ERROR 404: USER NOT FOUND Authenticating Social Media and other Electronic Evidence

by David J. Beck
and Cassie Maneen

I. Introduction

When introducing evidence at trial, one of a trial lawyer's greatest fears is to hear the words: "Objection. Lack of authentication," accompanied by the dreaded ruling, "sustained." This fear is heightened when attempting to introduce electronic evidence. To avoid such problems, it is critical that trial lawyers know exactly what is necessary to authenticate such evidence before offering it. Despite the greater frequency of electronic evidence in today's increasingly digital world, courts apply the same authentication principles that have long existed because the reliability considerations are essentially the same. A Pennsylvania court summarized well the common-sense approach of applying existing evidentiary frameworks to modern evidence like social media and instant message conversations:

> Essentially, appellant would have us create a whole new body of law just to deal with emails or instant

> messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. . . anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of [the rules of evidence and case law] . . . .[1]

Nonetheless, sponsoring parties of particular evidence should keep in mind that the threshold for authenticity is, by design, not an onerous one. Both the Texas and federal rules keep the preliminary judicial determination limited.[2] With this in mind, the steps you must take will differ depending on whether your case is in Texas state court or federal court.

---

[1] *In Re F.P.*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).

[2] *See Butler v. State*, 459 S.W.3d 595, 600 (Tex. Crim. App. 2015); *see also* Fed. R. Evid. 104 advisory committee's note, subdiv. (b) ("If preliminary questions of conditional relevancy were determined solely by the judge ... the functioning of the jury as a trier of fact would be greatly restricted and in some cases virtually destroyed. These are appropriate questions for juries.").

Authentication of electronic evidence, such as the contents of a website, data generated by an app, or information taken from a mobile phone or hard drive can pose a real challenge. Broadly stated, you must convince the trial court that the tendered evidence has not been altered or hacked, that it comes from a certain source, and that it is what it purports to be. In today's online world, that is no easy task.

Evidence from websites can present serious authenticity issues because their content will change over time. Information *currently* on a website is less of an authenticity problem because the parties can simply access the website and confirm its content. However, proving up *historic* information from a website raises the issue of whether the information was actually posted as the proponent says it was. The relevant inquiries are: What was actually on the website at the relevant time? Does the exhibit or testimony accurately reflect its content, and, if so, is it attributable to the owner of the site? Evidence must be submitted to address each of these questions.

II. Document Production

Texas Rule of Civil Procedure 193.7 provides some assistance in most readily establishing authentication. The rule indicates that authenticity of evidence for use at trial may be established when documents, including emails or other electronic evidence, are produced by a party in discovery. The fact that such evidence is in the possession of the opposing party and

produced in discovery suggests that it is authentic. In federal court, the act of production can constitute a statement of a party-opponent and therefore be evidence of authenticity.[3] Today, it has become common practice to include written discovery requests targeting an opposing party's online presence, such as social media accounts, email addresses, and the preservation of communications in messaging applications like WhatsApp.

But what if the desired electronic evidence is *not* included in the opposing party's legitimate discovery responses? How do you authenticate that evidence? Can authenticity be established through interrogatories or requests for admission? These discovery avenues, while available, are unlikely to be successful if the electronic evidence was generated *by a third party*. For example, one Texas Court of Appeals held that Facebook posts on a third party's account were not authenticated where the sponsoring witness was neither the owner of the account onto which the posts were made nor the owner of any of the accounts of the alleged posters.[4] The defendant, the court explained, had no part in the posting of the messages in question and, because the individuals purportedly responsible for the messages were not called to testify, there was no way of authenticating them.[5] Parties therefore need to be aware of what standard a particular court looks to when considering the authentication of electronic evidence.

---

[3] Fed. R. Civ. P. 801 (d) (2).

[4] *Dering v. State*, 465 S.W.3d 668, 670 (Tex. App.–Eastland 2015, no pet.).

[5] *Id.* at 673.

