Mortgage Banking
THE MAGAZINE OF REAL ESTATE FINANCE MARCH 2016

THE VIRTUAL MORTGAGE— Nearer Than You Think

— by JOHN HARRIS AND KATHY ZELENOCK —

Here's a quick rundown on the technology that's essential to electronic signatures.

Hot wax seals are no longer used in the mortgage industry to authenticate documents (and we're all the better for it). But its immediate successors—paper and ink (which came into acceptance somewhere around the 6th century)—are still the primary tools lenders use to finalize transaction documents. ¶ Other than the pen's evolution from quill to fountain to ballpoint, not much else has changed. ¶ To many, this is surprising. ¶ Most people today expect technology to permeate every part of business and life. In fact, more than 20 years ago, some industry experts predicted that within the span of a few decades, commercial mortgage loans would be fully automated so that a standalone kiosk would use biometric technology and large databases to make instantaneous underwriting decisions and finalize transactions. ¶

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES
www.signix.com | 877.890.5350 x1057 | sales@signix.com

While we remain woefully short of that particular vision—and are still reliant on paper processes—the industry is beginning to see incremental changes. This is particularly the case with electronic signatures.

In 2014, Forrester Research of Cambridge, Massachusetts, predicted that e-signatures could disrupt the age-old pattern of mortgage processing in as little as three years. That means that, after centuries as the standard practice, paper and ink may begin to become the tools of generations past.

The case for e-signatures in the mortgage industry

E-signatures have gained momentum across many industries by driving document efficiency. They are the final step of a digital transaction, and without them the journey is interrupted.

A document can originate, be modified, pass between parties and be stored online. But the moment it's time to close a deal, the printer needs to be warmed up.

The end game for all e-signatures is the same, but the technology used to get there can vary dramatically.

E-signatures keep documentation in a seamless digital workflow, and they present important opportunities for mortgage professionals, including:

■ ***Faster turnaround for transactions***—Cloud-based e-signatures allow parties to sign documents anywhere there is an Internet connection. This means lenders don't have to wait until everyone is assembled in one room, nor must they wait for documents to be shipped. Everything is accessible online and the signature process can happen in mere seconds.

■ ***Automated processing of documents***—Because the documents remain fully digital, they never have to be scanned back into a computer. Signed documents can automatically continue the processing workflow.

■ ***Money in the bank***—The materials and labor associated with a handwritten signature, multiplied many times over, are more costly than one might think. Paper, ink, shipping, storage and processing can cost thousands of dollars each month. E-signatures cut these expenses dramatically.

Further, the law makes it clear that acquiescence to an agreement can be expressed electronically.

The Electronic Signatures in Global and National Commerce Act (ESIGN), effective in October 2000, is a federal law ensuring the validity of electronic records and signatures for transactions. A similar law, the Uniform Electronic Transactions Act (UETA), has been adopted in some form by 47

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

states (with the remaining states adopting their own measures), establishing the equivalency of electronic signatures and manual signatures.

Widespread adoption of e-signatures requires technology that clearly addresses certain legal, authentication and security issues.

However, these laws are written broadly so as not to favor one technology over another or to stifle innovation. This can leave many looking to adopt e-signatures at a loss as to where to start in their search for an e-signature solution.

E-signature technology that works for mortgage lending

The end game for all e-signatures—to acknowledge approval of a document or transaction—is the same, but the technology used to get there can vary dramatically.

Some electronic signatures may be a simple scan of a wet-ink signature placed on a digital document. Others may just require clicking a box or typing in initials, and some are far more complex in their technical makeup.

Regardless of the options available, in an industry known for regulation and large sums of money, widespread adoption of e-signatures requires technology that clearly addresses certain legal, authentication and security issues.

Legal compliance

For assurance of a legally sound and valid e-signature within the mortgage industry, it's important to validate that:

- the correct party signed the documents;
- the party intended to be bound by his or her signature on the document; and
- the electronic record or document content associated with the signature has not been modified since the agreement was expressed.

Identification and authentication—making sure the right person signs

Making sure the right person signs the right document is obviously critical with something like a mortgage. In traditional closings, this is typically accomplished with a signing ceremony. A notary could check a driver's license, lenders may know the signers personally or sometimes just the act of signing a document in the presence of a third party implies the right person is signing.

With e-signatures, signer authentication can be more challenging, since parties may not be gathered around a closing table.

