DocuSign

FENWICK

Using E-Signatures in Court — The Value of an Audit Trail

Tyler G. Newby
Partner, Litigation
Fenwick & West LLP

From antiquity through the middle ages, the authenticity of a document's signature was confirmed by using a signet ring pressed into a wax seal. The signet was unique to the signer, so the presence of the stamp on a document provided assurance that the document had not been forged. While wax seals continue to carry romantic appeal today, they are hardly suitable for the speed and geographic reach of modern commerce. Fortunately, the process of creating a verifiable signature has evolved significantly in the last 1,000 years or so, and one can think of the digital audit trail provided by electronic signature services as the modern-day signet stamp.

The primary purpose of a signature on an agreement is to bind the signatory to the obligations set forth in the agreement if a dispute arises over that party's performance. Therefore, the ability to authenticate a signature as that of the signer in court is necessary in a contract dispute where a party disputes that he is bound to the agreement. Authenticating evidence is subject to a low evidentiary burden. In the United States, Federal Rule of Evidence 901 provides that authentication requires the proponent to "produce evidence sufficient to support a finding that the item is what the proponent claims it is." This rule is a far lower burden than proof by a "preponderance" (more likely than not) of evidence that is used in other situations in court. So how have courts approached authentication in the context of electronic signatures?

First, it is useful to look at how analog "wet ink" signatures are authenticated in court when, for example, a party attempts to show that the scribble on a signature block is the signature of another party. If contested, parties typically have used comparisons between known signatures and the questioned signature with corroborating witness testimony that a separate individual saw the signing of the document or the testimony of handwriting experts confirming the similarity of the signatures. All the proponent needs to produce is "sufficient" evidence that the signature is that of the other party; questions as to the strength of that evidence will go to the weight the fact finder gives the evidence in court.

E-signatures backed by an audit trail help clear this low authenticity bar even more easily. Audit trails are digital records maintained by the e-signature service that, among other things, identify when a document was sent, opened and signed, as well as the names, email addresses and unique signing identifiers of the signatories. They also may include records like IP addresses or machine IDs to further trace when and where a document was opened and signed.

While not strictly necessary under the rules of evidence, audit trails have proven very effective in authenticating a record to demonstrate that the e-signature is that of the signatory. Federal district courts have commonly found that detailed e-signature audit logs satisfy this authentication requirement. In *Schrock v. Nomac Drilling, LLC*, 2016 WL 1181484 (W.D. Pa. 2016), for example, an employer sought to enforce an electronically signed agreement with a former employee. The court rejected the former employee's challenge to the authenticity of the electronic signature as his own because the employer presented evidence that the e-signature program required the entry of the last four digits of the former employee's social security number, and the audit trail showed that the document was electronically signed at a specific location at a time when the former employee was at that same location.

Similarly, in Obi v. Exeter Health Resources, Inc., Case No. 18-cv-550-SM, 2019 WL 2142498 (D. N.H. May 22, 2019), a federal district court in New Hampshire rejected the party's argument that her electronic signature on an agreement had been forged, where DocuSign eSignature audit logs showed that she had viewed and signed the agreement through her DocuSign eSignature account. In another case involving a party seeking arbitration [Moton v. Maplebear Inc., No. 15 CIV. 8879 (CM), 2016 WL 616343 (S.D.N.Y. Feb. 9, 2016)], a U.S. district court in the Southern District of New York, found that an e-signature provider's "time-stamped audit trail that tracks – using IP addresses and other identifying data – when each [signatory] receives,

views and executes each agreement" was sufficient to establish that the signer's signature was his own, and that this evidence, in turn, established assent to the agreement.

State courts have reached the same conclusion. In IO Moonwalkers, Inc. v. Bank of America, 814 S.E.2d 583 (N.C. Ct. App. 2018), a DocuSign eSignature audit trail showed that a business accessed a document it claimed it had not signed, which supported the trial court's finding that the business had ratified the signature of the agreement with the other party. There, the party had argued that no one affiliated with his business had signed the agreements at issue and speculated that one of the other party's employees had signed them. However, the evidence showed that the owner of the business had provided the other party with an email address to send agreements for electronic signature, and that the business was familiar with how DocuSign eSignature worked. The DocuSign eSignature audit trail showed that someone with access to the business's email account accessed and then signed the agreements at issue. This audit trail evidence was critical to the court's rejection of the business's effort to create a material dispute of the facts in the case as to whether the agreements at issue had been signed by a representative of its business:

> Were this a more traditional contract negotiation, in which the parties had mailed proposed contracts back and forth, a sworn affidavit stating that Moonwalkers never reviewed or signed the contracts might be sufficient to create a genuine issue of material fact with respect to the knowledge element of ratification. But this case is different because [the other party] presented evidence from the DocuSign [eSignature] records indicating that it sent the merchant services agreements to Moonwalkers at the company email address. [The other party] also submitted evidence from the DocuSign [eSignature] records that someone with access to that email viewed both the emails and the accompanying contracts, electronically signed them, and later viewed the completed contracts, which were sent to Moonwalkers in a separate email.
>
> Simply put, the electronic trail created by DocuSign [eSignature] provides information that would not have been available before the digital age – the ability to remotely monitor when other parties to a contract actually view it.

Harpham v. Big Moose Inspection, 2015 WL 5945842 (Mich. App. Oct. 13, 2015) also found a more rudimentary audit trail of the party's receipt and electronic signing of agreement was sufficient to overcome the party's unsupported affidavit that he did not recall signing the agreement.

These cases demonstrate that, while audit trails may not be required to authenticate electronic signatures and establish assent to an agreement, they greatly simplify the task of an attorney who must overcome an adversary's claim that he did not sign an agreement or that his e-signature was somehow forged. These cases also reinforce the more general takeaway that an audit trail associated with other types of contracts, such as a clickwrap, also will greatly help in enforcing such contracts. Further, these cases demonstrate that not only does an electronic signature with an audit trail strengthen a party's position, it also provides no practical downside. Rather than needing to proactively cultivate corroborating evidence for a challenged paper-and-ink signature, counsel can justifiably rely on an e-signature audit trail to provide heightened substantiation of the authenticity of an electronic document.

This article was originally published by Fenwick & West, LLP

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040