DocuSign®

Whitepaper

Electronic signatures and transactions in the United States

An overview of key legislation and legal factors.

Table of contents

This whitepaper was drafted by the staff of DocuSign, Inc. and most recently updated in August 2019.
It is intended as educational material only and is not a substitute for professional legal advice.

Introduction

Electronic signatures are common in the United States, but confusion still persists regarding the law at a state and federal level. This document provides an overview of:

1. **Legislation enabling electronic signature usage.**
2. **Key legal factors related to electronic transactions.**

What is an electronic contract?

Before addressing the specifics of electronic signature legislation, it may be helpful to first emphasize one point: **under U.S. law, it is absolutely possible to form a contract electronically.** The ESIGN Act and UETA (discussed below) have helped cement this conclusion, but in most scenarios, this would have been true even without this legislation. Electronic contracting is essentially contracting, and contract law fundamentals apply.

Any contract, electronic or not, requires:

- An offer
- Acceptance
- Consideration (some promised exchange of value)
- No defenses (a contract, electronic or not, will not be enforced if a successful defense can be raised; for example, if an element of the contract is unconscionable or violates public policy, or if one of the contracting parties is too young to create a contract)

The most important contribution of ESIGN and UETA is establishing that electronic records satisfy the legal requirement that certain documents be in writing.

Part 1: Legislation

Federal Law: The Electronic Signatures in Global and National Commerce Act (ESIGN)

On October 1, 2000, the ESIGN Act became effective in the United States and is codified at 15 USC § 7001. ESIGN implements a national uniform standard for all electronic transactions and encourages the use of electronic signatures, electronic contracts, and electronic records by providing legal certainty for these instruments when parties comply with its standards. ESIGN preempts any state laws to the extent they aren't consistent with it.

The ESIGN Act establishes that electronic communication and contracts are equivalent to their paper counterparts. At a high level, the key elements are:

- A contract may not be denied legal effect or enforceability solely because of its electronic form.
- If a law requires a record to be in writing, an electronic record satisfies the law.
- If a law requires a signature, an electronic signature satisfies the law.

ESIGN is intentionally neutral regarding the type of technology used, and even goes so far as to specifically preempt any state law that prescribes specific technology.

General rule regarding electronic transactions and records

ESIGN provides as follows:

> "(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."

This establishes a baseline rule that electronic transactions are no less valid than their paper counterparts. Still courts that have examined ESIGN have consistently confirmed its broad effect.[1] Examples of relevant case law are provided in Appendix A to this document.

Electronic signatures

Electronic signature is defined in ESIGN as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

The broad definition of "electronic signature" was intended to allow many types of technology and methods for signing electronically. An electronic signature can be nearly anything produced by electronic means (for example, a symbol, result, or consequence) that has been created in order to demonstrate a party's intent to sign an electronic record.

1 See, for example, Specht v. Netscape Comm'cns Corp., 306 F.3d 17, 26 n.11 (2d Cir. 2002) (assessing whether clicking to download software created enforceable agreement to arbitrate, and noting that the matter of whether "the agreement is a 'written provision' despite being provided to users in a downloadable electronic form... has been settled by [the ESIGN Act]," although ultimately finding that consumers clicking "yes" in the context presented in that case did not manifest assent to license terms).

Examples of electronic signing include:

- Entering a password or personal information number (PIN)[2]
- Typing a name where indicated (or prompted) via computer keyboard[3]
- Responding to telephone keypad instructions (for example, press 3 to agree or 5 to hear this menu again)[4]
- Clicking a button or checkbox[5]
- Responding to an email thread in a manner that manifests assent[6]

It is important to note that while all of these methods (and potentially many others) are equally valid as signatures under ESIGN, they are not necessarily as useful in the context of enforcing an agreement. See the section titled "Common Methods of Electronic Contracting" for a discussion of some of the distinctions between electronic signature methods.

Consumer disclosures

In some transactions between businesses and consumers, the business has a statutory obligation to provide information to the consumer in writing (for example, Truth-in-Lending-Act disclosures). ESIGN permits businesses to make these disclosures electronically, so long as they meet the requirements set out in the Act.

Where a consumer would otherwise be entitled to receive information in writing, electronic information will satisfy the requirement, so long as the consumer:

- Is provided clear and conspicuous notice of the consumer's ability to receive the information on paper.
- Is provided with information about the hardware and software needed to access the information electronically.
- Affirmatively consents to receive the information electronically.

Consumers must provide this consent in a manner that "reasonably demonstrates" that the consumer can access information in the electronic form that will be used to provide the relevant information.[7] A literal reading of ESIGN indicates that the consent itself must reasonably demonstrate the consumer's ability to access the information, but the legislative history indicates that the requirement might also be met by the consumer responding affirmatively to a provider's question about their ability to access, or by showing that the consumer actually accessed the relevant information electronically.[8]

If there is a change to the hardware or software requirements to access the relevant information that creates a material risk whereby a consumer could lose access to the information, the consumer must be notified of the new requirements and of their right to withdraw consent to receive the information electronically. The reasonable demonstration requirement discussed above must also be met with respect to the new system requirements.

Though consumers may withdraw consent to receive information electronically, such withdrawal does not affect the legal effectiveness of any transactions already completed.

Also, while it is advisable to comply with the consumer disclosure requirements set out in ESIGN to the extent they apply, ESIGN states that a failure to meet those requirements will not render any contract invalid or unenforceable solely on that ground.

Electronic records

ESIGN provides that if any other law requires contracts or other records to be retained, that requirement may be met by retaining an electronic record of the applicable contract or record – so long as the electronic record accurately reflects the contract or other record and the record remains accessible to those entitled to access it in a form that can be accurately reproduced for later reference.

If a contract or record is required by law to be in writing (for example, if it is subject to the Statute of Frauds), ESIGN permits it to be completed electronically so long as the electronic record is in a form that can be retained and accurately reproduced by all parties who are entitled to retain the contract or record for future reference.

