The Computer & Internet Lawyer

Volume 31 ▲ Number 2 ▲ FEBRUARY 2014

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief

Features

Current Developments

Wolters Kluwer
Law & Business

"Certifying" Documents *via* Third-Party Software: Binding on the Court?

By William R. Wohlsifer and Tyler L. Thomas

Does the use of third-party software to certify documents or signed contracts outweigh the time and costs allocated to the process? is a common query from corporate clients. As an attorney, a more pertinent question in need of answering would be: Is the third-party software certification process necessary in order to meet today's evidentiary standards regarding electronic copies of documents as business records? The specific focus of this article is the admissibility into evidence of the conversion of original paper documents and contracts to digital image files, then back to paper form for use in court. Although digital image copies are widely recognized at federal and state levels to be admissible, in *Lorraine v. Market American Insurance Co.*,[1] the court identified a "growing recognition that more care is required to authenticate ... electronic records than traditional 'hard copy' records."[2] Determining the answers to these questions requires an examination of federal and state laws and court precedence in place regarding use of digital image copies as evidence.

Uniform Photographic Copies of Business and Public Records as Evidence Act

One of the first federal laws to recognize the evidentiary issue of photographic copies was the Uniform Photographic Copies of Business and Public Records as Evidence Act (UPA)[3] enacted in 1949. The UPA authorizes the destruction of original paper records that have been accurately reproduced.[4] Codified in Title 28, Ch. 115, U.S.C. §1732, it provides:

> If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any photographic, photostatic, microfilm, microcard, miniature photographic, or other process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law. Such reproduction, *when satisfactorily identified*, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not and an enlargement or facsimile of such reproduction is likewise admissible in evidence if the original reproduction is in existence and available for inspection under direction of court. The introduction of a reproduced record, enlargement, or facsimile does not preclude admission of the original. This subsection shall not be construed to exclude from evidence any document or copy thereof which is otherwise admissible under the rules of evidence.[5]

All original paper copies and digital copies of documents and contracts or other documents that are responsive to a filed or reasonably foreseeable lawsuit should not be destroyed, even if such destruction is part of an organization's established records retention policy as the court stated in *In re the Prudential Insurance Co. of America Sales Practices Litigation*.[6]

The *Lorraine* Analysis of Federal Rules of Evidence 901 and 902

While documents can be destroyed once they are copied, except for the circumstances enumerated above, the electronic copies must still meet evidentiary standards in compliance with state and federal rules of evidence. The

William R. Wohlsifer is a commercial litigation attorney with the law firm of William R. Wohlsifer, PA. He practices in both Florida and Washington, DC, with an emphasis on copyright and trademark infringement. Mr. Wohlsifer received his BA in political science from The University of Central Florida and his JD, cum laude, from The St. Thomas University School of Law. **Tyler L. Thomas** is a third-year student at the Florida State University College of Law and a clerk at William R. Wohlsifer, PA. His studies focus on commercial litigation, real estate law, intellectual property, and corporate law. A graduate of the University of Florida, he is a member of both the *Journal of Land Use & Environmental Law* and the *Business Review*. This article originally was published in the September/October 2013 issue of *The Florida Bar Journal* and is reprinted with permission.

Lorraine court took on the challenge of analyzing the evidentiary rules and case law that control the admissibility of electronic evidence.[7] The court found that Federal Rule of Evidence (Fed. R. Evid.) 901(a) requires that the electronically stored information be shown to be authentic by showing that it is what the party claims it to be—not a particularly difficult obstacle to overcome.[8] However, the court noted that "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[9]

Courts may eventually expressly recognize third-party software as a self-authenticating means or at least deem it a rebuttable presumption, but they do not uniformly do so at this time.

The *Lorraine* court further found that Fed. R. Evid. 901(b) provides examples of how authentication may be accomplished.[10] In particular, Rule 901(b)(4) provides, "Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[11] The third-party software certification process does not necessarily contribute to satisfying these examples. When discussing this particular subsection, the court in *Lorraine* noted:

> This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions.[12]

It is reasonable to expect the time-stamp feature of third-party software certification to assist a proffering party when a witness (the business records custodian) is called on to proffer a document as indeed, the "'final' or legally operative version."[13] Although the certification may add to the business records foundation, inclining the court to admit the proffered evidence, it is not dispositive on the ability to overcome objections of the opposing party and your client should be advised as such. Courts may eventually expressly recognize third-party software as a self-authenticating means or at least deem it a rebuttable presumption, but they do not uniformly do so at this time.

