OneSpan
Be bold. Be secure.

E-SIGN IS NOT ENOUGH: HOW TO REDUCE LEGAL & COMPLIANCE RISK WITH ELECTRONIC EVIDENCE

WHITE PAPER

TABLE OF CONTENTS

This whitepaper is not intended as legal advice or legal interpretation of ESIGN, UETA or any other laws or regulations. The information presented here is for general purposes only, and does not constitute legal advice.

INTRODUCTION

Today, businesses of all sizes are moving their customer transactions to the web. As the adoption of electronic signature technology grows, so does the number of e-signature solutions in the market. Because these solutions are all “ESIGN/UETA compliant”, you may think they will all provide the same level of enforceability in the event of a dispute. This is false.

The federal ESIGN and state UETA laws give electronic signatures the same legal weight as traditional ink signatures. These laws do not give e-signatures any special status. Contract and evidentiary rules apply to electronic records in the same way they do with paper. If ever a dispute over an electronically signed contract goes to court, judgment will be rendered based on the evidence admitted. Essentially, it is the strength – or weakness – of your electronic evidence that determines your exposure to legal and compliance risk.

If ever a dispute over an electronically signed contract goes to court, judgment will be rendered based on the evidence admitted. Essentially, it is the strength – or weakness – of your electronic evidence that determines your exposure to legal and compliance risk.

The good news is that using an electronic process to capture a customer’s signature provides stronger evidence than is possible with paper and more importantly, has been proven to reduce the risk of legal disputes. But what exactly is “electronic evidence”? What are the best practices for capturing and archiving all the digital fingerprints that customers leave when they transact with you online? How can this evidence help enforce e-contracts? And how can you use it to avoid going to court altogether?

To help secure the enforceability of your electronically signed contracts and agreements, this article presents the recommendations of legal experts, as shared at industry conferences and webcasts , including: Pat Hatfield and Greg Casamento, partners at Locke Lord LLP, and Frank Zacherl, litigator and partner at Shutts & Bowen LLP.

E-Signature Evidence 101

Electronically executed business transactions have unique advantages over the paper world. When your business sends a paper document package through the mail for a customer to sign, you have no control over what happens once the documents leave your hands. Similarly, if your business takes place in retail branches or through a remote sales force, you have little control over the process until the documents return to the back office for processing. Was the customer presented with the required disclosures? Did they sign in all the required locations on the document(s) to properly indicate intent? Were the proper procedures followed at every stage of the process?

The blind spots that exist with paper are eliminated when transacting online. In fact, businesses can leverage electronic signature technology to capture comprehensive evidence related to the signer(s), the document(s) and the entire signing process. Think of electronic evidence as the digital fingerprints the signer leaves as they go through an online transaction.

To head off potential litigation when using electronic signatures and transactions – especially in regulated processes – it is crucial to capture these digital fingerprints in the form of electronic evidence. Make no mistake: the courts recognize the legal validity of electronic records, signatures and transactions. The technology and laws have been tried in court and proven effective. But defending against legal disputes is about much more than just presenting an authentic signed record of an electronically signed agreement. It is about proving:

- The signer consented to the use of electronic signatures
- The signer intended to be bound by the terms of the contract
- The electronic records have not been altered since being signed
- How the records were presented to the signer
- That the signing process complied with all applicable laws and regulations
- That the signer had access to reliable copies of the signed document(s) after the fact
- And more

Capturing Evidence Through Dual Audit Trails

Proof of all of the above should be captured in two types of audit trails: a static audit trail and an active audit trail.

Document-level evidence is at the heart of any electronically signed transaction. This is captured in the static audit trail which enables you to verify basic signing-related information, such as who signed what document, and at what time, from where. It consists of a verifiable electronic record, the digital certificate used to sign, signature block image, time stamp and IP address.

The second type of audit trail, the visual audit trail, takes this a step further and provides context for how an electronic record was presented, reviewed and signed. It captures everything that occurred during the signing workflow, web page by web page. As a result, an organization can pull the active audit trail and play it back screen-by-screen to see what happened, like a security camera.

