ELECTRONIC SIGNATURE REQUIREMENTS FOR LENDERS

June 2015

Purpose

The Electronic Signatures in Global and National Commerce (ESIGN) Act (15 U.S.C. §§7001-7006), enacted in 2000, permits, but does not require, the use of electronic signatures (e-signatures). ESIGN generally:

- Applies to all transactions if the consumer affirmatively consents to the use of electronic procedures unless the transaction is specifically excluded under the terms of the Act itself.
- Permits the use of an e-signature in any transaction if both parties consent to the usage.
- Dictates that any document in electronic form or executed with an e-signature is fully enforceable.
- Sets forth electronic record retention requirements.
- Provides that electronic records are fully admissible in any legal proceeding.

In addition, Kentucky has adopted the Uniform Electronic Transactions Act (UETA). The Federal Housing Administration (FHA), USDA's Rural Housing Service (RHS), U.S. Department of Veteran's Affairs (VA) and Fannie Mae allow electronic closings (e-closings). The purpose of this policy is to notify lenders of Kentucky Housing Corporation (KHC) requirements regarding e-signatures and e-closings.

Definitions

Attribution- The process of associating the identity of a signer with their signature.

Authentication- The process used to confirm a signer's identity as a party to the transaction.

Authoritative Copy- The Authoritative Copy of an electronically-signed document refers to the electronic record that is designated by the lender or the holder as the controlling reference copy.

Biometric Signature- The unique pattern of a physical feature such as a fingerprint, iris, or voice as recorded on a database for future attempts to determine or recognize a person's identity.

Click Wrap Agreement- A type of agreement used with software licenses and online transactions in which a user must agree to terms and conditions prior to using the product or service. Most require the consent of the end user by clicking an "OK," "I Accept," or "I Agree" button on a pop-up window or dialogue box.

Closing Disclosure- A form which must be provided to consumers three business days before they close on a loan, designed to provide disclosures that will be helpful to consumers in understanding all the costs of a transaction.

Digital Signature- Digital signatures are a subset of electronic signatures that utilize public key cryptography which, in turn, involves two related keys: a unique "private key" for the user, which encrypts the information, and a corresponding "public" key which unlocks the information and verifies the user's identity.

E-Closing - The act of closing a mortgage loan electronically. Some or all of the closing documents are accessed and executed via the web in a secure electronic environment.

Electronic Record- A contract or other record created, generated, sent, communicated, received, or stored by electronic means.

Electronic Signature- Any electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent to sign the record.

E-Signature- Electronic Signature.

E-Signer- A person who places an electronic signature on a document.

IVES (Income Verification Express Services) Electronic Service Requirements- A document that includes the requirements for the suggested framework that all IVES Participants must adhere to in order to use electronic signatures for IRS Form 4506-T.

Loan Estimate- A form, which must be provided to consumers within three business days after they submit a loan application, designed to provide disclosures that will be helpful to consumers in understanding the key features, costs, and risks of the mortgage for which they are applying.

Out-of-Band/Wallet Authentication- Out-of-Band Authentication means that a transaction that is initiated via one delivery channel (*e.g.,* Internet) must be re-authenticated or verified via an independent delivery channel (*e.g.,* telephone) in order for the transaction to be completed. Out-of-wallet Authentication relies on information that is not often publicly available and is difficult for imposters to identify.

Personal Identifiable Information (PII)- Any information that could potentially identify a specific individual.

Public Key Infrastructure (PKI) – the combination of software processes and services that enable an organization to secure its communications and business transactions. It is based upon the exchange of digital certificates between authenticated users and trusted resources.

Private Key- An encryption/decryption value known only to the parties who exchange information.

Public Key- A value provided by some designated authority as an encryption key that is known to everyone and, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.

RESPA – The Real Estate Settlement Procedures Act, which ensures that consumers are provided with helpful information about the cost of mortgage settlements and protected from unnecessarily high settlement charges.

Special Information Booklet- The booklet prepared by the U.S. Department of Housing and Urban Development pursuant to RESPA to help persons understand the nature and costs of settlement services.

Third-Party Documents - Documents that are originated and signed outside the control of the lender. An example of a third-party document is a sales contract.

TILA – The Truth in Lending Act, which provides uniform disclosures to make it easier for consumers to shop wisely for credit and helps ensure that consumers understand the financial risks associated with credit.

TRID Disclosures – The Loan Estimates, Closing Disclosures and Special Information Booklets required to be provided to consumers pursuant to TRID.