III. Applicable Standards

Regardless of whether a party produces the electronic evidence or acknowledges its authenticity in discovery, courts are generally divided regarding the *standard* for authentication of social media evidence. The standard for authenticating such evidence in Texas is fairly lenient, requiring only the introduction of facts from which a reasonable juror could find that the evidence was created by the purported author.[6] More specifically, "in performing its Rule 104 gate-keeping function, the [Texas] trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic."[7] In contrast, other jurisdictions such as Maryland impose a relatively high bar, requiring the proponent to all but eliminate the possibility of phony authorship of social media content.[8] To illustrate, the *Griffin* court held that the potential for abuse and manipulation of a social networking site requires a greater degree of scrutiny and accounted for this by requiring witness testimony that *closely linked* the creator to the content, putting an increased burden on the proponent of the evidence

---

[6] *See, e.g., Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012); *Manuel v. State*, 357 S.W.3d 66 (Tex. App.—2011); *accord United States v. Vayner*, 769 F.3d 125 (2d Cir. 2014).

[7] *Tienda* at 638.

[8] *See Griffin v. State*, 19 A.3d 415, 423 (Md. 2011).

to affirmatively demonstrate that the evidence is not faked.[9]

Given these varying standards, practitioners should be armed with knowledge of the various approaches the evidentiary rules provide to authenticate social media and other electronic evidence. Consider the following hypothetical: Imagine a breach of contract claim between two corporate entities. The plaintiff is also seeking to pierce the corporate veil because it believes defendant is a mere shell company controlled by its better-capitalized parent corporation. The defendant's key company witness and corporate representative asserts that the defendant-company and its parent-corp. are wholly distinctive entities. Though this witness works for the defendant-shell entity now, he used to have a role with the "entirely separate" parent corporation. Assume further that the plaintiff comes across the same witness's Facebook page and discovers that he posted from a defendant-company dinner—during the relevant time period—that he was "glad to have worked for the *same* company his whole 20-year career!" Can plaintiff use this evidence to justify piercing the corporate veil? If so, how can this post be authenticated? There may be a few approaches available.

IV. Personal Knowledge

The Texas authentication rule, Tex. R. Evid. 901(b), sets forth ten different methods available to authenticate evidence. The most useful digital evidence authentication method is

[9] *Id.*

Rule 901(b)(1), which requires the witness to have personal knowledge of the evidence.

The proponent of electronic evidence can establish authenticity by producing evidence sufficient to support a finding that the proffered item is what it claims to be.[10] Can the witness testify, based on his or her personal knowledge, that the email came from a person's email address, at a time when that person was in the office, discussed a topic about which he or she had knowledge, and bears that person's name? If so, that testimony is sufficient to establish authentication in Texas state court under Tex. R. Evid. 901(b)(1). Caution must be heeded, however, because mere conclusory language is "not sufficient testimony" that an exhibit "is what it is claimed to be" as required by the rule.[11]

The personal knowledge method is also available in federal court. Fed. R. Evid. 901(b)(1) similarly permits authentication through the testimony of a witness *with knowledge* that the evidence is what it purports to be. For example, in *United States v. Barlow*, the court held that a chat log was properly authenticated by the testimony of a witness who created, and thus participated in, the chat.[12] The electronic communication was authenticated through the testimony of the author, who stated that he drafted

---

[10] *See id.*

[11] *Brown v. Tarbert, LLC*, 616 S.W. 3d 159, 164 (Tex. App.—Houston [14th Dist.] 2020, pet. denied).

[12] 568 F.3d 215, 220 (5th Cir. 2009).

or sent the communication.[13] Obviously, a recipient of the communication also may authenticate it. Such was the case in *Talada v. City of Martinez,* where a California court found e-mails were properly authenticated through a declaration from the recipient that they were true and correct copies.[14]

Once one piece of electronic evidence is authenticated, another potentially helpful method available is the related Tex. R. Evid. 901(b)(3), which pertains to the *comparison* of the proposed evidence with the previously authenticated item. Under this method, for example, a witness can authenticate electronic evidence based on personal knowledge and then compare the similarities between that item and the second proposed item. If multiple similarities between the two pieces of electronic evidence exist, the second item can be authenticated as well.

