# Guide to Validity of Electronic Signatures & Electronic Signature Laws


REVV

# OVERVIEW

Businesses are making exits from the house of wet signatures and joining the bandwagon of electronics signatures.

According to a report by P&S Intelligence, the global electronic signature market was valued at $1,198.6 million in 2020, and it is expected to grow at a CAGR of 26.6% during the forecast period (2021–2030).
Among other key reasons like time savings, cost savings, and convenience, the cause of this massive drift is to protect the authenticity and integrity of signatures.

Wet signatures are not foolproof and can be forged easily. When the forgery is carried out with a dash of motor skills, even the handwriting professionals can be tricked into believing that the signatures are real.

> *81% of business users consider e-signatures as the most essential in the legal and security aspects of their daily operations. These businesses and sectors include those from banking and finance, pharmaceuticals, healthcare, and government.*
> *Source - Cygnature, 2019*

Electronic signature technology addresses the overall inefficiencies of handwritten signatures and provides compliance and security to the transactions.

But, the application of eSignature technology goes hand-in-hand with eSignature laws.

Therefore, before initiating any transaction with e-signatures, businesses should be cognizant of the in-country and international (if the transaction involves other countries) eSignature laws.

Executing contracts and agreements as per the laws ensure that the virtual actions, approvals, and signatures businesses are offering are valid and enforceable.

This guide will help you gain an in-depth understanding of what makes electronic signatures legally enforceable, how long they are enforceable, where they're accepted, when they are not accepted, how they remain compliant, and much more.

## ARE ELECTRONIC SIGNATURES LEGALLY BINDING?

You open a document, click a box, select a font, and suddenly you've 'signed' an agreement. Bob Dylan was right: the times, they are a-changin'.

Whether you're on the sending or receiving end of an agreement that requires an electronic signature, you really want peace of mind in knowing that -

- The authorized person will actually be electronically signing the document.
- The signature will be accepted as binding and enforceable.
- Both parties will be protected and indemnified against the use of the electronic signature.

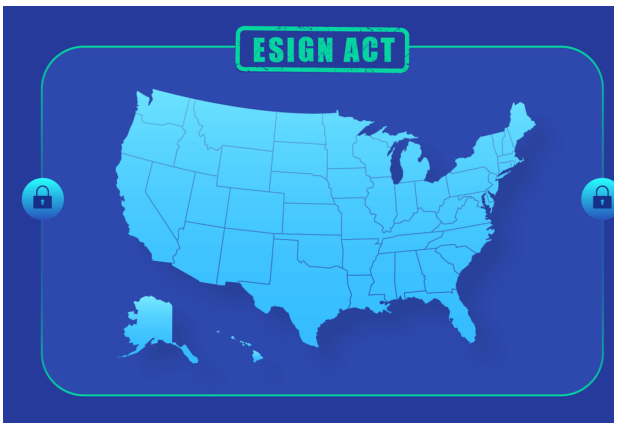
The good news is, you can relax. While e-signatures may seem new to you, or maybe just a lot more popular this year, they've actually been in use since the early 2000s to seal legal agreements like business contracts, employment agreements, non-disclosure agreements, mortgage contracts, and more.

## ELECTRONIC SIGNATURE LAWS IN THE U.S. | ESIGN ACT & UETA

The Electronic Signatures in Global and National Commerce Act (ESIGN) and Uniform Electronic Transactions Act (UETA) have given e-signatures the equivalent weightage as handwritten signatures at the state level (UETA) and federal level (ESIGN ACT) in the United States.

Let's take a deep dive and understand each Act -

### ESIGN ACT | Federal law




President Bill Clinton signed the Electronic Signatures in Global and National Commerce Act into federal law on June 30, 2000, in an effort to bolster electronic commerce and garner trust in the validity and safety of electronic business transactions.

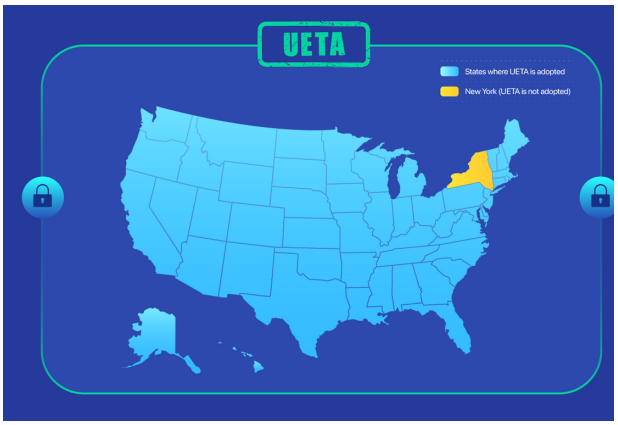
Electronic signatures have been in use since that time and have increased in popularity as more and more businesses move to more online-based models.

The ESIGN Act defines an electronic signature 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.”

- It establishes that any law that demands a signature may be fulfilled with an e-signature.
- Permits electronically carried out agreements to be presented as proof in court.
- Provides that an electronically signed document may not be denied legal effect, validity, or enforceability solely because it is in electronic form.

## Uniform Electronic Transactions Act (UETA) | State law

The Uniform Electronic Transactions Act was drafted by Uniform Law Commissioners on Uniform State Laws in 1999 prior to the enactment of the ESIGN Act.




While the Electronic Signatures in Global and National Commerce Act is for electronic signatures and records at a federal level, the UETA is established to provide a legal framework to operate government and commercial transactions on a state basis.

Till now, 49 states have adopted UETA, including the District of Columbia, Puerto Rico, and the US Virgin Islands.

Here are some key guidelines listed in the Uniform Electronic Transactions Act -

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

- 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.
- In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.
- An electronic record or electronic signature is attributable to a person if it was the act of the 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 person was attributable.