TRID Rule - The TILA-RESPA Integrated Disclosure (TRID) Rule, effective August 1, 2015. This rule requires lenders to provide consumers with a Loan Estimate, Closing Disclosure and Special Information Booklet. Under TRID, the initial Truth-in-Lending Disclosure and RESPA Good Faith Estimate are combined into the new Loan Estimate form and the final Truth-In-Lending Disclosure and RESPA HUD-1 are combined into the new Closing Disclosure.

Uniform Electronic Transactions Act (UETA)- A uniform act, the purpose of which is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures.

E-Signing and Electronic Delivery of TRID Disclosures

✓ KHC allows electronic delivery of TRID disclosures and accepts e-signatures on TRID disclosures.

If a lender chooses to allow applicants to confirm receipt of TRID disclosures via e-signature, the lender must ensure that the disclosures are delivered to the consumer with the option for electronic signatures. Lenders must provide consumers with notice of their rights, and this notice must include a statement that the applicant’s signature is about to be applied to, or associated with, the receipt confirmation.

However, prior to delivering TRID disclosures to consumers electronically, a consumer must affirmatively consent electronically to the use of electronic notices, in a manner that reasonably demonstrates that the consumer has Internet access, hardware and software suitable for the e-document receipt task, and the knowledge to use these things to receive, open, and use any documents Lender will send electronically.

One example of how the lender may accomplish this is by creating a test document in the format it will use throughout the course of the transaction and follow the steps outlined below.

- Create a PDF document which includes either a link or an instruction for the customer (e.g., "send an email to test@bank.net")
- Send sample document to customer
- Customer is able to open document
- Customer is able to follow instruction
- Lender receives response from customer
- Lender saves response as confirmation

Throughout the electronic signature process, lenders must comply with ESIGN; UETA; all HUD, USDA, VA and Fannie Mae requirements regarding e-signatures; the section entitled “Electronic Signature Performance Standards” in the FHA Single Family Housing Policy Handbook (Handbook 4000.1); all applicable state requirements; and the requirements of this document.

General Standards for E-Signatures

The use of e-signatures is voluntary, but lender transactions utilizing e-signatures **must** meet the following standards:

□ For borrowers that are entities, the signatory must be a representative who is duly authorized in writing to bind the entity;
□ Evidence of such written authority must be maintained by Lender;
□ Lenders are not permitted to have borrowers sign documents in blank or with incomplete documents;
□ E-signatures and the accompanying dates must be clearly visible on any and all e-signed documents; and
□ E-signatures are not permitted on promissory notes, mortgages, documents that require notarization or witnesses, or transactions utilizing a power of attorney.

KHC **does not accept** documents that have been signed solely via voice or audio. The electronic signature and date should be clearly visible on any and all documents when viewed electronically and on a paper copy of an e-signed third-party document.

Often certain key documents (such as the note and security instrument) are printed on paper and wet-signed while other documents throughout the process are signed electronically. An e-closing only produces an e-mortgage or e-note if the promissory note is signed electronically. KHC allows e-closings, but **does not accept** e-notes or e-mortgages. Promissory notes and mortgages must be wet-signed.

Additionally, when utilizing e-signatures lenders **must** ensure that the following ESIGN requirements are implemented:

□ The signature must be under the sole control of the signatory. Password-based signatures should be used in conjunction with PKI, signature stamps, and electronic seals as well as simple click wrap agreements.

□ The signature must be verifiable. E-signature technology will verify in real time using complex algorithms or thorough forensic analysis of the signature dynamics or measurements.

□ Each signature gathered must be unique to an individual regardless of whether it is a physical measurement like a fingerprint or a virtual measurement like the click of a mouse.

□ The signature must establish the individual’s intent to be bound to the transaction (*e.g.,* the signatory must be fully aware of the purpose for which the signature is being provided, regardless of underlying technology).

□ The signature must be provided in a tamper-evident manner. Industry standard encryption must be used to protect the users’ signatures and the integrity of the documents to which they are affixed.

Confidentiality Requirements

Lenders shall not divulge personal identifiable information (PII), and all documents transmitted electronically shall be in compliance with:

- Title VII of the Civil Rights Act;
- The Fair Credit Reporting Act (FCRA);
- The Right to Privacy Act;
- The Gramm-Leach-Bliley Act (GLBA);
- The Equal Credit Opportunity Act (ECOA);
- The Financial Privacy Act;
- All other federal and Kentucky statutes and regulations requiring confidentiality of PII; and
- All KHC policies requiring confidentiality of PII.