2 See, for example, the Internal Revenue Service ("IRS") Fact Sheet 2011-07 (http://www.irs.gov/uac/Taxpayers-Who-File- Electronically-Must-Use-e-Signatures), explaining the use of a PIN as e-signature on a tax return.
3 See, for example, Haywood Securities, Inc. v. Ehrlich, 149 P.3d 738 (Ariz. 2007).
4 See, for example, opinion number 04-08-15 of the Office of the General Counsel of New York, issued August 18, 2004, interpreting ESIGN to allow a life insurance agent to have an applicant sign a life insurance application by the entry of their Social Security number into an interactive voice response (IVR) system using a telephone keypad. http://www.dfs.ny.gov/insurance/ ogco2004/rg040815.htm
5 See, for example, United States v. Hair, 178 Fed. Appx 879, 882 n.3 (11th Cir. 2006).
6 See, for example, Int'l Casings Grp., Inc. v. Premium Standard Farms, Inc., 358 F.Supp.2d 863, 873 (W.D.Mo. 2005).
7 15 USC §7001 (c)(1)(C)(ii).
8 146 Cong. Rec. S5282 (daily ed. June 16, 2000) (colloquy between Senators Abraham and McCain).

State Law: Uniform Electronic Transactions Act (UETA)

The Uniform Electronic Transactions Act (UETA) was adopted in 1999 by the National Conference of Commissioners on Uniform State Law.

Forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have adopted UETA.[9] Most of these states have made few, if any, modifications to the model law (the most notable in terms of exceptions being California).

Only three states, New York, Illinois, and Washington, have maintained their own independently developed laws (which pre-date UETA), but all three have amended or interpreted them to be consistent with UETA in their effect. A discussion of each of these "outlier" state laws is set out in Appendix B.

Despite the slight differences among the states, there is enough consistency to permit most businesses to adopt a single process for electronically signing agreements across the country.

Preemption—which law applies?

As noted above, ESIGN preempts state laws (including those representing an adoption of UETA) to whatever extent such laws are inconsistent with ESIGN.

ESIGN also specifically preempts inconsistent state laws that are technology-centric. This eliminated or forced modification of state laws containing specific digital signature requirements which could be met only with the use of PKI-based digital certificates.

Although ESIGN and UETA provisions are similar, there are a handful of differences. Perhaps most notably, ESIGN includes additional requirements for contracting with consumers (discussed above) and is different in scope from UETA. ESIGN applies to "any transaction in or affecting interstate commerce," whereas UETA only encompasses transactions arising out of business, commercial, and governmental matters.

In practice, the requirements of the state and federal laws are so similar that businesses generally need not determine which law applies, because they can easily comply with both.

See Appendix C for an in-depth analysis of how ESIGN and UETA differ.

9 Uniform Law Commission, http://www.uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act

Exceptions to ESIGN and UETA, and the role of other laws

While ESIGN and UETA generally promote electronic contracting, a few categories of documents are excluded from the legislation. **This does not mean these documents may not be completed electronically.** It simply means that they are not covered by ESIGN and/or UETA. As discussed on the next page, many of the documents not covered by ESIGN and UETA may be electronically completed under other legislation specific to those documents.

Exceptions

ESIGN does not apply to contracts governed by:

- Laws overseeing the creation and execution of wills, codicils, or testamentary trust.
- Laws overseeing adoption, divorce, or other matters of family law.
- The Uniform Commercial Code, as in effect in any U.S. state, other than sections 1-107 and 1-206 and Articles 2 (Sale of Goods) and 2A (Leases of Goods)

In addition, ESIGN does not apply to:

- Court orders or notices, nor official court documents (including briefs, pleadings, and other writings), required to be executed in connection with court proceedings (as these types of documents generally are governed by court rules, and **many courts permit electronically signed documents pursuant to their court rules**[10])
- Any notice of:
  - The cancellation or termination of utility services (including water, heat, and power)
  - Default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual.
  - The cancellation or termination of health insurance/benefits or life insurance benefits (excluding annuities)
  - Recall of a product, or material failure of a product, that risks endangering health or safety.
- Any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

Most state electronic signature laws (whether or not modeled on UETA) contain similar exceptions.

Does state law ever apply to electronic transactions?

The ESIGN Act applies to "*any* transaction in or affecting interstate commerce" (emphasis added). This raises the question of what kind of transactions would not fall into its reach. The courts have historically taken a very broad view as to what "affects" interstate commerce, including many transactions where all parties are located in the same state. For example, if a transaction is part of a "class" of transactions that affect interstate commerce, the entire class can be regulated, even if many of the individual transactions occur solely in one state.[11] Even the local real estate market has been found to be within the scope of the federal government's power to regulate commerce.[12]

In theory, it is possible that a transaction could exist that does not affect interstate commerce and thus would not be subject to ESIGN, but for practical purposes, it will likely apply to most contracts entered by companies.

10 See, for example, the "Administrative Procedures for Filing, Signing, and Verifying" provided by the U.S. District Court for the Western District of Virginia at http://www.vawd.uscourts.gov/media/3355/ecfprocedures.pdf, permitting electronic attorney signatures.
11 See Perez v. United States, 402 U.S. 146 (1971) (sustaining the application of a federal "loan-sharking" law to a local culprit because the practice of loan-sharking, in general, impacted interstate commerce).
12 Russell v. United States, 471 U.S. 858, 862 (1985) (holding that an apartment rental "unquestionably" affects interstate commerce, and that "the local rental of an apartment unit is merely an element of a much broader commercial market in real estate").

UCC exclusions and transferable records

One of the more notable exceptions in both ESIGN and UETA are contracts governed by the Uniform Commercial Code (UCC), other than sections 1-107 and 1-206 and Articles 2 (Sale of Goods) and 2A (Leases of Goods). This exclusion reflects the fact that the UCC had already been revised to include provisions for electronic processes for the categories of transactions excluded.