## WHAT MAKES ELECTRONIC SIGNATURES LEGALLY BINDING?

The Electronic Signatures in Global and National Commerce Act makes provisions for what constitutes a valid eSignature. These provisions deal more with consumer consent and disclosure rather than the design or safety of the electronic signature itself.

Here are the requirements for obtaining a valid electronic signature -

### 1. Intent to sign

Like wet signatures, e-signatures will only be considered valid when a signer displays conscious intent to sign an agreement electronically.

### 2. Consent

If you're requesting an eSignature from a client, the ESIGN Act states you must first obtain the client's prior consent. The consent must inform the client of the following:

- They'll be signing electronically, not with pen and paper.
- Their consent covers a particular agreement, what the agreement is, and if any other documents, agreements, or transactions will be covered with this consent.
- Consent may be withdrawn. An explanation of how to withdraw consent must be included, and any expiration that may occur which would not allow for the consent to be withdrawn.

- How can they obtain a paper copy of what they're signing, and any fee associated with the cost of obtaining a paper copy?.

## 3. Hardware and software requirements for access to and retention of the electronic records

Before obtaining a client's consent, a person or company requesting an eSignature must make the client aware of the hardware and software requirements for obtaining the eSignature. This is to ensure that the client will have access to a computer and the software needed to effectuate the eSignature. The client must ensure they're able to access these items prior to giving their consent.

If at any time prior to signing the hardware and/or software requirements change, the client must be made aware in writing.

## 4. Association of signature with the record

Wet signatures, when done, get soaked by the paper, therefore, making it associated with the document.

But, how can one validate the same association when signing a contract electronically? In order to be certified as valid, the system used to sign documents must record the process of signature creation and each step taken by the signer to execute the transaction. The system can also produce a textual or graphical statement to certify the accomplishment of the transaction via eSignature.

An eSignature service provider must be able to accomplish this task as per the outlined standards. Also, the user should ensure that the 'association of signature' accomplished isn't proprietary to the eSignature vendor, which means -

- Should a situation arise, the user doesn't need any validation from the eSignature vendor to prove the association

- Association can be guarded even if the eSignature vendor is no longer providing their service or in case it no longer exists

## 5. Record retention

This is the last requirement for the enforceability of electronic signatures, which states that you should have the

right procedures and systems to reproduce the electronic signature records.

Records of electronic signatures and documents must be kept in accordance with appropriate law, and the company or person requesting the eSignature must be responsible for keeping these records.

This is achieved by providing a completely fulfilled agreement copy to the signer or by giving them permission to download a copy of the agreement.

## HOW LONG ARE ELECTRONIC SIGNATURES VALID?

Electronic signatures are valid as long as the agreement remains valid. In other words, the terms of the agreement will govern the terms of the signature. When the agreement expires, the electronic signature will expire.

## WHEN ARE ELECTRONIC SIGNATURES NOT VALID?

Electronic signatures are a convenient and time-saving way to conduct business, but there are some instances when only a pen and ink signature will be valid.

The following documents are not covered as valid by the ESIGN Act.

- Powers of attorney
- Wills, testamentary trusts, and codicils
- Adoption paperwork
- Divorce decrees
- Certain documents associated with Uniform Commercial Code (UCC)
- Court documents *a caveat here: many state and local courts have adopted eSign procedures that allow for electronic signatures, but the E-SIGN Act does not cover them. For example, court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings
- Notices of default, eviction, or foreclosure
- Cancellation of insurance benefits
- Product recalls or notice of material failures
- Documentation accompanying the transport of hazardous materials

*Revv Tip*

***The above points give you a comprehensive list of documents that can't be executed with e-Signatures. But, in addition to compliance with the ESIGN Act, each state in the U.S. runs individual laws regarding the use of electronic signatures. Therefore, it is recommended to determine if your state and/or local government has additional provisions regarding certain electronically signed documents.***

## RISKS INVOLVED WITH ELECTRONIC SIGNATURES AND WAYS TO MANAGE THEM

While technical advancement and legal measures have facilitated the use of electronic signatures, there also come associated risks that can lead to non-compliance, signature forgery, unauthorized signing, etc.

Suppose a contract you generated with other parties landed in court. After thorough investigation and analysis, the court concluded your contract as void.

Reason?

The electronic signatures weren't created under the right circumstances and are non-compliant with the eSignature laws.

What went wrong? Possibly -

- The eSignature technology of the chosen vendor did not comply with the laws and did not follow the basic rules of processing an electronic transaction.

- The electronic document wasn't at par with the legal needs of the content, presentation, sequence, and information to be acquired for each such document.

This section lists down all such risks and challenges, the right ways to mitigate them, and reinforces the legitimacy of electronic transactions.

**Risks involved with electronic signatures -**

### Parties identification risk

Initiating a deal over the internet is much simpler and faster. But, in this world of sight-unseen transactions, how do you ascertain the identity of the parties and ensure that the signature belongs to the right person.

Solution -

You can mitigate this risk by probing the eSignature service on the below points and ensuring they facilitate all of them -

- The e-signature service should provide an appropriate attribution method.
- It should demand signers to authenticate themselves before accessing a document and affixing an electronic signature to a document.
- It should provide robust authentication methods to confirm the signer, which could be one or a combination of below -

**Email authentication** - The signer is invited to eSign a document by clicking on the link sent in the email. Here authentication takes place when the signer logins to the account and clicks on the link.

**SMS authentication** - This method validates a signer's identity by sending a one-time password (OTP) or PIN to their mobile number. It requires the signer to enter the OTP/PIN in order to access and eSign the document.

**Knowledge-based authentication (KBA)** - The signer is asked to answer personal questions to access the document, such as mother's maiden name, grandfather name, favorite food, favorite teacher, etc.

There are two types of knowledge-based authentication methods - static KBA and dynamic KBA.

In static KBA, the signer opts for certain security questions and feeds their answers while setting up the account.