Also referred to as "evidence of the signing process", the active audit trail is a requirement stipulated by federal agencies such as the Internal revenue Service[1] (IRS) and the US Department of Education (DoE). The DoE stipulates when electronic signatures are used on federally-insured student loans, it is necessary to have "a copy of each screen as it would have appeared to the borrower of the loan or loans the Secretary is enforcing when the borrower signed the note electronically."

Because it provides proof of how a customer completed a transaction on the web or through a mobile device, an active audit trail's evidence is often so strong and compelling that it can deter cases from going to court in the first place. However, most ESIGN-compliant electronic signature solutions do not

STEPS IN AN E-SIGNATURE WORKFLOW

ACCESS · AUTHENTICATE · PRESENT · COMPLETE FORMS/ ENTER DATA · SIGN · DOCUMENT UPLOAD / UPDATE · DELIVER

offer an active audit trail. Most merely provide basic log files (not to be mistaken for an active audit trail). OneSpan Sign does it all, capturing the web pages that the customer viewed and signed, their order, time and date, email notifications, SMS codes sent and other transaction data.

How Effective Is Dual Audit Trail Security?

The true test of any technology is how it performs in the call of duty. One of the nation's top auto insurers can attest to the fact that electronic signatures decrease the risk of legal disputes compared to the traditional pen and paper signing process. This insurance company has been capturing customers' signatures electronically in applications for the last 10 years, and has only seen one case involving e-signed records go to court.

According to the insurer's attorney, Frank Zacherl, partner at Shutts & Bowen LLP, "Despite more than one million customer inquiries related to the electronic signing process, less than two dozen resulted in a lawsuit actually being filed. All except one of these plaintiffs almost immediately dropped their cases due to the persuasive electronic evidence that was captured by the electronic signature system."

Case law has also shown that if the e-signature process is clear to the signer, and an organization can prove that its customers knowingly consented to the terms and conditions of the agreement, the courts will enforce the electronic transaction. Recent court cases illustrate the importance of a well-designed process, backed by comprehensive evidence of the electronic transaction. The following are particularly instructive cases:

> David Whitaker, a lawyer with [DLA Piper], said that banks must be able to demonstrate that customer documents are protected, and that they can't be changed after they're signed. They also need to be able to demonstrate the process, down to the specific screenshots the customer sees, for putting an electronic signature on a document.
>
> "You want to be able to show at the courthouse what the customer experiences," Whitaker said.
>
> **American Banker**
> The Circuit: An E-Signature Event

Ultimately though, the goal of reliable and persuasive electronic evidence should not be to help you win in court. Rather, your electronic evidence should help you stay out of court altogether.

How to Stay Out of Court

To prevent going to court, there are a number of things you can do when bringing customer transactions online – with the most important taking place long before a legal dispute arises.

LONG V. TIME INSURANCE COMPANY	VINHNEE V. AMERICAN EXPRESS	BARWICK V. GEICO	LORRAINE V. MARKEL AMERICAN INSURANCE COMPANY	BAR-AYAL V. TIME WARNER CABLE INC.
In this case, the court ruled in favor of Time Insurance, validating the company's use of e-signatures for health insurance contracts, with the evidence generated being deemed admissible in a court of law. This case is helpful to anyone looking for support of the use of e-signatures in an application process, especially where the signed application is later provided to the consumer.	American Express lost a bankruptcy proceeding because it failed to lay a proper foundation for computerized records being submitted as evidence of the defendant's credit card statements. An appeals panel used an 11-point evidentiary foundation to determine if the records were admissible.	This case questioned the validity of the UETA law. The Arkansas Supreme Court sided with GEICO, noting that UETA could not be more straightforward in allowing the plaintiff's electronic record to satisfy the law that requires a record to be "in writing" (i.e., on paper).	This case demonstrates how capturing electronic evidence without laying the proper foundation can deem the evidence inadmissible, and thus an e-contracting business process unenforceable. Chief United States magistrate Judge Paul W. Grimm would not admit electronic records into evidence because neither party could demonstrate record and process reliability. In fact, he wrote a 100-page opinion that provides guidance on the authentication and admissibility of electronically-stored evidence.	In this case, the court upheld an "I Agree" online contract that required arbitration, based on the defendant re-creating the electronic process from its software in court to demonstrate acceptance of its agreement by the plaintiff.