The *Lorraine* court also discussed the issues surrounding Fed. R. Evid. 902 and its 12 methods by which documents or contracts may be authenticated without extrinsic evidence (self-authentication).[14] Rule 902(7) provides that exhibits may be self-authenticated by "[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."[15] This method reflects the mandates of Rule 901(b)(4), but with more specificity. The court also evaluated Rule 902(11) and found it to be "extremely useful because it affords a means of authenticating business records under Rule 803(6) ... without the need for a witness to testify in person at trial."[16] Rule 902(11) provides, (11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying 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 those 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. 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 declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.[17]

According to the *Lorraine* court, the rule "was intended to set forth a procedure by which parties can authenticate certain records of regularly conducted activity, other than through the testimony of a foundation witness."[18] As convenient as this may sound, some courts take a more demanding approach for authentication and still require a witness.

In re Vee Vinhnee: The Strict Standard

Currently, "there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed" and "more courts have tended towards the lenient rather than the demanding approach."[19] Since for the most part you cannot pick and choose your court, the prudent records custodian must balance the cost of preparation for the strictest court against the value of full and complete preparation. In one case in particular, *In re Vee Vinhnee*,[20] the court established the more stringent approach:

> The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created...; Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.[21]

In order to meet the stricter standard for authenticating electronic business records, the court adopted an 11-step foundation proposed by Professor Edward Imwinkelried:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout of certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.[22]

As can be seen, to meet this strict standard, counsel should advise his or her client to implement a number of safeguards to preserve the latter use of purposely destroyed hard copy evidence. The third-party software certification process provides an added layer of proof when establishing the foundation for admissibility in court. The *Lorraine* court believes that "[t]he methods of authentication most likely to be appropriate for computerized records are [Federal Rules of Evidence] 901(b)(1) (witness with personal knowledge); 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics); and 901(b)(9) (system or process capable of producing a reliable result)."[23] However, it should be noted that the method of authentication is somewhat less stringent for the governmental client.

Florida Law

Florida Statutes § 92.29 (2012) provides statutory admission of electronically reproduced documents for government entities.

> Photographic or electronic copies.—Photographic reproductions or reproductions through electronic recordkeeping systems made by any federal, state, county, or municipal governmental board, department or agency, in the regular course of business, of any original record, document, paper or instrument in writing or in an electronic recordkeeping system, which is, or may be, required or authorized to be made, filed, or recorded with that board, department or agency shall in all cases and in all courts and places be admitted and received as evidence with a like force and effect as the original would be, whether the original record, document, paper, or instrument in writing or in an electronic recordkeeping system is in existence or not.

Private sector litigants in Florida do not enjoy the benefit of this brigl.t-line rule. The evidentiary standard for digital image copies of documents and signed contracts when introduced by a private litigant remains reliant on the business records foundation and the best evidence rule.[24] To this end, Florida, as most states, has adopted uniform federal acts, such as the UPA. Florida

Statutes § 90.951(3) provides: "If data are stored in a computer or similar device, any printout or other output readable by sight and shown to reflect the data accurately is an 'original.'"[25] Clearly, this language provides that digital images can satisfy the best evidence rule. "[A] memorandum, report, record or data compilation, in any form, if kept in the course of a regularly conducted business activity and if it was the regular practice of that business activity" may be admitted into evidence under the best evidence rule.[26] The court in *Jackson v. State*[27] held

> In order to be admissible, a business record pursuant to section 90.803(6)(a) must be shown to have been: 1) [m]ade at or near the time of the event; 2) [b]y or from information transmitted by a person with knowledge; 3) [k]ept in the course of a regularly conducted business activity; and 4) [t]hat it was the regular practice of that business to make such a record.[28]

It should be emphasized that the witness or records custodian does not need to have personal knowledge of the contents of the record being proffered, but rather personal knowledge of the business' record-keeping practice.[29] As Florida evidence scholar Charles W. Ehrhardt opines, "[a]lthough some require stricter foundational standards for electronic records focusing on the reliability of the system, the better view is that demonstrating each of the elements traditionally required for the [business records] exception is sufficient to demonstrate the underlying reliability of the record."[30]

It may be beneficial for your client to include a clause in its multi-party documents that specifically provides for application of the UETA.

The Uniform Electronic Transaction Act (UETA) is adopted by Florida in F.S. § 668.50. This statute applies to transactions in which each party has agreed by some means to conduct electronic transactions.[31] Notably, this statute states that "evidence of a record or signature may not be excluded solely because the record or signature is in electronic form."[32] Therefore, it may be beneficial for your client to include a clause in its multiparty documents that specifically provides for application of the UETA. For example, the following suggestive language could be inserted to show the parties' intent to bring the anticipated electronic version of the document into the purview of the UETA:

> Party A hereby acknowledges that it is an ordinary and regular record-keeping business practice of Party A to ultimately scan or otherwise convert this written Agreement into digital form for the purpose of electronic storage and thereupon destroy the original. Party B hereby agrees that any subsequent reproduction of Party A's electronically stored version of this written Agreement that may later be produced by Party A in the ordinary course of its record-keeping procedure, shall have the same full force and effect as the destroyed original, for all purposes, including admissibility into evidence in all jurisdictions and tribunals.