The following table summarizes the Articles of the UCC and how electronic records relate to each:

UCC Code	Electronic Records Use	Example Transaction
Article 1. General Provisions	N/A	General
§ 1-107[13] **(renunciation)**	Covered by ESIGN/UETA	Waiver of rights after a breach of contract
§ 1-206[14] **(statute of frauds for personal property other than "goods")**	Covered by ESIGN/UETA	Sale of personal property other than goods (for example, IP)
Article 2. Sales	Covered by ESIGN/UETA	Sales contract
Article 2A. Leases	Covered by ESIGN/UETA	Lease agreements
Article 3. Negotiable Instruments	Duplicated in ESIGN Title 2, and UETA § 16	Mortgage notes
Article 4. Bank Deposits	N/A	Checks
Article 4A. Funds Transfers	N/A	EFT systems
Article 5. Letters of Credit	Allowed under UCC Art. 5-104	Bank letter of credit
Article 6. Bulk Transfers	N/A	Liquidation notice
Article 7. Warehouse Receipts/Bill of Lading and Other Documents of Title	Allowed under Rev. Art. 7-102[15]	Vehicle title
Article 8. Investment Securities	N/A	Securities
Article 9. Secured Transactions	Allowed under Rev. Art. 9-105	Chattel paper

As noted in the chart above, UCC provisions permit electronic records for certain document types. For example, section 9-105 sets out the rule for electronic chattel paper, including a list of requirements for the electronic system employed to evidence the transfer of interests in the chattel paper. The UCC stipulates that if the system enables such management of the note in electronic format, the electronic record shall have the same rights and defenses as equivalent paper records under the UCC.

13 This section was renumbered as section 1-306 following the 2001 amendments to Article 1 of the UCC. See http://www.uniformlaws.org/shared/docs/ucc1/ucc1_am01.pdf
14 This section was removed from the UCC in the 2001 revision to Article 1, but the provision still exists in many states' adoption of the UCC.
15 See discussion of the revisions to Article 7 dealing with electronic records at http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%207,%20Documents%20of%20Title%20%282003%29. The revisions have been adopted by most states.

Government exclusions

ESIGN generally applies to government actors, but some special provisions apply to them.

ESIGN permits federal and state agencies with rulemaking authority to interpret the Act in connection with statutes they administer. However, any such "regulation, order, or guidance" issued by an agency must be "consistent" with the general principles of ESIGN, may not impose additional requirements, and must be supported by a substantial justification. Agencies are permitted to require retention of paper records only if doing so is essential to attaining a compelling governmental interest relating to law enforcement or national security.

Some agencies have interpreted ESIGN as expressly excluding government filings. For example, the SEC released guidance in 2001 indicating that it did not believe ESIGN applied to SEC filings, but nonetheless authorized the use of electronic records and signatures for most purposes.[16]

In practice, government agencies take a variety of approaches to electronic records, with some agencies accepting nearly everything electronically, and others accepting only selected documents, or establishing regulations that require special treatment of certain documents. For example, the IRS has adopted a framework for the use of electronic signatures by Income Verification Express Services Participants, permitting electronic signatures on forms 4506-T and 4506T-EZ. The framework involves, among other things, taking steps to authenticate the signer, obtain their consent, and obtain third-party verification of the quality of the electronic signature process.[17] The IRS also permits a number of other forms to be submitted with electronic signatures, including individual income tax returns, which may be signed using a PIN.[18]

ESIGN also permits government actors to impose specific technical requirements in order to do business electronically with them as a market participant (for example, government procurement standards). This is discussed further in Part 2 below.

16 Application of the Electronic Signatures in Global and National Commerce Act to Record Retention Requirements Pertaining to Issuers Under the Securities Act of 1933, Securities Exchange Act of 1934 and Regulation S-T, 66 FR 33175 (June 21, 2001).
17 Accessed at https://www.irs.gov/individuals/income-verification-express-services-ives-electronic-signature-requirements.
18 IRS Publication 1345.

Part 2: Electronic contracting in practice

Common methods of electronic contracting

Clickwrap

With "clickwrap" agreements, end users are required to click a button or checkbox indicating their agreement to a set of terms before being able to proceed with an electronic transaction or gaining access to services or products.[19] Courts generally enforce clickwrap agreements even when the user has not read the contract terms, because clicking indicates that the user had actual and constructive knowledge that certain agreement terms apply to the offered products and services.[20]

In determining whether to enforce a clickwrap agreement, a court may scrutinize a website's design, how the button is labeled (for example, "continue" or "next" versus "I Agree"), use of all caps, use of colors or formatting that encourage or dissuade action, font size, important terms being visually obscured by advertisements, or even what the "reasonable Internet user" would conclude were the terms of the agreement.[21] These and other considerations should be taken into account when implementing a clickwrap process, especially as clickwrap is most often employed with contracts of adhesion – "take-it-or-leave-it" contracts which are not negotiable by the customer. Nevertheless, for the right use case, an appropriately configured clickwrap solution can be a highly effective way to achieve a valid, binding, admissible and enforceable agreement.[22]

Browsewrap

"Browsewrap" terms are typically posted on a website and accessible via a hyperlink. These agreements may not involve an electronic signature at all, but instead rely on some action of the user (like continuing to visit the website) to demonstrate "acceptance" of the terms.

While the enforceability of browsewrap is much less certain than clickwrap, it may be considered "accepted" when the end user (1) has actual and constructive notice of the applicable terms; and (2) takes some action to avail herself of the products and services that are subject to those terms.[23] Enforceability will turn on the particular facts, particularly the extent to which the website operator provided notice of the terms.

For example, in *Nguyen v. Barnes & Noble, Inc.*,[24] the court found that the plaintiff had not agreed to the arbitration provision in Barnes & Noble's browse-wrap agreement, because Barnes & Noble "did not position any notice even of the existence of its 'Terms of Use' in a location where website users would necessarily see it, and certainly did not give notice that those Terms of Use applied, except within the Terms of Use" (emphasis in original). Conversely, in *Cairo, Inc. v. Crossmedia Services, Inc.*,[25] the court determined that users had actual and constructive notice because they were presented with text that read: "[b]y continuing past this page and/or using this site, you agree to abide by the [t]erms of [u]se for this site..."

