Electronic Signatures in Washington: New State Law Should Prompt Employer Best Practices Review

By Leila Javanshir and David Rice
June 4, 2020

Come June 11, 2020, Washington will join the majority of states in adopting the Uniform Electronic Transactions Act (UETA). Previously, Washington was one of the three outlier states to resist adoption since the UETA was published in 1999, applying a different statute (which has now been repealed).

What is the UETA?

The UETA is a state law that provides a framework for states to address the validity of electronic signatures for transactions related to business, commercial (broadly defined to include consumers), and governmental matters. It has been adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

What makes an electronic signature valid under the UETA in Washington?

The change from Washington's prior electronic signature to the UETA may not have much practical effect on employers. Under both statutes, unless state or federal law requires a "wet" signature, an electronic signature can be used and must be given the same legal effect. But the change is a reminder that employers who use electronic signatures should review their practices to ensure the electronic signatures they obtain are legally valid.

The UETA states that a signature may not be denied its legal effect and enforceability solely because it is in electronic form. The Act lays out four necessary elements that must be met for an electronic signature to be valid:

1. The parties must intend to sign;
2. The parties must consent to doing business electronically;
3. There must be a connection between the electronic signature and the associated record; and
4. The electronic signature records created for each transaction must be capable of retention and accurate reproduction for reference by all parties entitled to retain the contract or document.

But while these four elements must be met, they are not the end of the analysis. One of the bigger issues facing employers in states that have adopted the UETA is proving that an electronic signature is attributable to a specific individual.

Under UETA, an electronic signature is attributable to a person only if it can be shown it was the act of the purported signer. Whether that is shown "is determined from the context and surrounding circumstances at the time of" the action that purports to be the electronic signature.

Under UETA, courts will analyze the facts of each case to determine whether there is enough evidence to show that a specific individual was in fact the individual who completed the electronic signature. This analysis includes an assessment of the security measures employers have in place to prove that only the intended individual could have completed the electronic signature.

A 2019 court decision provides an example of how one employer successfully used electronic signatures. In Czerwinski v. Pinnacle Property Management Services LLC, 9 Wn. App. 2d 1047 (unpublished) (2019), an employee filed suit on multiple employment claims, and the employer moved to enforce an arbitration agreement that had been electronically signed by the plaintiff. The plaintiff challenged the enforceability of her electronic signature, claiming that she did not remember the agreement to arbitrate. The court held that the employer met its burden in proving that the employee signed the contract because in addition to obtaining the employee's typed signature, the employee was required to enter the last four digits of her social security number, authenticating her electronic signature. Further, the signature page unequivocally stated that upon signing the signatory would be required to arbitrate all employment-related claims against the employer. The arbitration agreement was enforced.

While Czerwinski predates Washington's recent adoption of the UETA, the same result almost certainly would have been obtained under the UETA.

If your business uses electronic signatures, below is a list of best practices to ensure the enforceability of those signatures under the UETA:

- Determine the jurisdiction that governs the transaction to verify any variances in the applicable UETA and whether the transaction can be conducted electronically;
- Seek explicit consent to execute documents and to transact business under the documents electronically (most often within the terms of the document being executed);
- Implement effective measures to verify the actual identity of the individual who is electronically signing a document. Examples include:
    - Requiring the signatory answer questions that only the signatory would know;
    - Requiring the signatory to create a secure account that only they have access to in order to complete the electronic forms;
    - Requiring the signatory to submit their social security number in addition to their electronic signature; or
    - Sending a verification email to the signatory regarding the electronic transaction;
- Store electronic records accurately and do so in a way that makes the records accessible to all persons (including regulators) who are entitled by law to access such records.

What is excluded under the UETA?

Notably, electronic signatures are not appropriate in every situation. The UETA focuses solely on electronic contracts related to business, commercial, and governmental matters. The UETA does not apply to transactions governed by the laws relating to the creation and execution of wills, codicils, or testamentary trusts, and certain Articles under the Uniform Commercial Code, the Uniform Computer Information Transactions Act, and any other specific law identified as exempt in a state's adopted version of the UETA. Businesses should always be mindful of jurisdictional differences.

Please contact a member of our data security and privacy team if you have any questions regarding how the UETA will impact your business.

Disclaimer: This article is not legal advice. It is provided solely for informational and educational purposes and does not fully address the complexity of the issues or steps business must take under applicable laws.

Leila Javanshir is a certified information privacy professional (CIPP-US) and a member of the firm's business practice. A significant part of Leila's practice includes providing privacy compliance advice and drafting consumer-facing privacy policies and terms that comply with applicable privacy and data protection frameworks.

Direct: 206.777.7437 | **Email:** leila.javanshir@millernash.com

David Rice provides strategic advice to clients on data privacy and security, data breaches, technology transactions, and cloud services and infrastructure. David was a pioneer in understanding the legal aspects of collecting, managing, storing, and protecting data. He has over twenty years of experience working with clients on data privacy and security matters. David is CIPP-US certified by the International Association of Privacy Professionals.

Direct: 206.777.7424 | **Email:** david.rice@millernash.com