Electronic Signature Requirements

This document includes the requirements for the suggested framework to which all eCBSV participants must adhere to participate using electronic signatures on consent forms related to eCBSV, including the form SSA-89.

Background

Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (sec. 215) was passed in order to help curb synthetic identity fraud. Section 215 directs the Social Security Administration (SSA) to allow certain financial institutions and other entities servicing the financial institutions, called permitted entities, to receive the consent of an individual by electronic signature allowing SSA to disclose that individual’s Social Security number (SSN) verification to the permitted entity. Prior to the passing of section 215, SSA required these financial institutions seeking to verify SSNs to accept consents from individuals with wet signatures, only.

E-SIGN Requirements

The Electronic Signatures in Global and National Commerce Act, commonly referred to as E-SIGN (15 U.S.C. 7006) provides uniform standards for the use of electronic signatures, which have grown in use over the last few years.

An “electronic signature” is defined in section 1106 of E-SIGN as “an 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.”

A valid and enforceable electronic signature must satisfy the following requirements, which we propose to implement:

1. The signature must be executed or adopted by a person with the intent to sign;
2. The signature must be attached to or associated with the electronic record being signed;
3. The signature or signature process must provide a means to identify and authenticate a particular person as the signer;
4. The signature or signature process must include a means to preserve the integrity of the signed record;
5. The signature or signature process must provide a means for non-repudiation; and
6. The signature must be an acceptable electronic form of signature.

E-SIGN does not require specific technology to implement the six requirements, therefore, SSA is not requiring permitted entities implement specific technology to accept electronically signed consent from consumers for purposes of SSN verifications. Permitted entities have the option of using electronic signatures for an electronic version of Form SSA-89 or within their already-existing business workflow if their e-banking software or application(s) provides the capability, the consumer consents to using electronic signatures, and meets the requirements defined below, consistent with E-SIGN.

Consistent with E-SIGN, Permitted entities must get separate consent from the individual signing the SSA consent form before allowing the individual to sign SSA’s consent form electronically.
Electronic Signature Framework for eCBSV Participants

Prior to the acceptance of electronically signed consent, eCBSV participants must ensure they have implemented the requirements set forth in the following electronic signature framework.

Intent to Sign

Permitted entities must ensure that the electronic signature be executed or adopted by the signer with the intent to sign the associated record. Clear evidence of intent to sign must be included and demonstrated either in the record being signed or in the on-screen signing process so that it is clear to the signer that he/she is signing the record. Examples of intent to sign methods deemed appropriate include:

- Clicking a clearly labeled “Accept” button (i.e., “By [clicking the [SIGN/OK/I AGREE/I ACCEPT] button], you are signing the document electronically. You agree that your electronic signature has the same legal validity and effect as your handwritten signature on the document, and that it has the same meaning as your handwritten signature.”; or
- Allowing the signer to opt out of electronically signing the record by providing an option to decline).

Shorter, more cursory indicators of intent to sign are not permissible.

Association of Signature to Record

The electronic form of signature must be attached to or logically associated with the record being signed, and where applicable have the capability to be printed or downloaded by the parties involved. Specifically, the electronic signature must be attached to, or logically associated with the record being signed either by a process that appends the signature data to the record being signed or by a database-type link between the signature data and the record. Regardless of the approach selected, the electronic signature must be associated with the electronic record in a manner that allows for the establishment that a specific person applied a particular electronic signature to a specific electronic record, at a specific time, and with intent to sign the electronic record.

Identification and Authentication of Signer

E-SIGN and rules of evidence generally require the electronic signature method chosen identify and authenticate “a person” signing the document.

The electronic signature must be associated with a person. Therefore, ensuring the validity of any electronically signed record requires identification and authentication of the signer. The specific data object that constitutes the electronic signature or the overall method of signing must be able to generate evidence of the person the electronic form of signature belongs to, as well as generate evidence that the identified person is actually associated with the electronic record.

The purpose of section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act is to reduce the prevalence of “synthetic identity fraud,” the verification response provided by SSA should not be used as the sole basis of identity proofing and/or authenticating the signer. Instead, permitted entities must compliment the SSN verification response provided by SSA with existing identity proofing and authentication controls, such as those required by existing laws and guidance, which include but are not limited to the:
• Federal Financial Institutions Examination Council (FFIEC) guidance on Electronic Authentication and Authenticating E-Banking Customers;
• FFIEC BSA/AML Manual – Regulatory Requirements – Customer Identification Program; and
• The USA Patriot Act, see 31 CFR 1020.220.

Such guidance requires institutions, as a part of their customer identification program, to include risk-based procedures describing how the institution will verify the identity of the customer using documents, non-documentary methods, or a combination of both.

**Integrity of Signed Record**

After the electronic consent has been signed, it must be tamper-proof. Therefore, permitted entities must implement techniques that lock the consent and corresponding signature to prevent it from being modified. Storage systems must have secure access control to ensure that any party cannot modify the electronic consent after it was signed.

Additionally, storage systems must also contain a retrieval system that includes an indexing system, and the ability to reproduce legible and readable hardcopies of electronically stored records for auditing and monitoring purposes under section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act.

Permitted entities must adhere to the standards referenced in the FFIEC Security Guidelines and other applicable frameworks to ensure they maintain signed consent in a tamper-proof manner that can be retrieved and reproduced for purposes of satisfying auditing and monitoring requirements under section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act.

**Non-repudiation**

Regardless of the form of the electronic signature, permitted entities must maintain an audit log, which captures and retains the following for each signature for a period of five (5) years:

• Digital image of the signed form or equivalent (i.e., yes/no binary response);
• Date and time of the signature;
• Signer’s Internet Protocol address (remote transactions only);
• Results from consumer identity verification and authentication process; and
• Method used to sign the record, system log, or other audit trail that reflects the completion of the electronic signature process by the signer.

**Acceptable Forms of Electronic Signature Methods Deemed Appropriate by SSA, Consistent with ESIGN**

The following are examples of electronic signature methods that permitted entities may use when accepting consents from individuals, if implemented in a way that meets the framework described above:

• A typed name (i.e., typed into a signature block on a website form)
• A digitized image of a handwritten signature that is attached to an electronic record
• A shared secret (i.e., password or PIN) used by a person to sign the electronic record
• A sound recording of a person’s voice expressing consent
• Clicking or checking an on-screen button (i.e., clicking or checking an “I Agree” or “I Consent” button)

Other reasonable and comparable methods are also appropriate so long as it is clear to the signer that he/she is signing the record.