1 First, lay a strong foundation by designing your e-sign process with enforceability and admissibility in mind. “What has become clear is that a reasonably well-designed process supported by the appropriate technology can reduce litigation and compliance risk overall,” says Pat Hatfield, partner at Locke Lord LLP. Such a process supported by the right technology can generate admissible and credible evidence, and ultimately make the evidence easy to understand.

2 Second, “Prior to rolling out electronic signatures and electronic transactions, organizations should consider putting a plan in place for responding to the concerns of customers and attorneys, and quickly resolving potential legal disputes,” says Frank Zacherl, partner at Shutts & Bowen LLP. (See the best practices checklist at the end of this article)

In short, a good plan ensures that employees and representatives are trained and provided with scripts on how to field customer questions and regulatory inquiries with regards to the use of e-signatures. A special team of representatives can also be assigned to answer more involved questions. The example cited above shows how having verbal and written responses prepared in advance can quickly deflect disagreements and address customer concerns.

Settlement Negotiations, Compliance Audits and Court

To help prevent unfavorable outcomes in the event a dispute escalates, ask yourself:

- What can I prepare in advance?
- How reliable is my evidence? Can it be reproduced quickly and easily?
- Do I have an experienced e-signature vendor to support me?

Advance Preparation

First, prepare a file of legal memoranda. Preparing afidavits and discovery responses in advance will ensure you are in a position to quickly mount the strongest defense possible – even with limited in-house legal resources.

Second, prepare a list of subject matter experts. You can have the best technology and the best system in the world, but if you go to court, you will want to have experts who can explain it. Expert witnesses must be able to present the electronic evidence in a manner that can be easily understood. Keep in mind that opposing counsel, judges and juries are not always interested in the technology details, but rather the process used to obtain the electronic signature. This is best accomplished by having an expert walk through all of your process evidence, including the web pages that the customer was presented with as they reviewed, acknowledged and signed the e-contract or e-application.

How Reliable Is my Evidence?

For contracts to be admissible and enforceable, the signed documents and associated evidence must be reliably reproduced, meaning in a way that maintains integrity. Reproducing evidence of an electronic transaction that occurred several years back can be a daunting task. An electronic signature platform makes the process of e-discovery easier, more reliable and less expensive by providing you with tools that provide the ability to search, find and playback a specific transaction’s active audit trail in a few clicks.

Can I Rely On my Vendor for Help?

If a dispute proceeds to litigation, the vendor must be able to help defend its client’s legal position and fend off disputes. To do that, the vendor must still be in business and their legal expert must be available to assist the client and their legal team during a court case. According to Frank Zacherl, “An important factor in successfully defending the position of one of our insurance clients, was the testimony of our client’s electronic signature provider. Michael Laurie of OneSpan provided critical testimony with regards to the security and reliability of the technology in producing authentic records and accurately reproducing the process.”

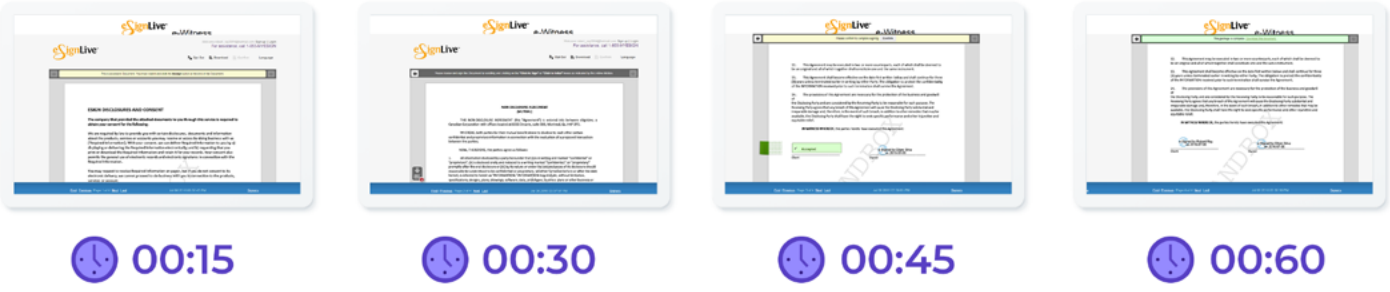

Figure 1. IRS e-signature regulations state, “An audit log of the entire electronic signing ceremony must accompany the electronically signed 4506-T to establish non-repudiation.” This image provides an example of how the visual audit trail in OneSpan Sign meets this requirement, by recording each screen seen and action taken as part of an electronic signature transaction.