To ensure an e-signature will be accepted, it must include three elements:

- ***Origin***—The signature should be unique to the person using it. In electronic communications, this is confirmed when a unique symbol travels across a verified path of communications.
- ***Authenticity***—The signature must confirm that the appropriate party has authorized the document and the document was delivered via a trusted path with no tampering at any time during or after the signing process.
- ***Non-repudiation***—The way the signature confirms origin and authenticity must be able to withstand scrutiny and legal challenge.

Only technologies that satisfactorily address these issues will be adopted widely and for the long-term.

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

Intention to be bound

The ESIGN Act and UETA both require that signing parties express a willingness to be bound by electronic communications—the person signing the contract must want to be bound by that contract—so e-signature technology also must address intentionality, or proof that the signature was deliberate and purposeful.

This is more important for electronic signatures than wet-ink signatures because, like origin, authenticity and non-repudiation, the act of signing a document has become an implicit expression of intentionality.

With e-signatures, that intentionality needs to be more explicit because we don't have centuries of legal tradition to act as a frame of intentionality. Usually this is handled through an obstacle challenge—a password or a checkbox that binds the user to a list of terms and conditions, and declares the intent to be legally bound. For multimillion-dollar commercial lending transactions, lenders will have to determine the technological methods most appropriate for the specific transaction at hand.

Document integrity

Finally, there must be assurance that a document, once signed, remains in its final state without any later changes, whether ill-intended tampering with the document's content or unintended changes made by any party during the signing process if there are multiple signers.

With electronic documents, it can be hard to determine which is the original and which is the copy. So the law makes it clear that the focus is on the integrity of the information, not the "originality" of the document.

Storing electronic records means occasionally migrating those records to new media as storage technology improves. So, if the original document is stored on a floppy disk, for example, subsequent copies must retain the same integrity as they move from outdated media to newer media or virtual storage. Otherwise, we'd be chained to decades-old technology (or no technology at all) in order to maintain the original document.

Long-term validity and acceptance

Mortgage documents are long-term agreements. They must remain valid over time, and e-signatures play an important role in that validity. If a signature can no longer be verified for any reason, the enforceability of the loan could be jeopardized.

It's no surprise that security is a significant factor in determining appropriate e-signature services for mortgage lending.

And while most sophisticated e-signature services will be able to meet legal obligations described here, the manner in which e-signature services protect long-term validity varies wildly. So it can be helpful to classify e-signatures into two categories: 1) those that are dependent on a vendor and 2) those that are independent of a vendor.

With dependent e-signatures, verifying the validity (proof that the right person signed the right document with no subsequent changes) of an e-signature requires a link to the e-signature vendor's servers or website. That's where the digital information intended to prove the right person signed the right document lives. But technology changes and vendors or servers might be replaced.

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

If that happens, you could lose the digital proof of your e-signature's validity over time.

Independent e-signatures, by contrast, do not require a vendor to verify the validity of an e-signature. These are also called digital signatures, and they permanently embed the legal evidence associated with a signature into a signed document using public key infrastructure (PKI) technology.

It's essential to implement e-signature solutions incrementally.

PKI uses encryption to scramble and unscramble electronic bits of a document back into their original order by matching two large, random numbers, known as keys. One key is public, and it's stored in a public repository where any authorized person can access it, or in the signed document itself (as what's known as a 'digital certificate'). The other key is private, and the owners of these keys keep them secure so no one can reproduce or access them.

This is also how independent e-signatures are proven to be unique to each individual signer, and can be used to prove that a document has not been modified since signature.

Independent e-signatures also provide independent, comprehensive audit trails—another essential factor for maintaining long-term validity of e-signed documents. These digital records track the process by which a document was signed and contain metadata necessary for a signature to stand up in court and prevent a signer from saying, "I didn't sign that."

Like e-signatures, audit-trail technology can vary from vendor to vendor. These records should track each moment in the e-signature's history, such as the proof-of-user authentication, an acknowledgement of receiving the document, what documents were viewed by each signer, the agreement to use an electronic signature or a cancellation. And a good audit trail collects that information on every signature and every initial in the document, not just the last one.

Security strength

Given the exhaustive number of headlines concerning data breaches and data privacy, it's no surprise that security is a significant factor in determining appropriate e-signature services for mortgage lending. After all, many documents contain sensitive information that hackers prize, such as Social Security numbers, bank account information and other financial information. And even the most highly regulated industries have become victims of cyberattacks.

While e-signatures are not tools for preventing data breaches outright, the right technology strengthens digital security by making sure only authorized people have access to the content of documents and the ability to sign them, and immediately detecting potential foul play.