Applying these methods to our corporate veil example, the Facebook post may be authenticated most simply by getting the company witness to testify to it being his post. If this route proves difficult, another witness who has personal knowledge of the corporate representative's Facebook page (*i.e.*, is his "friend" on that social networking site) and knowledge of when the post was made may establish its authenticity. Lastly, using the comparison method, other emails or communications authenticated by this witness may bear the same signature sign-off on all communications that appear in the post. By showing

---

[13] *Id.*

[14] 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009).

the court these idiosyncratic similarities, the threshold for authenticity under the comparison method may be satisfied.

The hard reality is that a witness with personal knowledge of a Tweet or Slack message, for example, may not always be available. In that instance, recognize that there are other useful methods to authenticate electronic evidence.

V. Circumstantial Evidence

Another useful authentication method is set forth in TEX. REV. EVID. 901(b)(4), which allows electronic evidence to be proven by circumstantial evidence. That rule permits a party to authenticate such evidence by using the "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." In federal court the virtually identical FED. R. EVID. 901(b)(4) also requires a consideration of the totality of "all the circumstances." While any one factor may be insufficient to warrant admissibility under either the Texas or federal standard, when circumstantial evidence factors are weighed together, authenticity may be established.[15]

To demonstrate, in *United States v. Barlow* the court held that internet chat logs of correspondence between defendant and a police contractor posing as a minor were adequately authenticated through the contractor's testimony alone which,

[15] For an excellent discussion of the many circumstantial factors that may be relevant to determining authenticity, *see* Grimm, Capra, and Joseph, "Authenticating Digital Evidence", 69 Baylor L. Rev. 1, 15-22 (2017).

when taken as a whole, supported that the chats were what they purported to be.[16] Similarly, in *Butler v. State* the court determined that the content and context of text messages themselves were sufficient circumstantial evidence in combination with the fact that the same phone number had texted the plaintiff previously to authenticate the texts.[17] Accordingly, if enough circumstantial evidence can be adduced, authentication of social media or online evidence also may be accomplished.

In truth, many cases across jurisdictions have dealt with the new world of online evidence by relying on circumstantial evidence to establish the authenticity of electronic evidence. In *Dickens v. State*, for example, a Maryland court upheld a decision to admit text messages proffered for the purpose of showing that the sender threatened his estranged wife over a period of time before he murdered her.[18] In reaching that conclusion, the court relied on circumstantial evidence that two of the messages were sent during a period of time consistent with the timeline of criminal events and that the substantive content of all three messages pointed to the defendant's authorship.[19] Likewise, in *People v. Pierre*, a New York court held that an instant message was properly authenticated as a communication from the defendant after "[t]he accomplice witness ... testified to the defendant's [instant messenger] screen name," and "[another witness]

---

[16] 568 F.3d 215, 220 (5th Cir. 2009).

[17] 459 S.W.3d at 600.

[18] 927 A.2d 32, 37 (2007).

[19] *Id.*

testified that she sent an instant message to that same screen name, and received a reply, the content of which made no sense unless it was sent by defendant [and] there was no evidence that anyone had a motive, or opportunity, to impersonate defendant by using his screen name."[20]

It is, therefore, important when preparing for trial to collect as much circumstantial evidence as possible to ensure that a totality of circumstances approach weighs in favor of authentication of any electronic evidence. This may include review of additional

