it was printed or downloaded.
- Once that is established, the social media post must be authenticated. This can be done in several ways.
    - Direct witness testimony can be obtained by the purported creator of the post, from someone who saw the post being created, and/or from someone who communicated with the alleged creator of the post through that particular social media network.
    - Testimony can be obtained from the social media network to establish that the alleged creator of the post had exclusive access to the originating computer and the social media account.
    - The subscriber report can also be subpoenaed from the social media network, which can identify all posts made and received as well as any comments, "likes," "shares," photographs, etc.
- As with e-mails and texts, circumstantial evidence may also be used for authentication pursuant to FRE 901(b)(4) if, for example, the post contains references or information relating to family members, a significant other, or co-workers; the writing style of the posts or comments is in the same style (i.e., slang, abbreviations, nicknames, and/or use of emoji/emoticons) the purported author uses; or there are private details about the author's life or details that are not widely known that are indicated in the post.

- Finally, do not overlook the option of having the author of the social media post authenticate the post and testify regarding the post in his or her deposition.

§ 9:9 Email, social media, web pages, text messages, instant messages electronic signatures, 5 Federal Evidence § 9:9 (4th ed.)

Proving by computer printout or electronic images – A witness who has seen the email or text message or instant message need only testify that a printout offered is an accurate reproduction. Rule 901 allows authentication by showing a process produces an accurate result. A court may take judicial notice of the processes. There is no best evidence problem with respect to printouts or electronic images, because Rule 1001(d) defines "original" to include "any printout – or other output readable by sight – if it accurately reflects the information."

Authenticating an email, text, or instant message can be simple depending on the purpose for which it is offered.

- Pre-trial –
    - Authenticity can be established in pretrial discovery, including identification at a deposition, in an answer to an interrogatory or in response to a request for admission.
    - These mechanisms can establish the receipt of material, but authorship as well.
- A witness can authenticate such material as having been sent by the witness himself by identifying it as such.
- One who receives an message can authenticate it has having been received simply by testifying
    - It is more difficult to prove the identify of the author of such a message.
- Testimony by the recipient indicating receipt of material satisfies Rule 901(b)(1) because it is testimony by a witness with knowledge "that an item is what it is claimed to be" that the witnesses received.
- Establishing authorship –
    - Testimony by a person who saw the purported author write and send such material would suffice.
    - If the computer, or the cellphone, etc, from which the material was sent is owned by a particular person, it could be seized from that

person's possession, or other compelling circumstances linking the computer to that person, such facts may be enough to authenticate the material as having come from that person.

- If it is a shared computer, or one to which others had access, additional evidence linking the purported author to the email seems essential.
- For emails, an expert may rely on the coded Internet Protocol Address appearing the email header to trace it back to the service provider who relayed the message and sometimes back to a particular computer, and electronic data can sometimes be authenticated by reference to metadata stored in documents and by "hashtags" used to encrypt data.
- If the email was encrypted by means of a digital signature and was therefore only available to a receiver who had a private key or access to a public key, a technical expert should be called to explain the encryption process and establish the necessary linkages to authenticate the email.
- The most common method of authenticating emails, texts, and instant messages involves showing "appearance, contents, substance, internal patterns, or other distinctive characteristics …, taken together with all the circumstances" which can suffice Rule 901(b)(4).
    - Included in the relevant circumstances are indications in the message itself of its source (whether name, phone number, or URL), connections between statements in the communication itself and known facts about the sender, behavior by the sender and the recipient that point toward the two as being send and recipient, a court of conduct or dealing between two people that regularly employs emails, texts, or instant messages and showing that the material in question fits into that course of dealing, and connections between the person in question and the phone in question, coupled with other information about behavior as it relates to content.
    - The fact that a person's name appears in the header as the "sender" should not be enough to authenticate the email as being from that person, just as self-identification by a telephone caller is insufficient to authenticate the call as being from that person.
    - However, self-identification can complement other authenticating factors such as circumstances, content, internal patterns and extrinsic evidence.

