## IV. Consent

### A. Forms of Valid Written Consent

1. The Permitted Entity or any Financial Institution being serviced by the Permitted Entity, if any, must obtain from each SSN holder a valid Written Consent that meets SSA's requirements as set forth in this user agreement and SSA's regulations. A valid Written Consent includes one of the three following forms of consent:

    a. SSA-89 (standardized consent form titled Authorization for SSA to Release SSN Verification), with the SSN holder's wet signature. See Exhibit B; or

    b. SSA-89, in a "pdf fillable" form, signed electronically by the SSN holder, with an Electronic Signature that meets the requirements set forth in section IV.E; or

    c. One of the two consent template options provided in Exhibit C, SSA Written Consent Template, that is incorporated into the Permitted Entity's or Financial Institution's existing electronic or paper-based business process. As shown in Exhibit C, SSA Written Consent Template, the title of SSA's Written Consent must be in "bold" font followed directly by the SSA-provided language. See SSA's Written Consent Template, attached and incorporated into this user agreement as Exhibit C.
        i. In addition to any requirements in this user agreement, consent incorporated into a Permitted Entity's or Financial Institution's electronic business process must use SSA's Written Consent Template, and the consent must be associated with the SSN holder's name, date of birth, SSN, the purpose for the transaction, and must be signed with an electronic signature that meets the requirements in section IV.E.
        ii. In addition to any requirements in this user agreement, consent incorporated into a Permitted Entity's or Financial Institution's paper-based business process must use SSA's Written Consent Template, and the consent must contain the SSN holder's name, date of birth, SSN, the purpose for the transaction, and must include the SSN holder's wet signature.

2. The Permitted Entity or Financial Institution must maintain documentation of the specific purpose in accordance with sections III, IV, and VIII of the user agreement.

3. SSA will process the request as a one-time-only disclosure using the same Written Consent.

4. If SSA's eCBSV system is experiencing technical difficulties, the Permitted Entity or Financial Institution may re-submit the SSN Verification to eCBSV using the same Written Consent until it receives a successful response.

5. The Permitted Entity or any Financial Institution being serviced by a Permitted Entity who obtains the Written Consent must return any Written Consent that does not meet these requirements to the SSN holder with an explanation of why the Written Consent is deficient.

6. The Permitted Entity or Financial Institution, if any, may not alter the Written Consent either before or after the SSN holder completes the Written Consent. If the SSN holder later changes the period during which the Written Consent is valid, the Permitted Entity may not rely upon the Written Consent to request an SSN Verification unless the SSN holder annotated and initialed this change in the space provided on the Written Consent, including by a new Electronic Signature meeting all requirements set forth in section IV.E.

7. The Permitted Entity may not rely upon the Written Consent to submit an SSN Verification request unless the request for SSN Verification is submitted to SSA within either the time specified on the Written Consent, or within 90 calendar days from the date the SSN holder signs the Written Consent.

**B. Retention**

The Permitted Entity or Financial Institution it services, if any, that creates, receives, or has access to Supporting Documentation must retain the Supporting Documentation for a period of five (5) years from the date of the SSN Verification request, either electronically or in paper form. The Permitted Entity obtaining or having access to the Written Consent must protect the confidentiality of each completed Written Consent and the information therein, as well as the associated record of SSN Verification. The Permitted Entity or Financial Institution, if any, with access to the Written Consent, evidence documenting specific purpose, or SSN Verification must also protect those records from loss or destruction by taking the measures below. (See section V.B for procedures on reporting loss of SSN Verifications or Written Consents). The Permitted Entity or Financial Institution it services shall restrict access to the Written Consent and SSN Verification to the minimum number of employees and officials who need it to perform the process associated with this user agreement. In accordance with section III.A.20, the stored Written Consent and SSN Verification must not be reused.

If the Permitted Entity or Financial Institution obtaining the Written Consent in paper format and chooses to retain the Written Consent in paper format, that entity must store the Written Consent in a manner that meets all regulatory requirements

If the Permitted Entity or Financial Institution obtains Written Consents electronically, or chooses to convert original paper copies of Written Consents to electronic versions, the Permitted Entity and any Financial Institutions it services, if any, must retain the Written Consents in a way that accounts for integrity of the Written Consents and: (1) password protect any electronic files used for storage; (2) restrict access to the files to the only necessary personnel; and (3) put in place and follow adequate disaster recovery procedures. SSN Verifications must also be protected in this manner.

When storing a Written Consent electronically, the Permitted Entity must destroy any original Written Consent in paper form.

**C. Onsite and other Reviews**

SSA may make onsite inspections of the Permitted Entity's or Financial Institution's site, including a systems review limited to eCBSV-related systems, to ensure that the Permitted Entity or Financial Institution has taken the above-required precautions in sections III A and IV B to protect the Written Consent, including evidence documenting purpose if records include the SSN Verification and Written Consent, and the SSN Verification and to assess eCBSV-related system security.