Beyond ESIGN Compliance

At OneSpan, our technology is based on decades of best practices and learnings from thousands of organizations, as well as the country's leading legal experts and industry associations. The following is a list of the top legal/compliance considerations to look for when selecting an electronic signature solution:

1 Process Design

As mentioned earlier, it is crucial to design your e-sign process with enforceability and admissibility in mind. If you are regulated, you also need to ensure you design a process that is compliant; otherwise, there is little point in capturing evidence of a flawed process.

How you choose to execute each step in your process determines compliance and enforceability. Solutions that offer too simple an approach or that are rigid in their workflow options may compromise your legal position. Look for flexibility in workflow, signer sequence, document sequence, approach to user authentication, method of document distribution and more. OneSpan Sign's flexible process design can help you ensure all of the proper procedures are followed at every stage of the process, including:

- Allowing you to define and enforce any number of business and workflow rules (e.g., in a multi-signer, multi-document process, you may need to define who signs first, in what order documents are presented, etc.);
- Offering secure, web-based document download rather than sending documents containing confidential information via unsecured email, which could compromise a customer's private data;
- Presenting documents in a way that respects every aspect of document integrity, right down to font size, to meet display requirements for documents such as disclosures;
- Presenting signature cues in a conspicuous way to ensure intent is properly established – and, if you need to capture confirmation of opt-in/out intent (think of the 'accept' or 'reject' statement in a uninsured/underinsured motorist auto insurance form) a checkbox or radio button can be added.

2 Active Audit Trail

Case law has shown that in legal disputes involving web-based processes, the entire electronic process becomes discoverable and the security, integrity and chain-of-custody of the documents and any other relevant information can be disputed by a plaintiff. For this reason, it is not advisable to rely on a simple list of web log files to convincingly prove intent was established and the right process was followed. Web log files alone will not deter people from claiming:

- "Somebody may have tampered with the system."
- "I wasn't presented with that information."
- "I didn't understand what I was signing."

AUTO INSURANCE USE CASE

According to *USA Today*, "Despite laws in nearly every state requiring auto insurance, one in seven drivers in the US goes uncovered."[1]

To illustrate this, when Mary Smith was involved in an accident caused by an uninsured motorist, she was not able to get compensation from her carrier to cover damages. Mary remembered electronically signing her auto insurance policy on her carrier's website, but did not remember rejecting the uninsured (UM) motorist coverage. When Mary called her insurer to discuss the claim, she was transferred to a specially trained e-signature team within the carrier's customer care department who knew how to address her inquiry. The special team coordinated with their document custodian to send Mary a copy of the UM rejection form she had e-signed when she took out the policy.

From there, the carrier's special team followed procedure and elevated the call to a supervisor, who initiated a discovery request to reproduce copies of the online transaction web page by web page, in order to show Mary:

- which documents she had viewed
- in what sequence
- the amount of time she spent viewing each and more

Mary conceded that she must have, in fact, signed the form. Had the insurance company not had the ability to reproduce Mary's entire transaction from beginning to end, the outcome might have been different. In fact, the carrier was even able to show that after completed the application process, she went back to the website the next day and downloaded copies of everything she signed, including the e-signed rejection of UM coverage form.

Best practice is to capture the full signer experience (i.e., all web pages, documents, disclosures, pop-up windows, and other on-screen information, as well as emails and SMS messages sent, together with the time and date of each event). OneSpan Sign records all actions taken by each signer, including moving to the next document or web page; clicking on a button; applying a signature; and downloading completed copies of documents after the fact.

3 Vendor Independence

E-Signed records must be tamper-evident to be considered enforceable by the courts. OneSpan Sign uses digital signature security to secure and authenticate data, in order to eliminate the risk of repudiation (e.g., "I signed something but that's not what I signed."). The embedded static audit trail should also be encrypted and tamper-evident.