In dynamic KBA, a signer is asked to answer the questions in real-time. These questions are derived from the user experience, which makes it easier to answer for the signer but extremely difficult for an impostor to crack, thus ensuring maximum security.

**Verification through IDs** - Signers are asked to confirm their identity via government-issued photo IDs by matching the details on the agreement with the details on the ID.

## Risk of Tampering of electronic records

In this, a signer admits to signing the document themself but claims that the

document associated with the e-signature has been altered. Many possible scenarios can lead to such a situation like -

- The signer has provided the wrong information in the agreement.
- The signer had a change of mind about the agreement, and he/she wants to make it invalid by denying their signature.
- The electronic records or signatures have been tampered.

**Solution** -

Whatever is the scenario, the crux of the matter is how to find who is at fault. E-signature technology makes this task a breezy affair. It provides credible and compelling electronic evidence, which makes the document enforceable in court.

The procedure selected by a sender for a signer should get archived in a completion certificate consisting of an audit trail. The audit trail records and recreates the entire electronic transaction from start to finish and registers the key information, including -

- Documents presented
- Signer details - name, email id, role, and a unique id
- Date and time stamp of each activity
- Actions taken by the signer - login, open, review, acceptance, and signatures
- Geolocation where the eSignature took place (only if the signer agreed to record their location)
- IP address
- Type of authentication process used

Once documented, the audit trail turns into an unalterable record. When a person refuses to accept that they have signed a particular document, the audit trail acts as adequate proof that validates whether there was any fraudulent move or forgery in the process.

Some electronic signature solutions also encrypt each agreement post its execution by the signer, making every alteration 100% detectable.

## Risks of losing electronic data

While eSigning accelerates document closures multifold compared to paper documents, the cloud-storage of electronic documents can concern many users regarding the security of their documents.

What if someone hacks my document and -

- Leaks all the confidential information
- Steals my identity and misuse my electronic signatures
- Makes changes to it

Does the eSignature vendor ensure the safety of the systems where my electronic records are placed?

**Solution -**

Always remember that all eSignature vendors don't provide the same level of physical and cloud security to your documents.

Scrutinize the protection features of each e-signature service provider and check if they are at par with your business's security demands.

Ensure that the eSignature service provider -

- Runs robust data encryption in transit and data at rest
- Provides 99.999% reliable storage and access
- Provides data access and transfer via HTTPS
- Stores records within an encrypted directory to meet your regulatory and compliance needs
- Partners with reliable cloud infrastructure service providers like Amazon Web Services (AWS) and Microsoft Azure
- Such service providers comply with the industry and IT regulations, applicable laws, security practices, data protection, and certifications like ISO 27001, SOC 1/2/3, HIPAA, PCI DSS, CSA, STAR, 21 CFR Part 11, and more
- Provides audit trails and multiple authentication methods (which covers fraud and identification risk as explained above)
- Provides malware protection

## Availability issues of electronic records

Record-keeping of your electronic records is crucial. You might need it for internal purposes in the future or to prove the

transaction should a dispute arise.

Solution -

Your eSignature vendor should give you the access to download and store all the document-related records and the access to retrieve them later if required.

Note - Do check the data retention policy of your eSign service provider.

## Summing up - Compliance is the key to avert risks

Ensure the chosen eSignature vendor -

- Complies with the local e-signature standards and laws like ESIGN and UETA in the USA
- Processes document presentation and signatures as per the governing law guidelines throughout a transaction
- Executes the right presentation, format, and sequence of all the documents and associated disclosures and information

# VALIDITY OF ELECTRONIC SIGNATURES IN CROSS-BORDER BUSINESS

eSignatures are a big boon to commence business between parties. And they are even more advantageous in terms of travel time and money, especially when the parties belong to different countries.

But, before initiating signatures via electronic means, businesses should have clarity on different regulatory approaches to electronic signatures across the world.

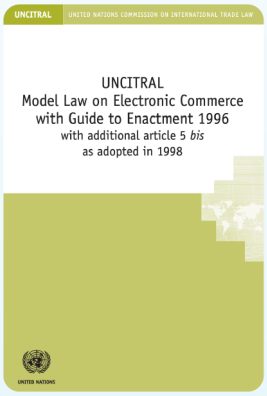
## International law

### UNCITRAL Model Law on Electronic Signatures (MLES)

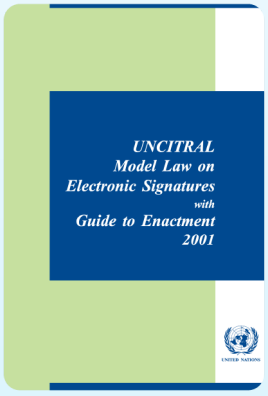
The UNCITRAL is a subsidiary body of the United Nations General Assembly.

It is responsible for refining the legal framework to ease international trade and investment.

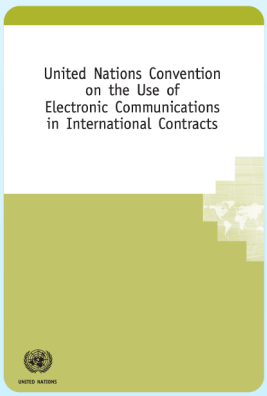
**Three important international regulations related to electronic signatures**




**UNCITRAL Model Law on Electronic Commerce**




**UNCITRAL Model Law on Electronic Signatures**




**United Nations Convention on the Use of Electronic Communications in International Contracts**

Adopted in 2001, the Model Law of Electronic Signatures is based on the signature provision provided in Article 7 of the UNCITRAL Model Law on Electronic Commerce (MLEC).

MLEC is intended to facilitate commerce via the use of modern means of communications and storage of information. The purpose of the MLES is to enable, promote, and bring legal surety to the application of electronic signatures. It establishes criteria of technical reliability for the equivalence between electronic and handwritten signatures.

