SHUTE, MIHALY & WEINBERGER LLP

396 HAYES STREET, SAN FRANCISCO, CA 94102
T: (415) 552-7272 F: (415) 552-5816
www.smwlaw.com

RICHARD S. TAYLOR
Attorney
rtaylor@smwlaw.com

October 2017

Streamlining Agency Operations with Electronic Signatures

Does your agency require "wet-ink" signatures on contracts, staff reports, or permit applications? Electronic signatures have been valid in California since 2000, but many agencies have been reluctant to make extensive use of the tool given legal and practical uncertainties. Recent legislation and lessons learned by early adopters have reduced the uncertainty, making electronic signatures a more attractive tool. Read on for an overview of the key features of the laws surrounding electronic signatures and suggestions on factors to consider in developing policies for use of electronic signatures.

Laws Governing Electronic Signatures

What exactly is an electronic signature? The answer is surprisingly broad. An electronic signature is "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record." Civ. Code § 1633.2(h). As you may have guessed from your own online activity, this can be as simple as checking a box or can involve complex multi-factor authentication using a third-party service.[1]

Electronic signatures stand on equal footing with their analog counterparts. Neither a contract, record, or signature can be denied legal effect or enforceability solely because it is in electronic form. If a law requires a signature, an electronic signature meets that requirement. Civ. Code § 1633.7. There are some exceptions to this sweeping rule, such as for various estate documents, some Uniform Commercial Code transactions, and others set forth in Civil Code section 1633.3.

As with traditional signatures, it is important to verify that an electronic signature is in fact the signature of the person purporting to have signed the document. To this end, the law provides that an "electronic signature is attributable to a person if it was the act of the

[1] Even a scan of a wet signature in a .pdf file falls within the black letter terms of this definition. And under Evidence Code sections 1521 and 1550, a physical copy of a wet signature, in the absence of the wet signature itself, can be acceptable evidence of a party's agreement.

person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." Civ. Code § 1633.9(a). This "is determined from the context and surrounding circumstances at the time of [the signature's] creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law." Civ. Code § 1633.9(b).

These rules are set forth in the Uniform Electronic Transactions Act (UETA), adopted in 1999 and codified beginning at Civil Code section 1633.1. California's law is based on a model statute adopted by all but 3 other states. The federal corollary is the Electronic Signatures Global and National Commerce Act (ESIGN), adopted in 2000 and found at 15 U.S. Code section 7001. ESIGN applies to contracts in interstate commerce and specifically does not preempt state enactments of UETA that conform to the model statute. 15 U.S.C. § 7002.

Public agency attorneys may also be familiar with the term "digital signature." A digital signature is a specific type of electronic signature—one that must satisfy more exacting security criteria than an electronic signature. The term was adopted by the state legislature in 1995 in Government Code section 16.5. Until amended in 2015, the wording of section 16.5 could be read as suggesting that "digital signatures" were the only type of electronic signatures that could be used by public entities. The 2015 amendments now make clear that while public agencies may use digital signatures, they are also free to use electronic signatures in the same manner as businesses and individuals operating under UETA.

Policy Considerations

Agencies wishing to make use of electronic signatures should do so deliberately, taking into consideration the numbers and types of documents handled by the agency, the costs of current practices compared to electronic procedures, and the relative risks and benefits associated with the agency's current and proposed procedures. Before undertaking any significant reliance on the technology, an agency should develop policies or best practices to guide use of electronic signatures. Key questions to be considered include the types of signatures that the agency will use and accept, the types of documents for which electronic signatures may be used, and records retention procedures.

An electronic signature may be something as simple as a check box. While this approach promises convenience, it is not without risk. A party wishing to evade the obligations of a

contract may argue that the electronic signature is for some reason not valid. In reviewing such claims courts have considered factors such as:

- Did signing require a unique login ID and password?
- Is there evidence of the date, time, location, or IP address associated with the signature?
- Is the signature accompanied by personal information that only the signer would know?
- Is the signer aware that she is manifesting her assent to the terms of the agreement (e.g., did the signer check multiple boxes demonstrating that intent (likely acceptable) or is intent being shown only by a signature block automatically included in all e-mails (likely unacceptable).)[2]

Accordingly, the agency should determine the types of electronic signatures it will accept for various types of documents and ensure that the authentication tools used will allow it to make a clear showing in the event of litigation concerning "the context and surrounding circumstances at the time'' the signature was made. Civ. Code § 1633.9.

In considering the types of documents suitable for use of electronic signatures, the agency will again want to weigh the convenience of an electronic signature against the associated risks and costs. For internal workflow (e.g., documenting compliance with internal procedures) the authentication risks will likely be low. The agency might reach the same conclusion for straightforward recurring agreements with other public agencies. Agreements with outside vendors and with residents can present greater authentication risks and the agency may wish to impose stricter standards. The agency also may choose to set higher standards for contracts with high dollar amounts or liability risks.

UETA applies only when both parties have agreed to conduct a transaction electronically. Civ. Code § 1633.5(b). Therefore, in moving into the electronic realm an agency's policies should continue to allow for traditional signatures in circumstances where the contracting party will not agree to proceed electronically.

---

[2] *See, e.g., Ruiz v. Moss Bros. Auto Group, Inc.*, 232 Cal.App.4th 836 (2014) (arbitration clause not applicable where employer could not show that employee had signed the electronic document); *Espejo v. Southern California Permanente Medical Group*, 246 Cal. App. 4th 1047 (2016) (upholding arbitration agreement and describing evidence presented by employer to demonstrate validity of electronic signature); *J.B.B. Inv. Partners, Ltd. v. Fair*, 232 Cal. App. 4th 974 (2014) (in the context of settlement negotiations at issue, attorney's standard signature block in an e-mail not a valid electronic signature).

Finally, an agency's practices and policies should consider document retention. Electronic signatures are generally attached to electronic records. Like all records, these are subject to the State's records retention laws (*see, e.g.*, Gov't Code § 34090 et seq.) and the Public Records Act (Gov't Code § 6252(g)). UETA provides that records may be retained electronically if "the electronic record reflects accurately the information set forth in the record at the time it was first generated in its final form as an electronic record or otherwise, and the electronic record remains accessible for later reference." Civ. Code § 1633.12(a); *see also* Evidence Code § 1550. The agency will want to give careful consideration as to how best retain, track, retrieve, and destroy electronic records in the course of its operations.

For more information, contact SMW attorney Richard Taylor at rtaylor@smwlaw.com.