

Patrick J. Hatfield
Locke Lord Bissell & Liddell LLP
phatfield@lockelord.com

Gregory T. Casamento
Locke Lord Bissell & Liddell LLP
gcasamento@lockelord.com

Kelly Purcell
eSignSystems
kpurcell@esignsystems.com

eVaults Are Essential to Creating Admissible and Enforceable Electronic Signature Transactions

While storage and retrieval of electronic transaction documents can sometimes be viewed as an incidental back-end storage issue, safely storing transaction documents for later retrieval in the event of an enforceability challenge is a critical component of any electronic signature process. This is because the rules of evidence, State and Federal, and the required evidentiary foundations that apply to every aspect of a paper based process utilizing a wet ink signature, apply equally to every aspect of an electronic signature process. This includes electronically securing, archiving and retrieving the electronically signed and reviewed transaction documents. Because the storage and retrieval aspect of every electronic signature process is subject to evidentiary attack, users must ensure their systems satisfy the admissibility standards by implementing a secure method to archive and retrieve electronic documents so that their process results in enforceable electronic transactions.

eVaults, such as *eSignSystems*' SmartSAFE™, are essential to meet the requirements under the evidentiary rules and in particular Federal Rule of Evidence 901. In the context of electronically archived documents, Rule 901 requires that the user demonstrate that the electronic transaction documents offered into evidence are authentic. That is essentially that the documents are what the user purports them to be - true and accurate transaction documents, signed by the party to whom the user seeks to enforce the transaction. eVaults help users meet this evidentiary challenge and establish in court the following:

- the documents retrieved from the eVault and submitted as evidence to enforce the transaction, such as the electronically signed documents, required disclosures, and the audit trail, are all true, accurate, and complete copies;
- the documents reflect what the user presented to the signer and the signers consent to the terms and conditions of the transaction; and
- the documents submitted in court to enforce the transaction were generated from electronic records that were electronically sealed and stored in such a way that each record, as accurately represented by the evidence submitted in court, could not have been altered without detection;

Thus, the proper use of an eVault enables users to securely archive and retrieve transaction documents, including audit trails, in a way to prove that the documents proffered to show what the customer was presented with and signed are true, accurate and complete. The eVault also can establish that those documents are “unalterable without detection”, i.e., that the documents could not have been altered without detection by the user between the time those documents were signed, sealed, stored, retrieved and then later presented in court by a witness, typically the user's evidence custodian.¹

Meeting these requirements should be sufficient to satisfy Rule 901's requirement of authentication and to allow the court to make a factual finding that the documents presented by the user are admissible and enforceable.

¹ Users should consider and identify who would be qualified, willing, and able to testify as a custodian on these items when a transaction record from the electronic signature process is challenged.