SSA may make periodic, random reviews of the Written Consents to confirm that the SSN holder properly completed the Written Consent.

**D. Requests from SSN holder's Parents or Legal Guardians**

The Permitted Entity can submit SSN Verification requests based on a Written Consent signed electronically by the legal guardians of adults, and parents or legal guardians of children under age 18 when two criteria are met: The parent or legal guardian has signed a Written Consent and the parent or legal guardian has submitted documentation to the Permitted Entity that proves the relationship. If the request is for a minor child (under age 18), a parent or legal guardian must sign the Written Consent and provide a birth certificate or court documentation proving the relationship. If the request is for a legally incompetent adult, a legal guardian must sign the Written Consent and provide court documentation proving the relationship.

The Permitted Entity may accept Written Consent signed by a third party with power of attorney only if the SSN holder signs the papers granting the power of attorney and those papers state exactly what information SSA can disclose to the Permitted Entity.
A third party without a power of attorney or with a power of attorney that does not meet the criteria described in this section (e.g., a spouse, an appointed representative, an attorney) is not authorized to execute Written Consent on the SSN holder's behalf.

The Permitted Entity shall retain proof of the relationship, e.g., a copy of the birth certificate or court documentation proving the relationship. The evidence of the relationship should be stored in such a manner that an auditor could ascertain whether the Permitted Entity had both the Written Consent and evidence of the relationship before requesting SSN Verification from SSA.

**E. Electronic Signature Requirements**

The Permitted Entity or the Financial Institution(s) it services that obtains the Written Consent from the SSN holder, if any, will obtain from the SSN holder an Electronic Signature, consistent with section 106 of the E-SIGN Act (15 U.S.C. § 7006). Section 106 of the E-SIGN Act defines an electronic signature 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."

Consistent with E-SIGN, SSA does not require the Permitted Entity to use specific technology to implement an electronic signature on a Written Consent, so long as the Electronic Signature meets the definition of and all applicable requirements set forth by section 106 of E-SIGN, as identified below.

1. The Permitted Entity must use a form of electronic signature consistent with E-SIGN.

   Permitted Entities obtaining the Written Consent must use a form of electronic signature consistent with E-SIGN (i.e., an electronic sound, symbol, or process). The following are non-exclusive examples of forms of Electronic Signature that are consistent with E-SIGN. The Permitted Entity obtaining the Written Consent may incorporate other comparable forms of electronic signature so long as they are otherwise in compliance with section 106 of E-SIGN.
   i. A typed name (i.e., typed into a signature block on a website form)
   ii. A digitized image of a handwritten signature that is attached to an electronic record
   iii. A shared secret (i.e., password or PIN) used by a person to sign the electronic record
   iv. A sound recording of a person's voice expressing consent
   v. Clicking or checking an on-screen button (i.e., clicking or checking an "I Agree" or "I Consent" button)

1. The Electronic Signature must be executed or adopted by a person with the intent to sign.

   It must be clear to the SSN Holder, either in the Written Consent or elsewhere in the signing process, that he or she is signing SSA's Written Consent. Examples of intent to sign methods deemed appropriate include, but are not limited to:
   i. Clicking a clearly labeled "Accept" button (e.g., "By [clicking the [SIGN/ I AGREE/I ACCEPT] button], you are signing the consent for SSA to disclose your SSN Verification to [Permitted Entity and/or Financial Institution]. You agree that your electronic signature has the same legal meaning, validity, and effect as your handwritten signature."); or
   ii. Allowing the signer to opt out of electronically signing the record by providing an option to decline).

2. The Electronic Signature must be attached to or associated with the Written Consent being signed.

   The Electronic Signature must be attached to or logically associated with the Written Consent being signed, and where applicable, have the capability for an accurate and unaltered version to be retained by the parties involved. Examples of acceptable

forms of associating the electronic signature to the record include, but are not limited to:

i. a process that permanently appends the signature data to the consent being signed; or
ii. a database-type link between the signature data and the consent.

Regardless of the approach selected, the Permitted Entity obtaining the Written Consent must ensure that the Electronic Signature be associated with the Written Consent 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 (signature data).

In addition to the requirements above set forth by section 106 of E-SIGN, the Permitted Entity obtaining or retaining the Written Consent must ensure there is a means to preserve the integrity of the electronic signature by retaining and implementing safeguards to prevent it from being modified or altered in accordance with the requirements set forth in section IV.B.

Regardless of the method the Permitted Entity uses to preserve the integrity of the Electronic Signature and Written Consent, there must be a means to retrieve and reproduce legible, accurate, and readable hard or electronic copies of the Written Consent reflecting all Electronic Signature requirements in this section for auditing and monitoring purposes under the Banking Bill and the Privacy Act of 1974, as amended. See section VIII for audit requirements.