- Stronger circumstantial evidence would be a showing that the actual email address, e.g., mailto:johndoe@aol.com, matches an account in that person's name with the indicated internet service provider, although this is not necessarily sufficient by itself because it is not technically difficult to send an email message using another's email address.
- In most modern cases, courts have relied primarily on the content of the message as a basis for authenticating emails. If an email contains particularized information that only the purported sender is likely to know, this will authenticate the email to the same extent that such knowledge would authenticate a written message. Obviously the more specialized or unique the information, the more such content tends to authenticate the message as being from a particular sender who has such knowledge.
    - Particularized content may include information about serial numbers, credit card numbers, ordering information, personal transactions, private communications, particular relationships, coded communications, and other types of private information, or at least information that is not known to the general public.
- A common type of content used to authenticate is content given in reply to an earlier email message. An email purporting to be a reply to an earlier message sent to a particular person is likely to be authored by that person.
    - Often an email message will include the message to which it is responding as an attachment or even in the body of the message.
    - Even though it is possible that a reply is sent by a person other than the recipient of the original message, the danger is no greater here than for written messages.
- Other circumstances that can be used to help authenticate an email include the fact that the purported sender promised to send an email to the recipient and one was later received, the fact that previous messages sent to a particular email address reached the purported sender of the email in question, or the fact that actions were taken by the purported sender in response to emails sent to the purported sender's address, such as the shipping of merchandise.
- Emails can also be authenticated under Rule 901(b)(3), which authorizes “comparison with an authenticated specimen by an expert witness or the trier of fact.” Thus emails that are not clearly identifiable on their own can be authenticated by allowing the jury to

compare them with specimens that have been previously authenticated.
    - Even if an email is successfully authenticated, it is not admissible to prove the truth of its content unless an additional foundation is laid showing that it fits an exception to the hearsay rule.
    - If the email is shown to be from a party opponent, this will ordinarily suffice to allow its introduction into evidence as an admission.
    - An email forwarding another email may sometimes constitute an adoptive admission of the original email by the person forwarding it.
    - In unusual circumstances, an email statement may qualify as a present sense impression or an excited utterance.
  - Emails, even if made in the course of business, do not necessarily qualify for admission as business records. While emailed billing statements and similar records may qualify, routine personal and professional email communications, like routine written correspondence, often fail to satisfy the exception because they lack the regularity and systematic checking of information that justifies making business records an exception to the hearsay rule.
  - The procedures for authenticating printouts of online conversations in internet "chat rooms" are essentially the same as those for authenticating emails.

Social Media –

- Modern cases have increasingly faced the question whether evidence from social media (Facebook, MySpace, Twitter, and others) should be admitted.
- Authentication issues resemble those found with other forms of electronic communication, but one distinguishing factor is that social media often involve postings that are accessible to large numbers of people, and sometimes to the entire world.
- It is uncertain whether social media accounts are more easily hacked than email accounts, but obvious concerns about security of social media arise, and it may well be that more people have both motive and access to social media, which heightens concerns over security and possibly malicious and fraudulent postings.
- The Maryland Supreme Court observed that "authentication concerns attendant to emails, instant messaging, and text messages differ significantly from those involving a MySpace profile and posting printout, because such

correspondence is sent directly from one party to an intended recipient or recipients, rather than published for all to see."

- As with other forms of electronic communication, the challenge is usually not in proving that a particular communication was received or posted, and the concern is rather in learning the identity of the sender or maker.
    - A mere showing that the message was sent from a particular account or posted on a particular web page is not necessarily sufficient to authenticate the message as being from the owner of that account or web page, and more should be shown to establish the identity of the person posting the message, such as evidence that the originating site has security features that tend to assure the identity of the source.
- The authentication method most commonly used by proponents of social media evidence is to demonstrate its distinctive characteristics.
    - Under Rule 902(4) the proponent must show that the circumstantial evidence of the case combined with the "appearance, contents, substance, internal patterns, or other distinctive characteristics" of the exhibit are sufficient to prove that the proffered evidence is what it is purported to be.
    - A distinctive characteristic particularly likely to persuade a court that the authentication requirement is satisfied is the use of code words known only to the parties.
- Circumstantial evidence varies significantly from case to case, and courts apply different levels of scrutiny when determining whether the authentication threshold has been satisfied. Some courts have applied a strict standard and others a more lenient one.
- If the proponent calls an authenticating witness to testify how a particular electronic communication is made, such as an expert from the company sponsoring the social media site, that person must be able to "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."
- Courts have held, however, that it is not essential to call such an expert, at least in cases where there are other forms of authenticating evidence available