

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW



<http://ddee.pf.com>

Reprinted from Vol. 5, No. 12 | December 2005

TALKING TECH

Legal Defensibility of E-Signatures Tested in Simulated Trial

By Brian Casey and Pat Hatfield

The law firm of Lord, Bissell & Brook LLP and on-demand electronic-signature firm DocuSign Inc. recently staged a two-hour mock trial to demonstrate the unique issues that challenge electronically signed documents. The event included a summary of applicable e-signature law, a trial demonstration and an expert panel discussion.

The outcome of the trial, heard before Judge Michael A. Yarnell, recently retired from the Maricopa County, Arizona Superior Court, revealed that while the issues may be different, proving an electronically signed document presents no greater risk than proving a paper document signature — if a well-defined e-signing process is in place. Moreover, a company can actually improve its ability to defend or enforce its rights by using an effective e-process.

Applicable e-Signature Law

The federal Electronic Signatures in Global and National Commerce Act (ESIGN), along with state-adopted versions of the model Uniform Electronic Transactions Act (UETA), establish a foundation for implementing e-signature and e-record processes. ESIGN doesn't preempt state versions of e-signature laws entirely; however, such state laws must be based on a pristine version of the model UETA.

As a result, state laws that are not "pristine" versions of UETA might be preempted in whole or part by ESIGN. With its broad preemption provisions and interplay with UETA, ESIGN provides a basis for developing a national e-signature strategy.

ESIGN doesn't require anyone to use or accept an electronic signature or record, but specifically provides that neither a signature nor e-record can be denied legal effect solely because it is in electronic form. Under ESIGN, an e-signature can be as simple or complex as one of the following:

- Clicking "I Agree;"
- Saying "I agree" into a recording device;
- A digital signature using PKI technology;

- An electronic image captured on a peripheral device;
- Any other way an electronic sound, symbol or process can be attached to or logically associated with an electronic record that is adopted by a person with the intent to sign.

Although ESIGN specifically exempts certain areas from coverage, exemptions are narrow and ESIGN covers most types of commercial transactions. Under ESIGN, for instance, an archived e-record will satisfy statutory requirements that a contract or other document be retained "in writing," if the electronic record is maintained in a form that all parties can retrieve later for reference.

ESIGN also recognizes that records of a transaction (whether completed electronically or not) may be archived exclusively electronically, but failure to archive records that can be accurately reproduced could render unenforceable the agreement the electronic record represents and bring about regulatory sanctions for failing to maintain the proper records.

Proving the Electronic Signature

The mock trial involved an electronically signed auto insurance application and whether or not the plaintiff's now deceased husband had purchased uninsured motorist coverage. The plaintiff, a very sympathetic widow, produced a paper copy of an insurance application that was different from the company's electronic record.

As a result the trial involved a challenge between the widow's paper copy and the company's electronic records. The mock trial included the widow's moving story and the company's testimony detailing its electronic signature process, which was based on the DocuSign web-based e-signature service.

A new process for eMutual, the name of the defendant in the simulated trial, allowed customers to complete insurance applications entirely online without the need to fax, mail, or courier paper documents. Through a Web browser

and Internet connection, eMutual customers were able to walk through coverage options, either independently or with the help of an agent, and then make selections to sign contracts online in DocuSign. This service provided a way for signers to create a unique electronic signature based on a number of identifiers including e-mail authentication, secret word authentication, and questions pulled from the customer's credit file.

To sign a document, signers dragged their signature to tagged locations in the document, with every action recorded in an audit trail. The signed document was then locked down and stored in a secure repository.

Electronically signed documents are essentially computer records that courts have long allowed as evidence. Under the Federal Rules of Evidence, and most similar state laws, objections to the admissibility of computer records are typically based on challenges to authenticity of computer records and challenges to computer records under the hearsay rule. Precedent surrounding these types of challenges has been exhaustively developed. As a result, the mock trial did not focus on admissibility arguments and methods. Most of the testimony was instead directed at how to develop the credibility of the competing documents where the original record was created electronically.