It follows a technology-neutral approach, which avoids favoring the use of any specific technology or process. This means in practice that legislation based on this Model Law may recognize both digital signatures based on cryptography (such as public key infrastructure - PKI) and electronic signatures using other technologies.

MLES is enacted by more than 30 nations.

**Types of legal frameworks for eSignatures**

Generally, the legal frameworks exercised in countries are categorized under three regulatory models -

**Minimalist or Permissive approach**

In this approach, the parties welcome all types of electronic signatures and give them equal weightage as handwritten signatures.

Since it gives freedom to opt for any eSignature technology, this approach saves money and provides flexibility and convenience of eSigning documents. Countries where Minimalist laws are implemented include the United States, Canada, New Zealand, and Australia.

**Prescriptive approach**

Adopted by a few countries, the prescriptive eSignature law is the strictest among all three. It considers only those electronic documents as legally binding that are signed using a particular technology and have followed a specific process to achieve the same.

These rules mandate the adoption of the chosen encryption method, which works in favor of strengthening security.

On the flip side, it can turn expensive to the parties as they are bound to pay a fee for each of such e-transaction processed through a specific eSignature service provider or certificate authority.

**Two-tiered approach**

This approach is a hybrid model, which is a mix of both minimalist and prescriptive laws.

Similar to the minimalist approach, the two-tiered model also accepts all kinds of electronic signatures. But, like the prescriptive approach, it also dictates and regulates the use of digital signatures to process specific forms of documents.

This model is executed in many European nations as well as in South Korea, China, and Japan.

Generally, the countries with two-tiered models devise their laws on the UNCITRAL Model Law on Electronic Signatures.

**Now, let's discuss how to ensure the enforceability of eSignatures in transnational business.**

Global commerce means global transactions and operating under different state laws. The varying domestic rules on electronic signatures question their validity and make cross-border business transactions complicated. This raises some fundamental questions -

- Whether or not we should seal the cross-border business deal with eSignature technology?
- Does my contract type qualify for electronic signatures or demand wet signatures to be signed in physical presence?
- Does the jurisdiction of the contract accept electronic signatures?
- Does my contract mandate to use a specific form of an e-signature to make it legally valid?
- Does my contract allow implementation and variation by electronic means?
- Are there any registry needs?
- How to overcome the disparities in the legal framework of e-signature laws and ease international trade?

For instance, are electronic signatures valid in Canada? Yes, they are valid in Canada, but the provisions for their legality are slightly different.

This means if you're preparing an agreement to be signed by a corporation or individual in Canada, you will need to comply not only with the U.S. ESign Act requirements but also with the Canadian Personal Information Protection and Electronic Documents Act.

Likewise, if you're conducting electronic business in any of the over sixty countries which accept electronic signatures, you will need to comply with their laws as well as the laws of the U.S. to ensure the validity of your e-signature.



## ELECTRONIC SIGNATURE LAWS AROUND THE WORLD

The use of electronic signatures is permitted in over 60 countries in the world. Like ESIGN Act and UETA govern electronic signatures in the United States, here is a brief overview of eSignature legislation in other parts of the world.

### European Union

**Electronic signature laws -** electronic Identification, Authentication, and Trust Services (eIDAS)

Brief -
Enacted in 2016, the Electronic Identification and Authentication Services (eIDAS) Regulation govern electronic signatures across the 27 countries that belong to European Union (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom).

The eIDAS regulation across Europe saves time, money, and resources spent on the validity of transnational agreements.

It falls under a tiered jurisdiction. But, unlike other countries that follow a tiered or hybrid model, the eIDAS regulation allows the application of three types of electronic signatures - simple e-signature, advanced e-signature, and qualified e-signature.

## Canada

**Electronic signature laws -**
Personal Information Protection and Electronic Documents Act (PIPEDA)

Brief -
The PIPEDA Act came into existence in the year 2000 and provides that electronic signatures carry the same weight and same legal status as handwritten signatures.

The prime intention behind this Act was to promote electronic commerce by establishing trust with regard to the privacy and security of consumer data.

It follows the minimalist model of electronic signatures which means no special status is given to any particular technology to enforce the legality of an electronic signature.

However, the Act requires to obtain the consent of all the concerned parties involved to conduct business electronically.

## Australia

**Electronic signature laws -**
Electronic Transactions Act 1999

Brief -
The Electronic Transactions Act ensures that a transaction can't be deemed invalid simply because it was executed electronically. Australian eSignature laws

subscribe to the minimalist model, which means all types of electronic signatures are admissible in court.

## India

Electronic signature laws -
Information Technology Act 2000

Brief -
Also known as the IT Act, the Information Technology Act was passed in 2000 making electronic signatures legal and enforceable. It comes within the scope of the tiered eSignature model and accepts various forms of electronic signatures but gives greater evidentiary weight to digital signatures.

## Know more about electronic signature laws across the globe

Here is a table that covers most of the countries that have enacted e-Signatures laws. Click on the links to know more about each country's e-signature usage guidelines.