19 Kwan, et. al., v. Clearwire Corporation, No. C09-1392JLR, 2011 U.S. Dist. LEXIS 150145, at *1 (W.D. Wash. Dec. 28, 2011).
20 See, generally, I-Systems, Inc. v. Software, Inc. Quantum Management Systems, LLC, No. 02-1951 (JRT/FLN), 2005 U.S. Dist. LEXIS 47592 (D. Minn. Mar. 7 2005).
21 See Berkson v. GoGo LLC, 97 F.Supp.3d 359 (E.D.N.Y. 2015) (establishing general principles for enforceability of internet agreements: (1) the evidence must show that the user had notice of the agreement, (2) the link to the terms is located where users are likely to see it and (3) a "user is encouraged by the design and content of the website and the agreement's webpage to examine the terms clearly available through hyperlinkage.") In this case, the court required that "the offeror must show that a reasonable person in the position of the consumer would have known what he was assenting to" and accordingly distinguished the noticeably smaller hyperlink for the contract terms from the large, colored "Sign In" button.
22 See The Effectiveness of Clickwrap for Legally Enforceable Agreements, available at https://www.docusign.com/sites/default/files/resource_event_files/Click-Legality-Whitepaper-US-May-2019.pdf.
23 Specht v. Netscape Communications Corp., 306 F.3d 17, 25 (2d Cir. 2002) citing Windsor Mills, 25 Cal App. 3d at 992 (2001) quoting Restatement (Second) of Contracts §19 (1981). See also, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004) (holding that provisions disclosed solely through browse-wrap agreements are typically enforced if the website user had actual and constructive knowledge of the site's terms and conditions, and has manifested assent to them).
24 Nguyen v. Barnes & Noble, Inc., No. 8:12-cv-0812-JST (RNBx), 2012 U.S. Dist. LEXIS 122455 (C.D. Cal. Aug. 28, 2012).
25 Cairo, Inc. v. Crossmedia Services, Inc., No. 04-04825, 2005 U.S. Dist. LEXIS 8450 (N.D. Cal. Apr. 1, 2005).

Signing with an electronic signature system

The method of electronic signature that most closely resembles the familiar paper contracting process is signing with an electronic signature system. Documents are prepared by the sender within the system, then presented to the intended signer. The signer may then review the document and will be prompted to sign in the appropriate location(s). The form of the signature may be a free-form mark made with a stylus or touch screen, or may be a text version of the person's name, in a font selected by them as part of the signing process.

Case law is strongly in support of the validity of this type of process, with a range of reported cases confirming the legally binding effect of electronically signed agreements.[26] Further, the breadth of evidence collected by this process has been shown in a number of cases to be of dispositive legal value even in the face of a party's sworn allegations that they did not sign the agreements in question, leading to summary judgment for the party seeking to enforce the agreement.[27]

26 See, for example, Newton v. American Debt Service, 854 F.Supp.2d 712 (N.D. Cal. Feb 22, 2012) (finding the plaintiff had entered into a binding contract that she had signed using DocuSign, though declining to enforce an underlying provision of the contract on other grounds).
27 See, for example, IO Moonwalkers, Inc. v. Banc of Am. Merch. Servs., LLC, 814 S.E.2d 583 (N.C. Ct. App. 2018) (affirming summary judgment that plaintiff had ratified the agreement in question, relying on DocuSign audit trail as evidence of intent).

Common considerations about electronic contracting

Most of the factors that may arise in enforcing and interpreting electronic agreements are not unique to the electronic sphere. However, they may manifest themselves somewhat differently, or cause more concern than they would otherwise, because lawyers and judges may be less familiar with the technology.

The following sections attempt to shed some light on common considerations raised by attorneys about electronic signature.

Admissibility as evidence

It is important to begin by emphasizing that electronic records are absolutely admissible as evidence. Like any evidence, they must be authenticated, or the parties must agree to their authenticity.

In the federal court system, Federal Rules of Evidence 901 and 902 govern authentication. Courts have permitted electronic data to be admitted under Fed. R. Evid. 901(b)(4), which allows authentication through distinctive characteristics of the document ("Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances"),[28] and Fed. R. Evid. 902(7), which allows business emails to be self-authenticating with information showing the origin of the transmission or other identifying marks (for example, company logos and email addresses).[29]

Confusion sometimes arises in connection with requirements that an "original" document be produced, since the concept of an "original" is not very meaningful in the electronic context. Fortunately, this is addressed in Fed. R. Evid. 1001(d), which provides in pertinent part that "For electronically stored information, 'original' means any printout – or other output readable by sight – if it accurately reflects the information."

Delivery: when an electronic record is "sent" and "received"

ESIGN is largely silent regarding delivery of electronic records; however, UETA provides a set of default rules that can be modified by agreement of the parties.

An electronic record is considered "sent" when the following criteria are met:

- The record is addressed or directed to an information processing system designated or used by the recipient for receiving records of the type transmitted and from which the recipient is able retrieve the record.
- The information is in a form the recipient's system is capable of processing.
- The information enters an information system outside the sender's control or, if the sender and the recipient are using the same system, enters a part of the system under the recipient's control.[30]

An electronic record is considered "received" when the following criteria are met:

- It actually arrives at a system to which the recipient has access for retrieving the record.
- The system has been designated or actually used by the recipient for receipt of the type of record in question.
- The system is capable of processing the record.

It is not necessary for the recipient to actually open or view the electronic record in order for it to be considered received.[31]

UETA also provides that if one of the parties to a transmission is aware that a record was not actually sent or actually received, even though it met the criteria of UETA's default rules, then the effect of the electronic record and its transmission is determined by other law.[32] This provision cannot be modified by agreement of the parties. A few states have expanded on this provision, adding that

28 United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008) (admitting emails based on the email addresses contained in the "to" and "from" fields, and other identifiable material such as the subject matter, signatures, and other personal and professional references).
29 Scheuplein v. City of W. Covina, No. B206203, 2009 Cal. App. Unpub. LEXIS 7805, at *26–27 (Cal. Ct. App. 2d Dist. Sept. 29, 2009) (finding emails to be authenticated when accompanied with a declaration that the emails were retrieved from the company's computers and the printouts were accurate representations of the retrieved messages).
30 UETA §15(a).
31 UETA §15(e).
32 UETA §15(f).

a "bounceback" message will automatically prevent a message from being deemed sent or received.[33]

Most judicial decisions considering delivery of information via email, whether or not they relied on the UETA rules, have determined that if the sender's business records establish that an email was transmitted to the correct email address, a "rebuttable presumption" of delivery arises.[34]

Proving the identity of the signer

As with any contract, an electronic contract will not be enforced if the identity of the party to the contract cannot be established. This can be challenging when parties are contracting remotely, either through electronic means, or by mail.