[20] 838 N.Y.S.2d 546, 549 (2007); *see also, e.g., State v. Thompson*, 777 N.W.2d 617, 623 (N.D. 2010) (holding that evidence that a recipient of threatening text messages was familiar with the defendant's phone number and his distinctive electronic signature was sufficient to establish that the messages were sent by the defendant); *United States v. Lewisbey*, 843 F.3d 653, 658 (7th Cir. 2016) (finding incriminating Facebook posts properly authenticated because, among other circumstantial links between the defendant and the Facebook account, the app on a mobile phone confiscated from the defendant was linked to the account from which the incriminating statements were posted); *Allen v. Zonis*, 6 Wash. App. 2d 1045 (2018), *10–12 (holding, in an internet stalking case, that the plaintiff's testimony that the all capital letter writing style in abusive emails she received from anonymous senders matched what the defendant had sent her previously was sufficient circumstantial evidence to authenticate the author of the posts); *Burgess v. State*, 742 S.E. 2d 464, 467 (Ga. 2015), (finding that a Myspace account bearing the name "Oops" was properly authenticated through an officer's testimony that he had confirmed with the defendant's sister that the defendant's nickname was "Oops."); *Commonwealth v. Jackson*, 2022 PA Super 156, 283 A.3d 814 (2022) (reasoning that substantial circumstantial evidence that linked two social media accounts to the defendant was sufficient to properly authenticate photos and videos posted to online accounts because both accounts had usernames containing nicknames used by defendant, both accounts featured pictures of defendant taken by himself and by others, and the information contained in the accounts included substantially similar biographical sections and identical hashtags, locations, and statements to another account admitted to by the defendant.).

posts from the target witness for similar styles; investigation of the online connections of the declarant who may be able to corroborate the post; or an inspection of the alleged poster's various devices for evidence of linked accounts.

VI. Lessons Borrowed from Hearsay

May the business records exception to the hearsay rule be used to satisfy an authentication requirement? If the effort seeks to authenticate *the contents* of the business record, the answer may be "no" because the content may not have been supplied by a person connected to the business. The content therefore cannot automatically be authenticated as a business record under FED. R. EVID. 902(11). However, FED. R. EVID. 902(11) and (12) render self-authenticating business records that are certified as satisfying FED. R. EVID. 803(6) by "the custodian or another qualified witness." Information extracted from websites that are maintained by, for, and in the ordinary course of business or other regularly conducted activity of the site owner can satisfy this standard.[21]

On the other hand, if the effort seeks to authenticate only information such as metadata regularly maintained by the business, the answer to whether a business records foundation can provide authenticity is probably "yes." It has long been the case that where writings are automatically computer-generated and are non-assertive, or not made by a "person," courts

[21] *United States v. Hassan*, 742 F. 3d 104, 132 (4th Cir. 2014).

hold that they do not constitute hearsay at all, as they are not "statements."[22]

As the law develops with the growing necessary use of electronic evidence, similar technological assurances such as internet archives, cloud-based back-ups of social media profiles, and other automated computerized fail-safes may make authenticity an easier hurdle to overcome than otherwise expected.

VII. Certification

Existing evidentiary rules also provide for certification of certain evidence as authentic by definition. TEX. R. EVID. 902 addresses self-authentication and is substantively identical to most of FED. R. EVID. 902. Texas Rule 902(10)(a) addresses self-authenticating business records accompanied by an affidavit. However, the affidavit must be by the custodian of record or other qualified witness, which can create another hurdle.

Two fairly recent amendments to the Federal Rules of Evidence have authorized self-authentication of digital evidence by certification. FED. R. EVID. 902(13) allows the use of a certification to authenticate evidence generated by an electronic process or system but dispenses with the business records foundation. FED. R. EVID. 902(14) authorizes a certificate to authenticate a digital

---

[22] *See, e.g., Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 564 (D. Md. 2007) (mem. op.); *Ly v. State*, 908 S.W.2d 598, 600 (Tex. App.—Houston [1st Dist.] 1995, no pet.).

copy of data taken, for example, from a mobile phone or hard drive. However, Rule 902(13) and Rule 902(14) certifications establish *only* authenticity, not admissibility.

To be clear, the proponent of any piece of authenticated evidence must still demonstrate the evidence's relevance and overcome any other admissibility issues. At a minimum, however, the existing framework to establish a piece of digital evidence as reliably authentic can be used to satisfy the initial evidentiary hurdle.