- Argentina
- Australia
- Austria
- Belgium
- Bermuda
- Brazil
- Canada
- Chile
- China
- Colombia
- Czech Republic
- Denmark
- Ecuador
- Egypt
- Finland
- France
- Germany
- Greece
- Guatemala
- Hong Kong
- Hungary
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Luxembourg
- Mexico
- Netherlands

- New Zealand
- Norway
- Peru
- Philippines
- Poland
- Portugal
- Romania
- Russia
- Saudi Arabia
- South Africa
- South Korea
- Spain
- Sweden
- Switzerland
- Taiwan
- Thailand
- Turkey
- United Arab Emirates
- United Kingdom
- United States
- Ukraine
- Uruguay
- Vietnam

## HOW DOES REVV MAKE ELECTRONIC SIGNATURES LEGALLY VALID?

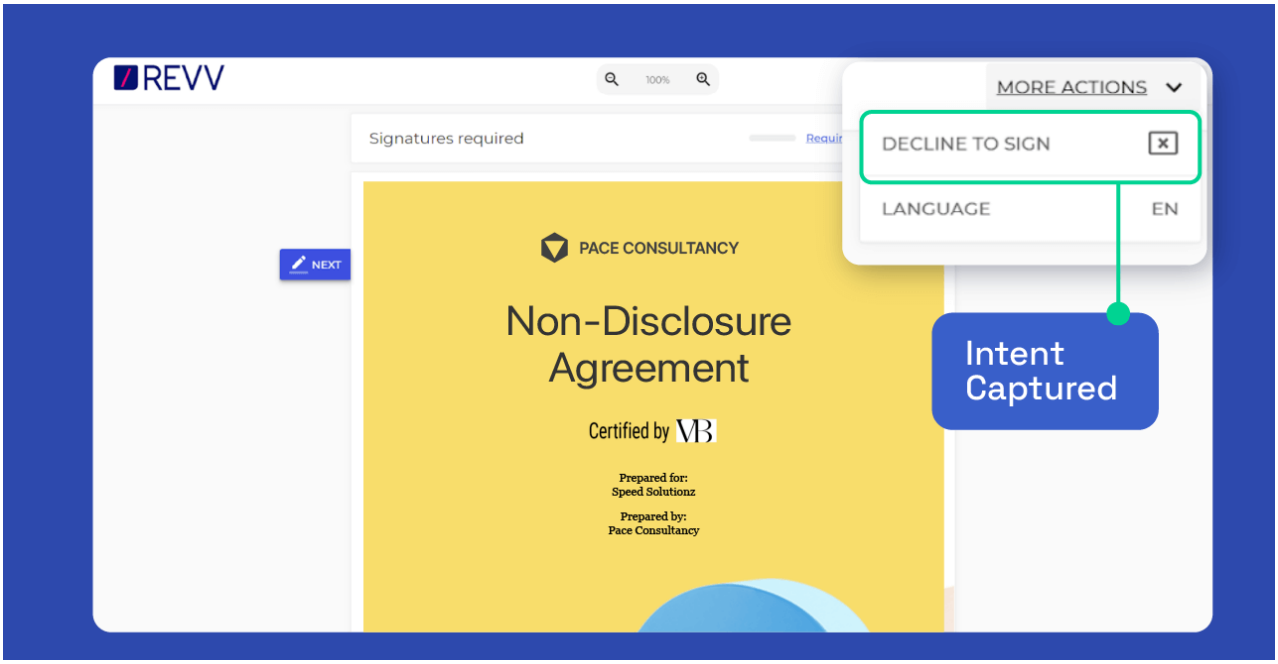
As stated above, electronic signatures should comply with the following requirements under ESIGN Act and UETA in order to be legally valid under U.S. law.

- Intent to sign
- Consent to do business electronically
- Association of signature with the record
- Record retention

Revv ensures compliance with all these four rules throughout the e-signature process.

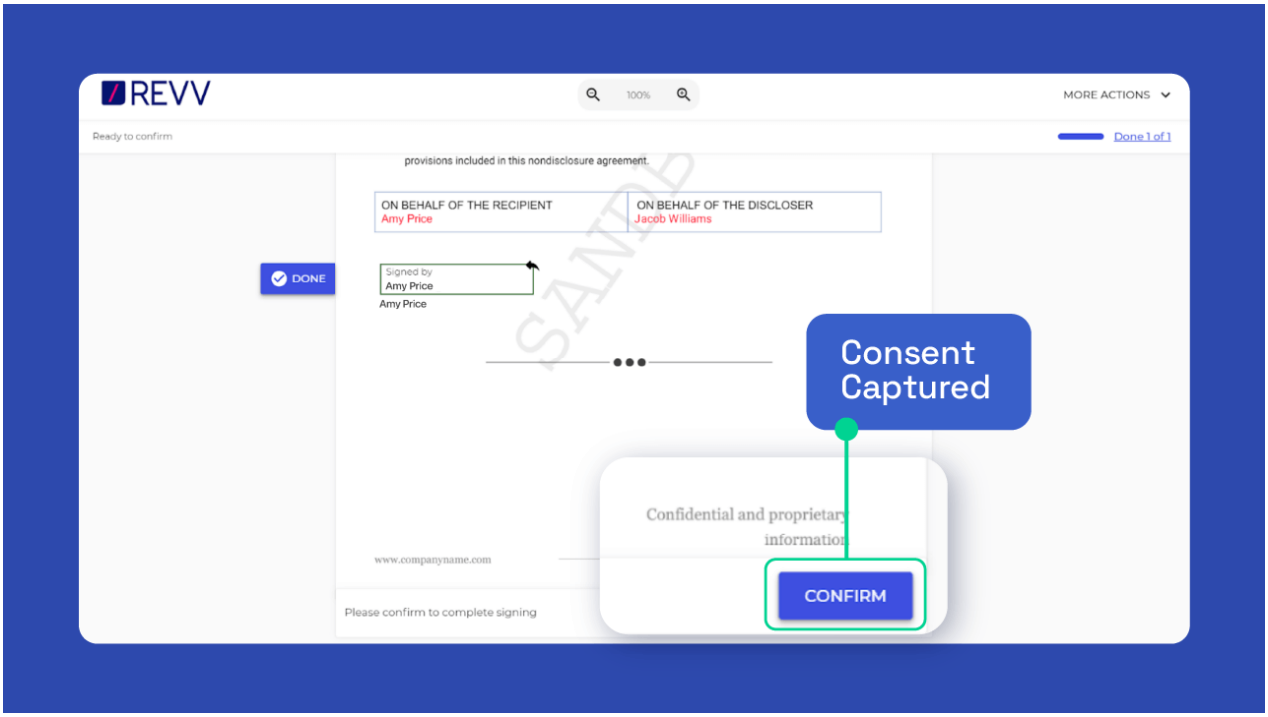
### Intent to Sign - How Revv complies?