The identity of the signer is an evidentiary issue, and can be proven in a variety of ways.[35] For example, in *Zulkiewski v. Am. Gen. Life Ins. Co.*, the court found that the insurance company's authentication process, which involved association with an email address, and knowledge of certain personal information (for example, mother's maiden name) were sufficient to establish the identity of the signer.

Electronic security may also play a role in establishing identity. For example, in *Kerr v. Dillard Store Services*, the court declined to enforce an arbitration agreement purportedly signed by the plaintiff, because the defendant "did not have adequate procedures to maintain the security of intranet passwords, to restrict authorized access to the screen which permitted electronic execution of the arbitration agreement, to determine whether electronic signatures were genuine or to determine who opened individual emails."[36]

Similarly, in *Ruiz v. Moss Brothers*, the employer was unable to enforce an arbitration agreement where the court found that they failed to demonstrate how an electronically signed document had been generated, leaving it unclear whether reasonable measures were in place to verify the signer's identity.[37]

It is worth noting that, although there are potential pitfalls with an electronic signature process, it is often still superior to a paper-based system from an evidentiary standpoint. An electronic signature will frequently be associated with an email address, IP, or other elements associated with the signer, where a contract sent by mail will only be associated with a physical location (where others may reside) and a written signature (which may be forged).

Using electronic signatures with government agencies

ESIGN is made applicable to federal and state governments.[38] In practice, however, government agencies often decline to accept electronic records, or impose additional requirements upon them.[39] ESIGN does not grant a right to make electronic filings with the government, and it permits agencies to interpret ESIGN through the issuance of regulations. Some agencies have chosen to impose specific technical requirements, such as the use of public key cryptography, upon the agency's use of electronic signatures.

Over time, government agencies appear to be moving toward greater acceptance of electronic contracting and electronic signatures, though they are generally doing so more slowly than the private sector.

That said, the federal government appears poised to leap forward in its adoption of electronic signatures. On December 20, 2018, the 21st Century Integrated Digital Experience Act ("21st Century IDEA") was signed into federal law. The Act requires all executive agencies to modernize their websites, forms, and processes for improved user experience and compliance with appropriate legal standards. It specifically requires that, "[n]ot later than 180 days after the date of enactment of this Act, the head of each executive agency shall submit to the Director and the appropriate congressional committees a plan to accelerate the use of electronic signatures standards established under the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.)."[40]

The 21st Century IDEA can be seen as a strong endorsement of the value of modern digital services, including electronic signature, for a broad range of government use cases.[41]

33 See, for example, Pa. Stat. Ann., tit. 73 § 2260.115.
34 See, for example, American Boat Co., Inc. v. Unknown Sunken Barge, 418 F.3d 910, 914 (8th Cir. 2005) (holding that the same presumption of delivery applicable to paper communications should apply to email); Kennell v. Gates, 215 F.3d 825, 829 (8th Cir.2000) (absent evidence to the contrary, emails properly dispatched via a generally reliable method are presumed delivered and received).
35 Zulkiewski v. Am. Gen. Life Ins. Co., No. 299025, 2012 Mich. App. LEXIS 1086 (Mich. Ct. App. June 12, 2012).
36 Kerr v Dillard Store Services, Inc., 2009 WL 385863 (D. Kan. Feb. 17, 2009).
37 Ruiz v. Moss Bros. Auto Group, Inc. (2014) 232 Cal. App. 4th 836.
38 15 U.S.C. § 7004.
39 For example, the Food and Drug Administration has released regulations regarding electronic creation, maintenance, and submission of information subject to FDA regulations, which are set out at 21 CFR Part 11.
40 21st Century IDEA Act, Public Law 115-336, Sec. 5, available at https://www.congress.gov/bill/115th-congress/house-bill/5759/text].
41 For more information on the 21st Century IDEA Act, see https://www.docusign.com/21st-century-idea-act].

Appendix A

Notable case law

For a summary of all U.S. case law addressing the use of the DocuSign eSignature service, see the DocuSign white paper "**Court Support for the Use of Electronic Signatures in the United States**."[42]

For a summary of key case law surrounding clickwrap agreements, see the DocuSign white paper "**The Effectiveness of Clickwrap for Legally Enforceable Agreements**."[43]

Below are examples of instructive case law addressing a range of issues related to electronic contracting.

Signed writing requirements

Buckles Management, LLC v. InvestorDigs, LLC
No. 10-cv-00508-LTB-BNB, 728 F.Supp.2d (D. Colo. 2010)

Though email may be sufficient to meet the signed writing requirement under the statute of frauds, in this case it did not qualify as an electronic signature under ESIGN because the sender did not intend to be bound by the terms.

Kaufman v. American Family Mut. Ins. Co.
No. 05–cv–02311–WDM–MEH, 2007 WL 437641 (D. Colo. 2007)

An automated signature on a written letter could meet the statute of fraud requirement, precluding dismissal.

Barwick v. GEICO
2011 Ark. 128 (Ark. 2011)

The plain language of Arkansas UETA authorized the use of electronic records and signatures to satisfy the requirement under Arkansas insurance law that medical benefits coverage could only be rejected by a signed "writing."

Naldi v. Grunberg
80 A.D.3d 1 (N.Y. App. Div. 1st Dep't 2010)

New York Statute of Frauds may be satisfied by an electronic writing and electronic signature because, among other reasons, the Electronic Signatures and Records Act (ESRA) incorporated the substantive provisions of ESIGN, which allow for such electronic records and signatures.

Johnson v. Astrue
No. CIV S-08-0182 GGH 2009 U.S. Dist. LEXIS 130558 (E.D. Cal. June 18, 2009)

Electronic signatures are not "rubber stamp signatures" as prohibited in the Code of Federal Regulations and, as such, electronic signatures meet the requirements for submitting examination reports under CFR for disability insurance claimants.