There are three essential security components that mortgage lending professionals should investigate when determining the right platform: authentication, tamper evidence and digital shredding.

Authentication

An e-signature is only as strong as its ability to authenticate signers. Most vendors offer several different identity authentication processes, but they can range in level of security. Some focus on user convenience and simplicity, and others are more stringent. Common methods are as follows, from least secure to most secure:

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

- ***Email verification:*** An email containing a verification link is sent to the signer. Once the link is clicked within an email platform, the signer is directed to his documents.
- ***Shared-secret questions:*** The signer must answer personal questions once she accesses the portal link via email. These questions are based on information known by the signer and by the submitter of the transaction (such as an account or identification number), or supplied by the signer to the submitter (such as a childhood pet's name). The shared questions are not widely known outside of the signer and the submitter.
- ***Text message verification:*** The signer is sent a one-time, random PIN code via a text message that he or she must enter in order to access documents.
- ***Know your customer (KYC):*** The signer is prompted to supply his or her Social Security number and date of birth before accessing documents. If the Social Security number is valid and matches with the date of birth, the user is verified.
- ***Knowledge-based authentication (KBA):*** KBA also requires the correct Social Security number and date of birth from signers. Once verified, the signer must then answer a number of multiple-choice questions. These questions are based on information found within 30 years of public data records, and all answers must match public records before the signer can proceed.

Authentication methods can go further still. Multifactor authentication requires a signer to pass at least two levels of identity verification—usually combining something you know (e.g., an email password or an account number) with something you have (e.g., a code sent to your phone via text message).

In the mortgage industry, as with others, authentication must be strong enough to reasonably prevent fraudsters from laying digital hands on sensitive documents. But it must also be simple enough for the lenders, borrowers and other parties to actually understand and use it.

Tamper evidence

For a signature to be legally sound, there can be no alterations to the document once it's been signed. Even an innocent mistake, such as correcting a typo, could call the enforceability of the entire loan into question. Or worse, document tampering could indicate a deliberate security breach that, if left uncorrected, could change the intended terms of the transaction or at least cause substantial confusion as to the deal terms. Tamper evidence is the remedy.

Tamper-evident technology takes a "snapshot" of the document after each individual signature. If at any time the document doesn't match the prior snapshot, the technology can alert signers of tampering in real time. While simple in practice, it's one of the most effective tools for ensuring a document's integrity.

Digital shredding

Mortgage papers are big-deal documents containing a lot of sensitive information, and that information shouldn't be in anyone's hands except those who absolutely need it. Digital shredding capabilities, which can only be done by independent e-signature vendors, allow mortgage professionals (and their clients) to control where signed documents reside and keep information in essential hands only.

With this process, vendors digitally shred their copies of signed documents, which also deletes all accompanying metadata. It is just as effective as paper shredding—if not more so—because no paper pieces remain. And neither the signature nor the

continued on next page

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

document's validity is compromised, because the independent e-signature vendor doesn't need to play a role in storing or proving legal evidence.

Documents can stay on a vendor's server, if desired. But when bank account information and Social Security numbers are present, digital shredding is an effective tool for mitigating cybersecurity risks.

Mortgage closings in the future

As mortgage professionals take the next step and begin to adopt e-signatures, it's important to seek out and use the technology that best meets your short- and long-term business objectives.

It's essential to implement e-signature solutions incrementally: Test a proposed solution for loan applications or loan commitments before implementing them for full loan closings. Start a pilot program with your most technologically sophisticated clients, rather than introducing a solution immediately across the board. Make sure that every proposed change has the features necessary so every party is comfortable with each step. Then, expand a successful solution to new areas.

Whether Forrester Research is right and we see e-signatures disrupting the industry by 2017, or whether it takes a bit longer, the mortgage e-closing of the future is getting closer. Who knows—for the next generation, wet ink and paper may be as antiquated as hot wax and stamps. MB

John Harris is chief technology officer at SIGNiX, a Chattanooga, Tennessee-based digital signature solutions provider that makes signing documents online safe, secure and legal for any business. **Kathy Zelenock** is a member of the Real Estate Group of Dickinson Wright PLLC, and is based in the firm's Troy, Michigan office. She represents national and regional lenders, mortgage bankers and loan servicers on a national basis for commercial and multifamily mortgage loans destined for Fannie Mae, Freddie Mac and other commercial mortgage-backed securitization (CMBS) executions, as well as for loans held for portfolio by the originating lender. They can be reached at jharris@signix.com and kzelenock@dickinsonwright.com.

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com