Revv captures intent by giving an option to the signers to decline the signature request and empowers them to decide whether they want to affix their e-signatures in the document.



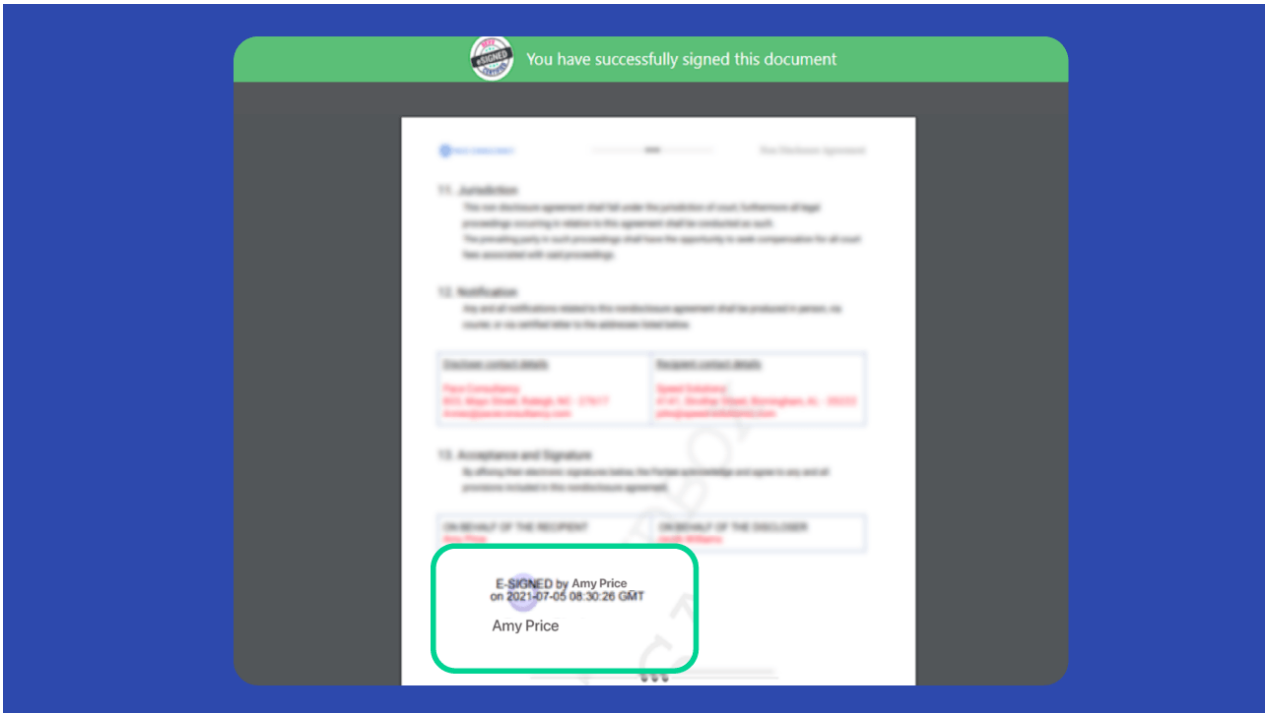

## Consent to do business electronically - How Revv complies?

After a signer registers the eSignature in the signature placeholder, Revv asks them to clearly express their consent by confirming it.



## Association of signature with the record - How Revv complies?

Once signed, Revv makes those eSignature as a part of the document along with the date and time of when it was done.

