WHITE PAPER

OneSpan

TOP 6 LEGAL RISKS WHEN ADOPTING E-SIGNATURES

AND HOW TO ADDRESS THEM

CONTENTS

This white paper is not intended as legal interpretation of relevant laws or regulations. The information presented here is for general purposes only and does not constitute legal advice.

RISK AND ENFORCEABILITY

HOW TO REDUCE RISK AND STRENGTHEN THE ENFORCEABILITY OF SIGNED RECORDS

Moving business processes online without introducing new risks is not a simple task. The fraud, repudiation, admissibility, and compliance risks are challenging enough to address when executing transactions on paper. If not done properly in the electronic world, these risks can be far greater. This paper discusses how a well-designed process, supported by new-generation electronic signature technology, can actually reduce risk and increase the enforceability of e-transactions compared to paper processes.

While the ESIGN Act gave electronically signed records the same legal validity as their pen and paper counterparts, it did not guarantee that e-records will be admitted into court as evidence or provide adequate defense to ensure a positive outcome in the event of a dispute. Moreover, meeting the basic requirements of the ESIGN Act does not mitigate against several other risks associated with bringing high-value consumer transactions online.

A new generation of electronic signature technology has emerged in response to evolving market demands for a more comprehensive solution that provides better compliance and control of highly regulated transactions. Electronic signature solutions today must go beyond simple signature capture to control the execution of transactions electronically from start to finish, reducing risk and capturing the most comprehensive audit trail evidence.

This paper explains how OneSpan Sign addresses the top six risks of bringing processes online as identified by leading e-commerce law firm, Locke Lord LLP, which has guided Fortune 500 companies in the design and implementation of electronic signature processes.

RISK 1: USER AUTHENTICATION RISK

“THIS ISN’T MY SIGNATURE”

While the vast majority of legal disputes challenge the terms and conditions of a signed document, not whether a signature belongs to a person, user authentication is still a risk organizations must address, especially when doing business with new and unknown customers over the web.

Locke Lord defines the user authentication issue as the risk that a document is signed by someone other than who the person actually signing claims to be, and therefore, a forger. The risk, according to Locke Lord, is that a company will not be able to enforce the document against the person with whom the company thought it was contracting, because the person claims, “That is not my signature!”

It is important to note, however, that a signer’s identity is rarely authenticated in one instance or based on a single point technology, regardless of whether transactions take place remotely over the web or face to face. Normally, a combination of events and evidence is used to establish the identity of a party to a transaction, including conversations with agents or representatives, the provision of personal information, and signatures.

E-Signature technology combined with a solid business process can mitigate user authentication risk with a number of identity and credential verification techniques. A well-designed e-signature solution supports a wide variety of authentication methods, including digital identity verification, user ID/ password, knowledge-based authentication, smart cards, or multi-factor authentication services (e.g., OneSpan’s Digipass®). Look for an e-signature solution that can easily integrate with many types of authentication methods throughout the e-sign workflow. This provides the flexibility to calibrate the level of authentication to the risk associated with each process.

A WELL-DESIGNED E-SIGNATURE SOLUTION SUPPORTS A WIDE VARIETY OF AUTHENTICATION METHODS, INCLUDING:

- Digital identity verification
- User ID/password
- Knowledge-based authentication
- Smart cards, or multi-factor authentication services (e.g., OneSpan’s Digipass®).

In the event that a person denies having signed a record, a point to consider for determining the legitimacy of the claim is whether the person, subsequent to the transaction, made a payment to obtain the product or service? Further, what would motivate the person to make a fraud claim, knowing that without the existence of a valid contract, the relationship would be rendered null and void, and the claim would be moot?

RISK 2: REPUDIATION RISK

“THAT’S NOT WHAT I SIGNED”

●●●●●●

E-Signatures can mitigate repudiation risk by ensuring that a person’s signature is permanently bound to the exact contents of the record at the time of signing.

Locke Lord defines the second risk, repudiation, as the risk that a person claims the document was altered after they signed it. “The risk is that a company relying on an applicant’s electronic signature seeks to enforce the terms of the signed document bearing the applicant’s signature and the applicant claims, ‘Yes, that is my signature, but the terms and conditions of what I signed are different than that document!’”

Repudiation generally occurs when a customer has provided false information in a document or now disagrees with terms and conditions to which they had originally agreed. Therefore the customer is asserting that although they did sign a document, either the document or their signature has been altered.

E-Signatures can mitigate repudiation risk by ensuring that a person’s signature is permanently bound to the exact contents of the record at the time of signing.