Having the static audit trail embedded within the e-signed document – as opposed to "logically associating" separate files in a vault or proprietary database – is more secure, easier to manage and more portable. There are two very pragmatic reasons you want to ensure the signature(s) and audit trail are embedded in the e-signed document: (1) the authenticity of the record can be verified independent of the e-signature software, meaning you do not need to worry about your vendor or service provider being around to validate it, and (2) the record can securely travel through any email, storage or archival system without being compromised or requiring additional programming.

4 Easy Access To Audit Trail Evidence

With OneSpan Sign, the visual audit trails are securely and reliably housed in a single archival system. The software's Process Reviewer provides the ability to search, find and playback any transaction. Search criteria include unique process ID, date range and other variables – making it easy to quickly find what you need.

Further, a self-contained evidence package can be exported out of the OneSpan Sign database to either a standalone file or imported into an enterprise content management or records management system. This way, you can manage the evidence in a manner that meets your long-term retention requirements. In addition, screens from the visual audit trail can be securely output to PDF or paper and sent to attorneys or auditors so they can review it offline.

5 Additional Considerations For Mobile Transactions

For mobile transactions, OneSpan Sign offers the ability to capture additional evidence beyond static audit trails, visual audit trails and log files. Depending on the risk level associated with the mobile e-sign process, your organization may want to capture GPS coordinates, voice/video recordings and uploaded images relevant to the transaction, such as a photo of a driver's license for additional customer authentication, or a photo of car damage in an insurance claim.

Conclusion

When evaluating electronic signature solutions, there are valid legal and business reasons why you need to set the bar higher than simply "ESIGN/UETA compliant". Millions of civil suits are led in the US each year. A typical contract dispute takes about 300 days to resolve through the courts. With the average lawsuit costing $300,000, adopting an electronic signature solution with strong audit trail evidence – combined with a good business process and the protocols described in this article – can save you costly settlement expenses and legal fees. Satisfying regulators' inquiries, passing audit, avoiding regulatory fines and lowering the cost of e-discovery are all equally important reasons to consider an e-signature solution that captures comprehensive audit trails.

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US

For more information:
info@OneSpan.com
OneSpan.com/sign

Last Update August 2018.

BEST PRACTICES CHECKLIST: TECHNOLOGY REQUIREMENTS FOR STRONG ELECTRONIC EVIDENCE	
REQUIREMENT	**DETAILS**
Capture as much document-related data as possible	The audit trail needs to include the: • Digital signature • Digital certificate • Signature block image • Time stamp
Secure the document and signature(s) so they cannot be altered	• The audit trail, signatures and documents must be secured in a manner that renders the information tamper-evident. • Use digital signature encryption to hash each document and hash the audit trail. Eliminate risk of repudiation, e.g., "I signed something but that's not what I signed."
Capture as much process-related data as possible	• IP address • Date and time stamp of all events • Web pages, documents, disclosures and other information presented • The length of time spent reviewing each document • What each party acknowledged, agreed to and signed • All other actions taken during the transaction
Go beyond log files	Web log files alone will not deter people from claiming: "Somebody may have tampered with the system."; "I wasn't presented with that information." ; or "I didn't understand what I was signing." To safeguard against this, be sure the e-signature solution captures a record of the full signer experience.
Ensure the electronic evidence can be easily retrieved	The signature audit trail should be embedded into each document, rather than storing the signatures separately and "logically associating them" in a database. Otherwise, pulling data from a variety of systems and databases will result in a lengthy and costly e-discovery process and make it difficult to establish the authenticity of e-signed documents.
Plan for long-term archiving & accessibility	The electronic document and associated signatures, audit trails and evidence must be accessible for the lifetime of the record (50+ years some cases, e.g. a life insurance policy). Adobe PDF, an ISO standard, is a reliable choice for the long term.
Verify that the evidence is portable	Can you export evidence to PDF or paper? Can you export evidence to a single HTML file?
Ensure there are tools to access the evidence	Do you have the ability to search for, find and playback a specific transaction's active audit trail evidence, in just a few clicks?
Ensure there is flexibility in process design	Solutions that offer too simple an approach or that are rigid in their workflow options may compromise your legal position. Look for flexibility in workflow, signer sequence, document sequence, approach to user authentication, method of document distribution and more.

[1] http://michiganinsurancecoalition.com/2011/09/12/one-in-seven-drivers-have-no-insurance/