42 "Court Support for Electronic Signatures in the United States" is available at https://www.docusign.com/white-papers/court-support-for-electronic-signatures-in-the-united-states.
43 White paper is available at https://www.docusign.com/white-papers/the-effectiveness-of-clickwrap-for-legally-enforceable-agreements.

Attribution of electronic signature and proof of consent

Espejo v. Southern California Permanente Medical Group

246 Cal. App. 4th 1047 (2016)

Use of a unique username and password is sufficient to establish the identity of the signer in the context of an employee arbitration agreement.

Labajo vs. Best Buy Stores L.P.

478 F.Supp.2d 523 (2007)

Although a valid electronic signature existed, it was not clear whether the signer had actual knowledge of the contract terms to which the signature purportedly evidenced agreement.

Kerr v. Dillard Store Services

No. 07-2604-KHV, 2009 WL 385863 (D. Kan. Feb. 17, 2009)

Court declined to enforce an arbitration agreement because the defendant "did not have adequate procedures to maintain the security of intranet passwords, to restrict authorized access to the screen which permitted electronic execution..., to determine whether electronic signatures were genuine or to determine who opened individual emails."

Ruiz v. Moss Bros. Auto Group, Inc.

232 Cal. App. 4th 836 (2014)

Court declined to enforce an employee arbitration agreement where the employer failed to demonstrate how the employee was authenticated and how the record was produced and maintained.

Zulkiewski v. Am. Gen. Life Ins. Co.

No. 299025, 2012 Mich. App. LEXIS 1086 (Mich. Ct. App. June 12, 2012)

An insurance company's authentication process, which involved association with an email address and knowledge of certain personal information (for example, mother's maiden name), was sufficient to establish the identity of the signer.

Adams v. Superior Court [Adams v. Quicksilver, Inc.]

No. G042012 2010 Cal. App. Unpub. LEXIS 1236 (Cal. App. 4th Dist. Feb. 22, 2010)

An electronic signature could not be attributed to an employee because the system used did not have sufficient controls (that is, it did not require a password, the record could be modified after the fact, it did not include an audit trail, etc.).

Email as electronic signature

JBB Investment Partners Ltd. v. Fair

232 Cal. App. 4th 974 - Cal: (Court of Appeal, 1st Appellate Dist., 2nd Div. 2014)

Although a typed name in an email may be an electronic signature, it must meet the other elements of an "electronic signature" under UETA; in this case, there was no evidence of intent to sign.

Int'l Casings Grp., Inc. v. Premium Standard Farms Inc.

358 F.Supp.2d 863, 873 (W.D. Mo. 2005)

Email messages including "a header with the name of the sender" were sufficient to satisfy the signature requirement under Missouri's version of the UCC and UETA.

Cunningham v. Zurich Am. Ins. Co.

352 S.W.3d 519, 530 (Tex. App. 2011)

Court declined to hold the mere sending of an email containing a signature block to be an enforceable electronic signature "when no evidence suggests that the information was typed purposefully rather than generated automatically, that [the sender] intended the typing of her name to be her signature, or that the parties had previously agreed that this action would constitute a signature."

Admissibility of electronic evidence

Hook v. Intelius, 10-CV-239(MTT)

2011 U.S. Dist. LEXIS 31879 (M.D. Ga. Mar. 28, 2011)

Screenshots regenerated from archive data (not actual images) were deemed admissible and offered probative value in enforcing an online agreement.

Lorraine v. Markel American Ins. Co.

241 F.R.D. 534, 538 (D. Md. 2007)

Established generally that electronic evidence can be admitted, subject to a showing of reliability.[44]

Delivery of electronic records.

Roling v. E*Trade Sec. LLC

860 F. Supp. 2d 1035, 1043 (N.D. Cal. 2012)

Court found that an email notice sent within a reasonable time before a fee increase was sufficient notice.

In re Leventhal

No. 10 B 12257, 2012 WL 1067568 (Bankr. N.D. Ill. Mar. 22, 2012)

Court extended to email the concept that "a properly addressed item mailed to someone is presumed to have been received."

Abdullah v. Am. Exp. Co.

No. 3:12-CV-1037-J-34MCR, 2012 WL 6867675 (M.D. Fla. Dec. 19, 2012)

Court found, based on presented evidence showing proper delivery of email to the plaintiff, that "a rebuttable presumption was created that Plaintiff received that email."

Ball ex rel. Hedstrom v. Kotter

746 F. Supp. 2d 940, 953 n. 10 (N.D. Ill. 2010)

Court found presumption that, because no evidence was presented to the contrary, the plaintiff had received and had knowledge of information sent to him by the defendant via email.

SEC v. Global Online Direct, Inc.

No. 1:07-cv-0767-WSD, 2007 WL 4258231 (N.D. Ga. Nov. 29, 2007)

Email notices to investors are appropriate if the process creates a reasonable expectation that the investors will (1) receive notice, (2) understand what it relates to, and (3) make a knowing and deliberate decision to read or disregard the communication.

44 For more information on the case, see http://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorraineVMarkel.pdf.

Appendix B

Outlier states: Illinois, New York, and Washington

Illinois, New York, and Washington have not adopted UETA, but have passed their own legislation to support ecommerce. Each state's law is summarized below.

Illinois

The Illinois legislature adopted the Electronic Commerce Security Act[45] (ECSA) in 1998. Although it has not been updated to mirror the language of UETA or ESIGN, it is similar to both in its approach. Most importantly, the ECSA provides that electronic records and signatures shall not be denied legal effect, validity, or enforceability solely on the grounds that they are in electronic form.

ECSA also explicitly provides for the admission of electronic records and signatures as evidence in legal proceedings, prohibiting the denial of admissibility on the sole basis that the record or signature is in electronic form.