Using encryption and related technologies, an electronically signed document is effectively locked so that subsequent alterations are virtually impossible (tamper-proof) or readily detectable (tamper-sensitive). Key mock-trial testimony centered on the storage of the electronically signed, encrypted, and hashed insurance application within a secure central data repository.

Tom Gonsler of DocuSign, who played the role of expert witness for the defendant, testified a document cannot be modified once it is in the system. "What goes in is locked and can't be changed," he said. "Documents are not 'sent' to anyone, but stored on a DocuSign computer called a server the whole time during the signing process, and merely accessed and viewed for signing. The way the system checks the fingerprint or hash each time, and then can only be displayed if the numbers add up, virtually ensures that the data has not been manipulated or altered after it gets placed in that system."

Moving to cross examination of the defense witness, the plaintiff's attorney explored the possibility of what it would take to make changes to an electronically signed document without detection. In contrast to paper documents which can easily be modified using simple tools such as paper cutters, correction fluid, and copy machines, Gonsler pointed out that cracking an electronic vault is a far more complex process.

"It is technically possible, but the effort required to do it would be impressive," Gonsler said. "DocuSign uses an electronic key to lock the documents. The National Institute of Standards and Technology has estimated that it would take

approximately 149 trillion years to break this security key. However, the real challenge would be to also access the DocuSign database in Los Angeles, and break into that system without being detected, find the right file, decrypt the document, which could take years using very powerful computers, then ensure the audit system did not notice the intrusion."

Also critical to system trustworthiness was its ability to collect and record real-time transaction-related data in the mock trial. Systems such as the one described in the mock trial are designed to capture audit-trail data specific to the critical elements of a particular transaction. The audit-trail data included the date and time the late husband signed his electronic auto insurance application and the contents of that document at the precise moment it was electronically signed.

Ultimately, an effective e-signature process incorporates technology and redundant processes that could improve a company's ability to defend and enforce electronically signed documents. For example, the ability to make a document essentially tamper-proof and tamper-sensitive with common encryption and hashing technologies, and the ability to collect audit-trail data are not available when dealing with paper documents signed in wet ink.

Equally important, however, is how the proponent of the signature uses trial testimony to explain the system and the technology that makes that system secure and the e-signed documents tamper-proof and tamper-sensitive. With effective trial witnesses and testimony that a jury will understand and believe, the benefits of the electronic signature process and its technology have much to offer.

The Verdict

In the end, Judge Yarnell first found undisputed evidence that the insurance company, eMutual, had made uninsured coverage available to the insured and did so by a written electronic offer, complying with relevant statutory requirements.

From there he determined that "credible, substantial, and persuasive evidence" had been admitted from the electronic systems showing that the plaintiff rejected the offer of uninsured motorist coverage and electronically communicated that rejection to eMutual, and that no credible evidence of corruption, forgery, or alteration of those electronic records had been presented. He also concluded, "The electronic systems of eMutual and third party DocuSign used by the parties in this insurance transaction are secure, redundant, and encrypted."

Although neither party in this case was able to explain the inconsistency between the electronic records and the paper copy of the Uninsured Motorist Selection form, the preponderance of evidence and the credibility of the witnesses led Judge Yarnell to rule in favor of the defendants.

Key pieces of evidence included testimony that the electronic system and processes used by eMutual conformed to ESIGN legislation and accurately captured the plaintiff's intent. And that eMutual stored the signed contract in a secure repository where it effectively could not be altered in any way.

Given the rapid growth of online commerce activities involving larger and more complex contracts and agreements that normally would require a wet ink signature, it's

only a matter of time until a case such as this comes to trial. Careful examination of the technology involved from a legal perspective and effective planning will help ensure a similar outcome.

***Brian Casey and Pat Hatfield** practice in the Atlanta office of **Lord, Bissell & Brook LLP**. They focus a significant portion of their respective practices on e-signature and e-commerce. Reach them at bcasey@lordbissell.com and phatfield@lordbissell.com.*