A secure e-signature solution uses digital signature technology to create a link between the electronic record, the user authentication data, and any additional evidence related to the transaction. A digital “fingerprint” of the record is taken at the time of signing using industry-standard hashing algorithms. This fingerprint can then be used to detect even the smallest change to the signed document. A person cannot, therefore, claim that someone tampered with the e-signed record, nor can the person claim that their signature was fraudulently added to another document, because the solution would visibly invalidate the electronic signature.

RISK 3: ADMISSIBILITY RISK

"OBJECTION, YOUR HONOR"

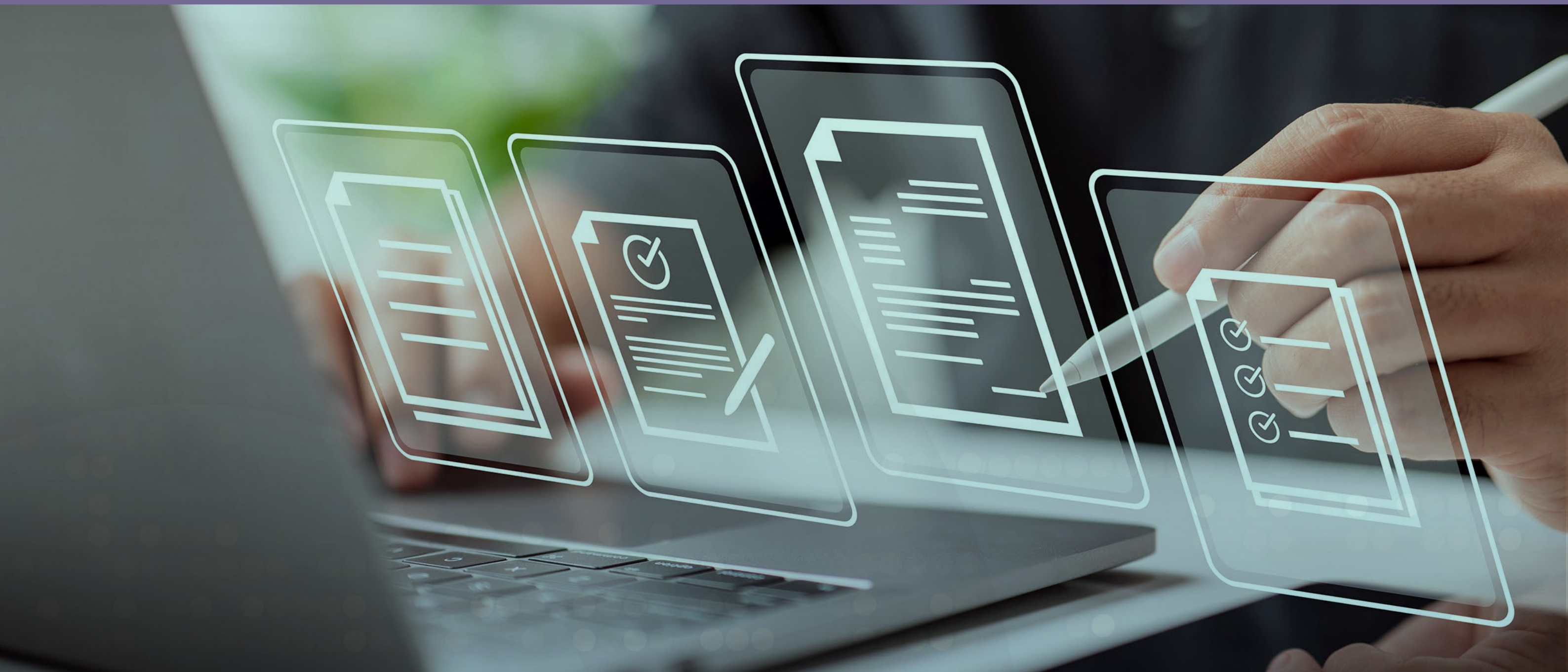
●●●●●●

Locke Lord defines the risk of admissibility as the risk that an e-contract cannot be enforced, because it does not provide strong enough evidence and, therefore, is not admissible in court. Laying the proper foundation, according to Locke Lord, is critical.

Producing reliable and persuasive electronic evidence, however, can be challenging, especially when processes take place over the web. Web interfaces and processes change frequently in response to compliance requirements and usability feedback, making it difficult for organizations to recreate a customer experience that occurred months or years past. Even if historical web interface information is retained, it is likely stored in a number of separate databases and content management systems, making it difficult to retrieve and reproduce in a reliable manner.

To mitigate admissibility risk, look for an e-signature solution that enables organizations to capture and reproduce every step that occurred during the transaction execution. By capturing a digital audit trail of the entire transaction from beginning to end, the e-signature solution offers organizations better visibility into processes and stronger evidence than is possible with paper.

Look for an e-signature solution that captures evidence of the entire e-transaction from beginning to end. This offers better visibility into the process and stronger evidence than is possible with paper.