The ECSA states that it aims to "facilitate electronic communications by means of reliable electronic records," "facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements," "minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce," and "promote public confidence in the integrity and reliability of electronic records and electronic commerce."[46]

The exceptions to the ECSA are somewhat different than those to ESIGN and UETA. As with the other signature laws, this does not mean that electronic signatures are prohibited, but they must be supported by some other law or common law principle. The exceptions to ECSA are:

(1)When it would be "clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law[.]" (the "manifest intent" referred to in the Act requires more than a mere showing of a requirement of a "signature" or that the document be "signed")

(2)The "creation or execution of a will or trust, living will, or healthcare power of attorney"

(3)"[A]ny record that serves as a unique and transferable instrument of rights and obligations"

The law goes on, however, to state that electronic signature may suffice under the ECSA for a negotiable instrument or other conveyance when an electronic version of the record exists, is "stored and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original"; and "can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy."

Furthermore, ECSA differs from ESIGN and UETA in its narrower definition of electronic signature and its distinct definition of electronic and digital signatures. An electronic signature is defined as "a signature in electronic form attached to or logically associated with an electronic record."

A digital signature is defined as:

[A] type of electronic signature created by transformingan electronic record using a message digest function and encrypting the resulting transformation with asymmetric cryptosystem using the signer's private key such that any person has the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key and whether the initial electronic record has been altered since the transformation was made. A digital signature is a security procedure.

45 5 ILCS 175.
46 5 ILCS 175/1-105.

Although ECSA includes an extensive discussion of digital signatures, they are not required for enforceability or admissibility into evidence. Like many states, Illinois may require digital signatures in some cases when contracting directly with the government or submitting documentation to government agencies.

New York

New York adopted the Electronic Signatures and Records Act (ESRA) in 2000. ESRA is technology neutral, supports use of electronic signature and electronic records for business and personal use, and provides for the admissibility of electronic records into evidence. As described on the website of the New York State Office of Information Technology Services (ITS), "[ESRA] provides that 'signatures' made via electronic means will be legally binding just as hand-written signatures now are.... There is now no doubt that electronic records have the same legal force as those produced in other formats such as paper and microfilm."

Similar to ESIGN, ESRA defines electronic signature as "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with intent to sign the record."

ESRA originally did not apply to electronic transactions involving transfer of title due to death or incompetence, or to the appointment of fiduciaries, but the legislature expanded the scope of ESRA to include such transactions in 2012. As noted on the ITS website sited above: "Effective September 23, 2012, ESRA will allow the use and acceptance of electronic signatures and records with conveyances and other instruments recordable under Article Nine of the Real Property Law, and permit recording officers to electronically accept for recording or filing digitized paper documents or electronic records of real property instruments such as deeds, mortgages and notes, and accompanying documents."

In the case of *Naldi v. Grunberg*,[47] the New York Appellate Division confirmed that the New York Statute of Frauds may be satisfied by an electronic writing and electronic signature because, among other reasons, ESRA has incorporated the substantive provisions of the ESIGN Act.

47 80 A.D.3d 1 (NY App Div 2010).

Washington

From 1997 to mid-2019, electronic signatures in Washington were primarily governed by the Washington Electronic Authentication Act (WEAA). The state repealed WEAA in its entirety effective July 28, 2019, essentially finding the law outdated (in the context of a legal and business climate that has actively embraced e-signature) and confusing (in light of inconsistencies across Washington state law arising from evolving e-signature provisions).

While the repeal of WEAA arguably leaves Washington without a singular overlay statute regarding electronic signatures, it is plainly not intended to negatively impact e-signature acceptance or enforceability in the state. The totality of legislative and judicial activity manifests Washington's recognition of ESIGN and alignment with the federal law's core principles:

- A broad definition of "electronic signature."
- The legal equivalency of electronic and wet signatures.
- Technology neutrality, that is, a lack of any legal preference for any particular e-signature methodology over any other.

Passed well before UETA or ESIGN, WEAA was originally limited in scope, conferring legal enforceability only on "digital signatures" (electronic signatures that use PKI-based digital certificates) and establishing standards for Certificate Authorities (entities that create and maintain digital certificates).[48] The emphasis on digital certificates was intended to encourage the public to become more comfortable with electronic commerce.[49] However, the use of digital certificates failed to emerge as a standard means of transacting business, mostly due to the common consensus that the limited extra assurance provided by digital certificates was not worth the added time, expense, and hassle of requiring signers to procure them.[50]

In 1999 and 2011, amendments to WEAA were passed with the intent of expanding the scope of the law to embrace a broader range of electronic signatures and to relax restrictions on government agencies that previously had limited their acceptance to only digital signatures.[51]

Then, in 2015, came new e-signature legislation, embodied in the Revised Code of Washington (RCW) as 19.360.000 et seq. This new law formally recognized that ESIGN "applies to federal and state transactions, including certain government transactions, in or affecting interstate or foreign commerce relating to [Washington] state."[52] While the law still allows state and local agencies to decide whether to accept electronic signatures for particular government use cases, it nonetheless affirms that electronic signatures carry the same force and effect as wet signatures.[53] Notably, the definition of "electronic signature" in RCW 19.360.030[54] is identical to that in ESIGN, which created a discrepancy in Washington state law between this definition and the legacy definition in WEAA.

The 2019 bill that repealed WEAA, according to state congressional reports, "cleans up confusion in existing law"[55] and recognizes the fact that the "[p]rivate sector has put [WEAA] out of business."[56] The bill also amends several other Washington statutes that previously referenced different sections of WEAA (for example, RCW 43.07.120, RCW 43.07.173, RCW 48.185.005, RCW 58.09.050, RCW 58.09.110).[57] Some of these amendments insert a definition of "electronic signature" into the amended statutes by referring the reader to RCW 19.360.030 (where the ESIGN definition of "electronic signature" was formally adopted).

Though Washington e-signature law has taken an atypical approach, its consistent trend toward recognizing and aligning with ESIGN provides a compelling legal foundation for the continued full recognition of electronic signatures for private intrastate transactions – just as ESIGN ensures the legality of e-signatures for transactions affecting interstate and foreign commerce.