Associating Signature with Document

All documents must be presented to the signatory before an e-signature is obtained. Lenders must ensure that the e-signature is attached to, or logically associated with, the document that has been e-signed.

Intent to Sign

The lender must be able to prove that the e-signer certified that the document is true, accurate, and correct at the time it is signed. E-signatures are only valid under the ESIGN Act if they are "executed or adopted by a person with the intent to sign the record."

*Lenders **must** establish intent by:*

1. Identifying the purpose for the borrower signing the electronic record;
2. Being reasonably certain that the borrower knows which record is being signed; and
3. Providing notice to the borrower that his/her e-signature is about to be applied to, or associated with, the electronic record.

This intent may be demonstrated by, but is not limited to, one of the following methods:

- An online dialogue box or alert advising the borrower that continuing the process will result in an electronic signature;
- An online dialogue box or alert indicating that an e-signature has just been created and giving the borrower an option to confirm or cancel the signature; or
- A click-through agreement advising the borrower that continuing the process will result in an e-signature.

Single Use of Signatures

Lenders must require a separate action by the signer, evidencing intent to sign, in each location where a signature or initials are to be applied. This requirement does not apply to lender employees or contractors provided the lender obtains the consent of the individual for the use of their e-signature. Lenders must document this consent.

Authentication

Lenders must validate that the signer is who they say they are and that the document(s) are delivered to the intended recipient.

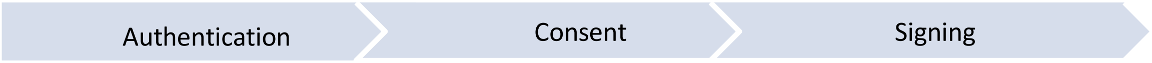
Lenders must verify the signer's name and date of birth, and either their Social Security Number or driver's license number and make this information available to KHC.

*Lenders **must** identify each signer by authenticating data provided by the signer with information maintained by an independent source, including, but not limited to:*

- National commercial credit bureaus;
- Commercially available data sources or services;
- State motor vehicle agencies; or
- Government databases.

Consent

The lender must obtain the advance, written consent of the borrower to receive and sign documents electronically. This is typically done after authentication and prior to signing.



Attribution

Lenders must use one of the following methods, or combinations of methods, to establish attribution:

- Selection by, or assignment to, the individual of a Personal Identification Number (PIN), password, or other shared secret that the individual uses as part of the signature process;
- Delivery of a credential to the individual by a trusted third party, used either to sign electronically or to prevent undetected alteration after the electronic signature using another method;
- Knowledge-based “out-of-band/wallet” authentication;
- Measurement of some unique biometric of the individual and creation of a computer file that represents the measurement which, together with procedure, will protect against disclosure of the associated computer file to unauthorized parties; or
- Public key cryptography.

Credential Loss Management

Lenders must have a system in place to ensure the security of all issued credentials. One or a combination of the following loss management controls is acceptable:

- Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password;
- Ensuring that identification code and password issuances are periodically checked, recalled or revised;
- Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise compromised identification code or password information, and issuing temporary or permanent replacements using suitable, rigorous controls;
- Using transaction safeguards to prevent unauthorized use of passwords or identification codes; or
- Detecting and reporting any attempts at unauthorized use of the password or identification code to the system security unit.

Required Documentation and Integrity of Records

Lenders must ensure:

- ✓ to employ industry-standard encryption to protect the signer’s signature and the integrity of the documents to which it is affixed; and
- ✓ that their systems will detect and record any tampering with the electronically-signed documents.

If changes to the document are made, the electronic process must be designed to provide an “audit trail” showing all alterations, the time and date they were made, and the identity of the person who made them.

Lenders’ systems must be designed so that the signed document is designated as the Authoritative Copy.

Quality Control

Lenders must update their quality control plans to ensure they meet all requirements and perform adequate oversight of the electronic signature process.

Audits

Lenders must use an independent party to audit and ensure that each e-signature meets all the requirements of this document. Lenders shall provide this audit, along with its findings, to KHC on an annual basis, *no later than January 31st of the following year*. Lenders with findings indicating a failure to meet all requirements will not be allowed to continue using e-signatures.

Lenders must maintain an audit log of the entire e-signing ceremony for the purpose of future non-repudiation. The log should contain the following data:

- Date and time of each e-signature;
- IP address of each signer;
- Notifications;
- Result of authentication;
- Result of consent; and
- Each e-signature in the document.