Again, the proffering party must still satisfy the business records foundation in order to overcome the best evidence rule. However, including a clause allowing for coverage under the UETA may stifle an objection to the electronic form of the document.

Conclusion

The admissibility of electronic copies of documents comes down to a showing of the trustworthiness and accuracy of the reproduction of the original. While most courts now tend toward a more lenient rather than a demanding approach to authenticate electronic records, it appears better to err on the side of caution until the evolution is complete. Certifying documents and signed contracts *via* third-party software adds to the predicate required under Florida Statutes § 90.803(6)(a) to lay down the foundation required to overcome an objection to admissibility and aid in establishing the trustworthiness and accuracy of the digital reproduction. In some instances, third-party software certification may alleviate the need for the in-person appearance of the proffering party's records custodian, but in the opinion of the author, most times it will not. Third-party software certification (including time-stamping) does not presently rise to self-authentication and is not binding on the court.

Based on the understanding that the time and costs associated with a third-party software certification process are considerable, your client should be advised on balancing the beneficial return on such costs. Because third-party software certification only adds to the business records foundation, it is not uniquely probative. Your client's sound records retention policy may add to the admissibility of electronically stored records in the same manner that evidence is traditionally proffered, that is, by laying down a foundation through the testimony of a witness with personal knowledge of the document's history. Indeed, even the original document,

when available, is put to the same scrutiny, but for statutorily self-authenticated evidence.

The underlying challenge to the authenticity of an electronically stored document is to overcome the possibility that it could have been altered sometime during the interval between when it was digitally reproduced and the time of trial. Although the same concerns as to alteration can be raised in an objection to the admissibility of original hard copies, the North Carolina Supreme Court in *State v. Springer*[33] aptly noted that "[t]he rules of evidence governing the admissibility of computerized business records should be consistent with the reality of current business methods and should be adjusted to accommodate the techniques of a modern business world, with adequate safeguards to insure reliability."[34] Third-party software certification provides such a safeguard by facially comparing and time-stamping the document, professing to certify that it is the same as the original, and by the custodian of records e-signing it; but is not by itself probative of the accuracy of the reproduction.

Does the cost outweigh the benefit? For government attorneys the answer is a simple yes because of the reduced burden made available under Florida Statutes § 92.29 (2012). For private litigants this is a business decision for the client to make, taking into account the advice of counsel with knowledge of these evolving trends.

Notes

1. Lorraine v. Market Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).
2. *Id.* at 557.
3. 28 U.S.C. § 1732 (2012), available at *http://www.law.cornell.edu/uscode/text/28/1732*.
4. *Id.*
5. *Id.* (Emphasis added).
6. In re the Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598 (D.N.J. 1997). *See, e.g., id. at* 615.
7. *Lorraine*, 241 F.R.D. at 534.
8. *Id.* at 541-542 (*citing* Fed. R. Evid. 901(a)).
9. *Id.* at 542.
10. *Id.* at 544 (*citing* Fed. R. Evid. 901(b)).
11. Fed. R. Evid. 901(b)(4).
12. *Lorraine*, 241 F.R.D. at 547.
13. *Id.*
14. *Id.* at 549-552 (*citing* Fed. R. Evid. 902).
15. Fed. R. Evid. 902(7).
16. *Lorraine*, 241 F.R.D. at 552 (*citing* Fed. R. Evid. 902(11)).
17. Fed. R. Evid. 902(11).
18. *Lorraine*, 241 F.R.D. at 552.
19. *Id.* at 558.
20. In re Vee Vinhnee, 336 B.R. 437 (B.A.P. 9th Cir. 2005).
21. *Id.* at 444 (this analysis is relevant, but more applicable to internal business records, such as invoices, ledgers, etc., rather than mutually executed contracts).
22. *Id.* at 446-447 (*citing* Edward J. Imwinkelried, Objections at Trial § 4.03(2)).
23. *Lorraine*, 241 F.R.D. at 559.
24. *See* Fla. Stat. § 90.952.
25. *Id.* at § 90.951(3).
26. *Id.* at § 90.803(6)(a).
27. Jackson v. State, 738 So. 2d 382 (Fla. 4th DCA 1999).
28. *Id.* at 386.
29. *See* Specialty Linings, Inc. v. B.F. Goodrich Co., 532 So. 2d 1121, 1122 (Fla. 2d DCA 1988).
30. Charles W. Ehrhardt, West's Florida Practice: Florida Evidence § 803.6b (2013).
31. *See* Fla. Stat. § 668.50 (2012).
32. *Id.* at § 668.50(13).
33. State v. Springer, 197 S.E.2d 530 (1973).
34. *Id.* at 536.