As for state and local government use cases, RCW 19.360.000 et seq. still controls; it declares that wherever the use of a written signature is authorized or required by a state or local agency, an electronic signature may be used with the same force and effect as a wet signature unless specifically provided otherwise by law or agency rule.[58]

48 Stephanie Curry, Washington's Electronic Signature Act: An Anachronism in the New Millennium, 88 Wash. L. Rev. 559 (2013), available at http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1252/88WLR559.pdf?sequence=1
49 Id.
50 Id.
51 Id.
52 RCW 19.360.010, available at https://app.leg.wa.gov/RCW/default.aspx?cite=19.360.010
53 RCW 19.360.020, available at https://app.leg.wa.gov/RCW/default.aspx?cite=19.360.020
54 RCW 19.360.030, available at https://app.leg.wa.gov/RCW/default.aspx?cite=19.360.030
55 H.B. Rep. No. 1908 (2015), available at http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/House/1908%20HBR%20PL%2019.pdf
56 H.B. Rep. No. 5501 (2019), available at http://lawfilesext.leg.wa.gov/biennium/2019- 20/Pdf/Bill%20Reports/Senate/5501%20SBR%20APS%2019.pdf
57 Id.
58 RCW 19.360.020, available at https://app.leg.wa.gov/RCW/default.aspx?cite=19.360.020

Appendix C

Comparison of ESIGN and UETA (as drafted by the Uniform Law Commission)

1 Excluded state laws

ESIGN explicitly excludes more state laws from its reach, but UETA gives the states the flexibility to exclude additional state laws. Compare ESIGN 103 with UETA 3(a)-(c).

2 Government affairs

UETA covers government affairs, rather than just the commercial transactions covered by ESIGN. Compare ESIGN 101(a), 106(13) and UETA 2(16). Its inclusion of government affairs would appear to provide the state's agencies with the enabling legislation that they may need should they choose to conduct their own business electronically. Because many state statutes and regulations implicitly or explicitly require that the government conduct its business in writing, and the enabling legislation for state agencies is silent with respect to electronic activity, UETA provides an essential foundation for the transition to e-government.

3 Consumer protections

UETA does not contain explicit consumer protection provisions as set forth in section 103 of ESIGN, but it leaves in place existing consumer protection laws and makes clear that they will still apply in electronic transactions (UETA 5(b), (e); 8(a), (b), (d)(1)-(2); 15). ESIGN anticipates some of the consumer problems unique to electronic transactions, and deals with them explicitly, while UETA does not.

4 Record retention

UETA enables parties who are required to keep written records to have an agent keep the records for them (UETA 12(c)). ESIGN lacks such a provision.

5 Electronic agents

UETA is clearer and more specific with respect to this topic. Compare ESIGN 101(h) and UETA 14.

6 Insurance

ESIGN provides a liability exemption for agents or brokers; see ESIGN 1010(j). UETA does not.

7 Record retention

ESIGN forbids states to impose written record keeping requirements on persons required to keep records of particular transactions, unless the requirement of a written record serves a compelling government interest related to national security or public safety (ESIGN 101(b)(1); 101(d)(1); 101(d)(3); 101(d)(4); 102(c); 104(c)(1); 104(b)(3)(B)). UETA would permit states to require paper record keeping, but only if they pass a law after UETA is enacted specifically permitting the same (UETA 7(c)(d); 12(f); 12(a)(1)-(2); 12(d)-(e)). Given the preemptive effect of ESIGN, any such after-adopted legislation would probably have to meet ESIGN's test for written record requirements.

8 Additional provisions

ESIGN does not contain provisions addressing the following issues, which are addressed in UETA:

- Temporal application, that is, what transactions the statute will apply to (UETA 4)
- Parties' ability to vary some of the terms of UETA by agreement (UETA 5, 8(d), 10(4), 15(g))
- Attribution of electronic signatures (UETA 9(a)-(b))
- Change or error in electronically conducted transactions (UETA 10)
- Rules governing the time and place of sending and receipt of electronic records (UETA 15)
- Admissibility of electronic records and signatures as evidence (UETA 13)

9 Transferable records

ESIGN limits transferable records to notes secured by real estate, while UETA would apply to a broader range of commercial paper. Compare ESIGN Title II and UETA 16.

10 Federally mandated vs. voluntary state e-procurement

ESIGN appears to require government entities to use or accept electronic records and signatures in the procurement process where they engage in transactions affecting interstate or foreign commerce with private parties who choose to conduct business electronically (except with respect to a contract to which the state is a party). See ESIGN 101(b)(2).

In other words, ESIGN appears to require that state governments accept electronic records and signatures on all documents related to procurement processes except for contracts to which the state is a party (ESIGN 101(b)(2); 102(b); 104(b)(4)). This follows because ESIGN indicates implicitly in section 101(b)(2) that states are required to accept electronic records or signatures except with respect to contracts to which states are parties. Furthermore, ESIGN explicitly exempts state procurement from only one of the two requirements that it imposes on states that have not adopted UETA and want to specify alternative means of conducting electronic transactions (see ESIGN 102(b)) and only one of the three requirements imposed on states exercising their interpretive authority by interpreting their laws and regulations in light of ESIGN. See ESIGN 104(b)(4). Both of these explicit exemptions for state procurement extend only to ESIGN's requirement that states adhere to technological neutrality. Thus, provisions of state procurement laws mandating the use of written documents "relating to" procurement transactions are preempted to the same extent as other laws and regulations requiring written documents, except to the extent that they apply to contracts entered by a state and/or specify the technology to be used in the conduct of the procurement process.

By comparison, UETA gives states the option to use and accept electronic records in such circumstances (UETA 5(a)(c), 18). Therefore, UETA provides states with far more flexibility in determining the degree to which they want to conduct business transactions electronically, and the time frame during which they will migrate to electronic commerce.

11 Enabling e-government

In addition, optional provisions of UETA, which do not appear in ESIGN, pertain specifically to states' creation and retention of their own electronic records, conversion of their written records to electronic records, acceptance and distribution of electronic records, and the interoperability of systems adopted by state governments to facilitate e-government (UETA 17-19). While section 17 of UETA does not appear to be appropriate because it could result in multiple interpretations of records retention laws by different agencies, sections 18 and 19 may provide needed guidance to state agencies faced with questions about their authority to conduct their own business electronically after UETA.

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

docusign.com

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