RISK 4: COMPLIANCE RISK

“I NEVER SAW THAT”

●●●●●●

In addition to the ESIGN Act, organizations must comply with rules and regulations for presenting documents, disclosures, and other information at specific stages during a transaction. Failure to comply can cost organizations dearly, including possibly rendering the signed document null and void. Locke Lord explains that organizations can be sanctioned by regulatory authorities and the other party involved in the transaction may be permitted to avoid its obligations under the documents signed. Further, depending on the industry, organizations may be subjected to hefty fines, lose accreditation status, or compromise brand equity.

E-Signatures can mitigate compliance risk by enforcing regulatory requirements and proving that compliant processes were followed throughout a transaction.

A well-designed e-signature process enables organizations to configure the business logic needed to control the execution of transactions so that compliant processes are followed throughout. This includes ensuring that ESIGN Consent is obtained, that all required documents, disclosures and information are presented in the correct format, sequence, and timeframe; that no signatures are missing; and that all parties receive a copy of the final records. Moreover, because the transaction remains electronic, there is no need to re-key data and potentially introduce errors.

RISK 5: ADOPTION RISK

"AM I DONE YET?"

●●●●●●

While user adoption is not a legal risk per se, it is important to consider in the context of this discussion. Organizations often look to adopt more rigorous security in an attempt to address legal or compliance risk. This approach is not recommended, because security and usability are most always in conflict and adopting excessive security measures can negatively impact return-on-investment. Locke Lord defines adoption risk as "the risk that the e-process takes longer than the traditional process or is not as convenient as the traditional process and consequently, adoption of the process is slow. The risk is that a company invests considerable resources to design an e-process only to find that there is little use of the e-process."

In an effort to address the user authentication and admissibility risk, organizations often inadvertently make the electronic process more complex and difficult to use, because they set a higher standard for security than is normally required. It is important to remember that the primary reason for moving transactions online is to make them more efficient and convenient for all parties involved. If e-transactions become too complex, users will simply abandon the process and an organization will not realize the full potential of its investment.

E-Signatures can mitigate adoption risk by offering flexible options for e-signing, security, and authentication to accommodate the unique requirements of each process.

A flexible e-signature solution provides options for identifying and authenticating customers, presenting documents, and applying electronic signatures to ensure high adoption and an optimal user experience across all channels and processes. For instance, organizations can use digital identity verification to confirm that unknown online applicants are in fact who they say they are.

> E-Signatures can mitigate adoption risk by offering flexible options for e-signing, security, and authentication to accommodate the unique requirementsof each process.

In point-of-sale environments, documents can be presented to customers in paper format for review and customers can add their signature to records by hand-signing on an electronic pad, tablet, smartphone, or other device. For web processes, customers click-to-sign documents directly within the browser, thereby eliminating the need to download special software. These options mean organizations do not have to compromise on requirements and can achieve the optimal balance between security and usability.

RISK 6: RELATIVE RISK

“HOW DOES IT COMPARE TO PAPER?”

Locke Lord defines relative risk as the risk the e-process poses compared to traditional processes: “There are authentication risks, repudiation risks and compliance risks with the traditional process of using wet ink and paper to complete transactions. Many companies have not examined such risks until they begin developing an e-process. For most electronic signature and e-discovery processes, the goal will be to have the transaction, on the whole, be no riskier than the current processes.”

E-Signatures decrease overall risk compared to paper by providing greater control and visibility into processes.

When processes fall to paper, organizations not only decrease their operational efficiency and incur unnecessary costs, they lose control and visibility into their processes. The only evidence that a business agreement or transaction took place is the resulting document or contract. While this paper evidence captures signing intent, it does not reproduce all events leading up to the act of signing which may render a document ineffective or unenforceable. Further, paper documents are more easily lost and destroyed, and may be archived in a manner that makes them difficult and time-consuming to retrieve for litigation, regulatory, and internal control purposes.

When processes remain electronic, organizations gain unprecedented control and visibility into their business. E-Signature software fully executes and captures e-signing processes electronically from start to finish to enforce business, legal, and regulatory requirements and enables organizations to reliably reproduce all events and actions. And because processes remain electronic, they can be monitored for anomalies and security breaches, and system administrators can be alerted.

CONCLUSION

The ESIGN team at Locke Lord has concluded that a reasonably well designed process, which includes making sure the correct version of the mandated forms are used, supported by e-signature technology such as OneSpan Sign, can reduce the authentication, repudiation, admissibility, and compliance risk below the levels of paper processes, and capture a reliable record of the entire transaction.

About OneSpan

OneSpan, the digital agreements security company™, helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at **OneSpan.com**
Contact us at **www.onespan.com/contact-us/onespan-sign**