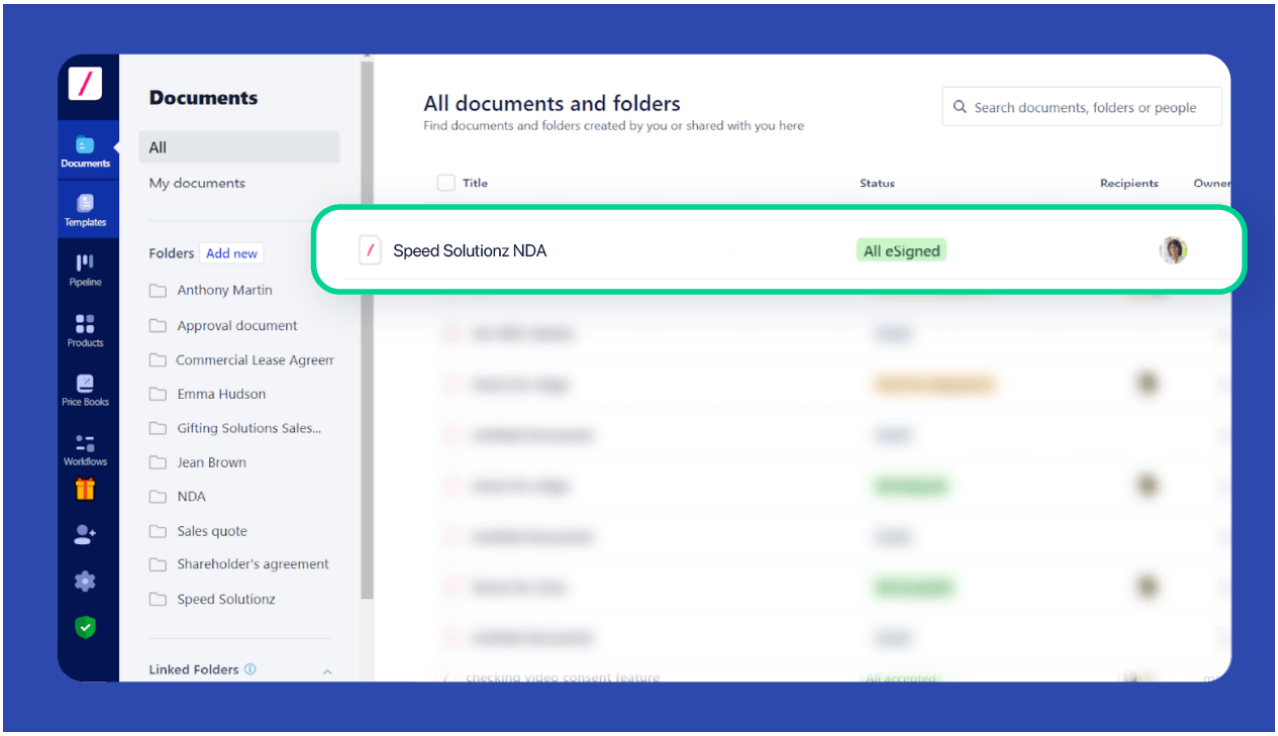



Revv also generates an audit trail, which includes - signer's information, date and time stamp of each action taken by the signer, IP address, and other details that act as legal proof.

Here's a video that shows how Revv authenticates and validates electronic signatures by providing an evidence summary with full audit trail.

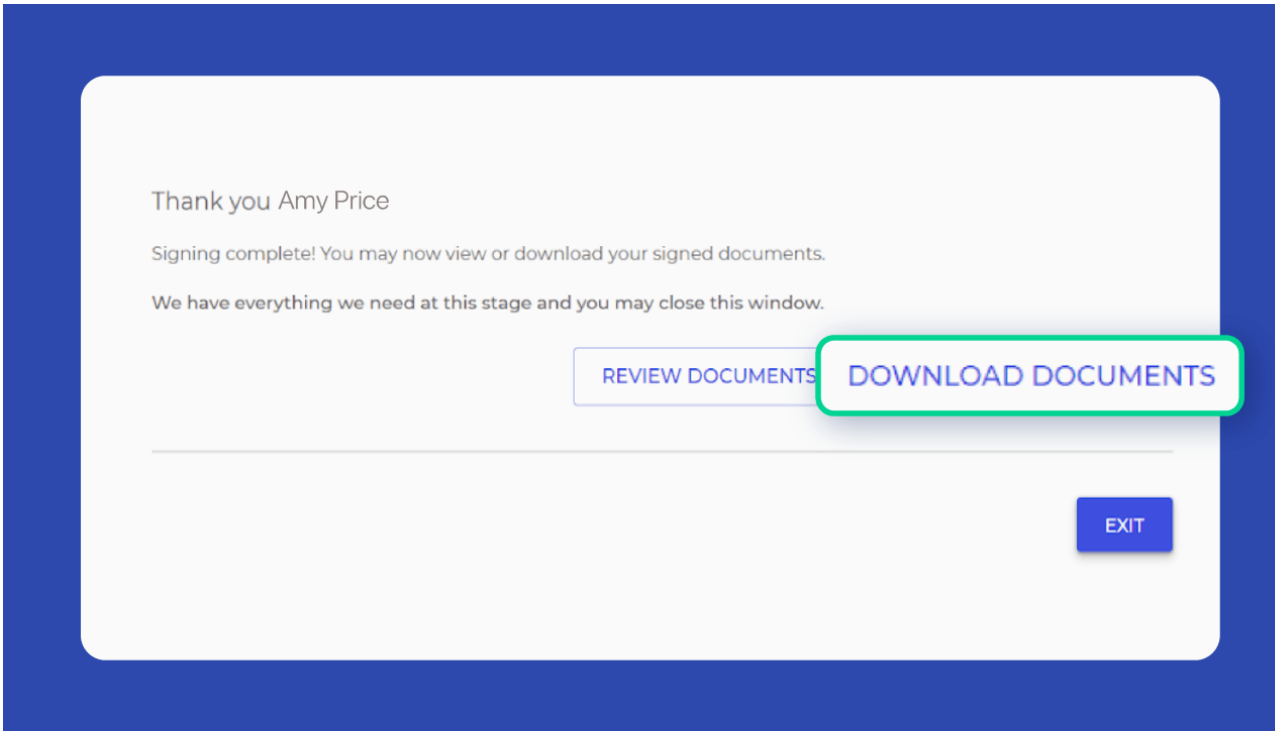
## Record retention - How Revv complies?

Revv provides a secure and forever cloud storage of all electronically signed documents using AWS SSE-S3 (Amazon Web Services Server-Side Encryption).

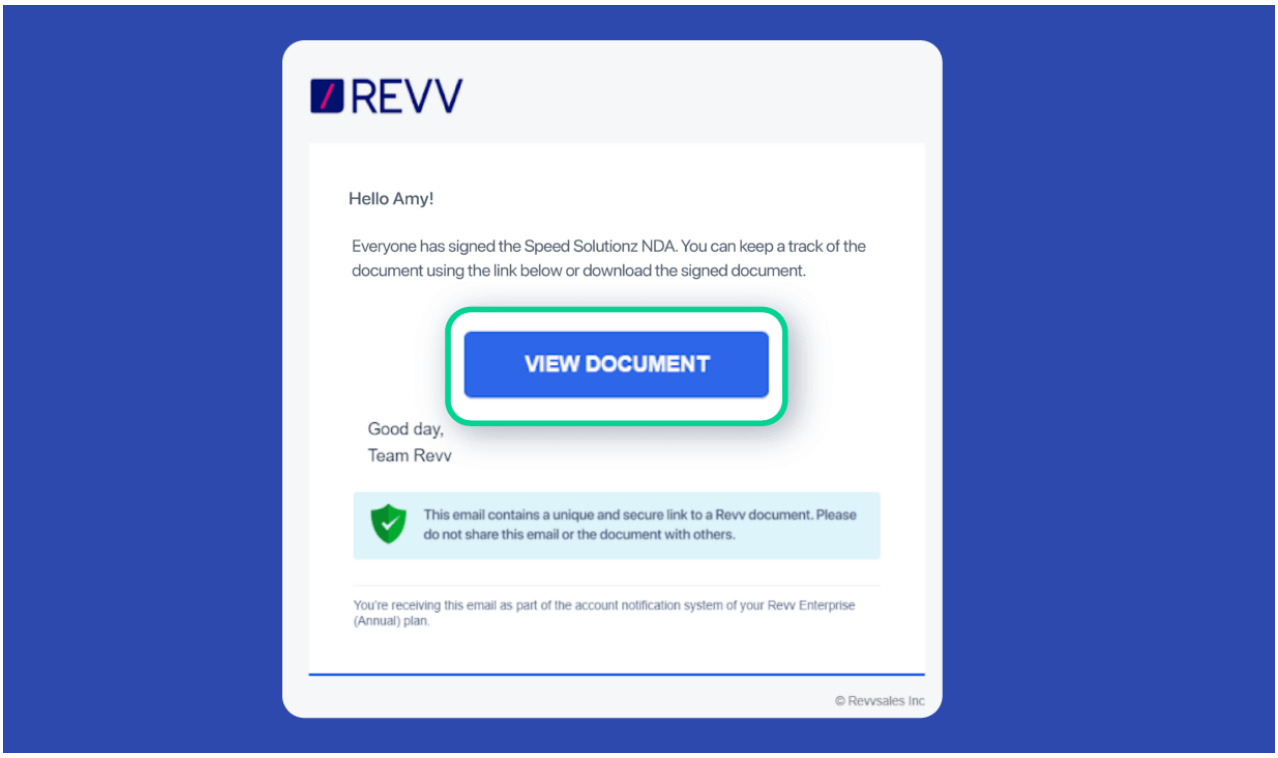



For signers -

Once signed, Revv offers the signers to download a copy of the signed document.



Alternatively, Revv also sends a link to the signed document to the signer's email box.




## ARE ELECTRONIC SIGNATURES I CREATE WITH REVV SAFE?

Want to begin using electronic signatures but not sure where to start? We can help. Using Revv to create your electronically signed documents is easy, and you can trust our team to ensure your electronic signature transactions are not only safe—they're effective.

Revv, an electronic signature platform, comes with document automation features that offer perfect solutions for businesses of varying sizes.

Creating electronic signatures with Revv is easy. You can choose from two forms of document approval:

**Soft sign** - Send a document that does not need an electronic signature with an option to 'accept or reject.' This is essentially the equivalent of clicking "I agree" when you accept cookies or install an app and agree to the terms of service. There is also legal precedence for soft signatures being legally binding in the U.S. and Europe. Revv offers video

authentication for soft signatures.

**Bank-grade electronic signature** - For documents that need an electronic signature, Revv offers secure, bank-grade electronic signature technology that is safe, fast, and easy to use. It facilitates three types of electronic signatures - click-to-sign, draw a signature, or click-to-initial.

Revv complies with industry standards and local and global eSignature regulations - ESIGN Act, UETA, eIDAS, and more to give you the ease to do business anywhere.

Revv secures each transaction by protecting it with multiple layers of encryption and AWS global cloud certification - CSA, SOC 1, SOC 2, and ISO 27001.

For an added layer of security, you can enable more layers of recipient verification by using SMS-OTP-based authentication. And it's not only the documents that you create via Revv that are safe: the emails sent for e-signing are equally safe, due to their unique, secure links.

Revv's evidence summary provides a step-by-step audit trail of each action taken during the signing process with data and time stamps along with signers' details and IP addresses. The evidence summary safeguards your contract from the risk of fraud, forgery, admissibility, and ensures compliance and validity.

Revv is an intelligent business partner that helps you create professional documents with safe and effective electronic signature blocks using simple drag and drop functionality. Revv's electronic signature blocks are easy for you to create, easy to edit, and easy for signers to understand and execute. Moreover, you can choose the type of signature you want with Revv.

Want to send your document for eSignatures to multiple recipients altogether? Use Revv's 'Bulk Send' feature, and you are good to go. Revv provides a forever cloud-based storage, retains all your electronic records, and keeps them safe, organized, and easily accessible.

Best of all, electronic signatures created with Revv are mobile-friendly, making for a more convenient process.

## TAKE THE STEP

Obtaining electronic signatures is lightning fast, valid, and an acceptable method of document execution in the United States as well as in over sixty other countries. You can feel confident obtaining electronic signatures for your most important documents and reduce the execution time for agreements simply by switching to electronic signatures.

You get unparalleled control and visibility into your business process. Revv makes transitioning to electronic signatures easy by providing fully integrated software that guides you in an easy step-by-step process and provides a seamless workflow. The drag and drop editor means virtually anyone can create a professional document with electronic signature blocks. There's even a selection of hundreds of ready-made document templates to get you started.

Revv carries out and captures the eSigning processes from beginning to end and makes them legally enforceable by empowering businesses to replicate all events and actions in audit trails.

## RESOURCES

Learn more about electronic signatures, refer to the following resources -

- UETA and ESIGN Act - A Practical Guide
- Why Businesses Need Online Electronic Signature Management
- Best Electronic Signature Software: Comparing the Top Brands
- What Does an Electronic Signature Look Like
- Digital Signature vs. Electronic Signature: What's the Difference
- What is a Digital Signature and How it Works
- Electronic Signature Sample: Different Ways To ESign A Document
- Creating An Electronic Signature Workflow

This article intends to provide you information w.r.t the validity of electronic signatures. While we have taken all steps to ensure that all the information provided here is right, please note that this article is not a substitute for legal advice. E-signature laws can change, and we don't guarantee that the details in this article stand correct all the time. If you need to know about the legality and implementation of electronic signatures in your location, you should consult legal counsel.