

### **III. Responsibilities**

#### **A. Permitted Entity Responsibilities**

Failure to follow the requirements listed below may result in suspension or termination of the eCBSV service.

1. If the Permitted Entity is operating as a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution, the Permitted Entity will ensure that each Financial Institution it services abides by all terms, conditions, and requirements of this user agreement through a contractual relationship or other express written agreement.
2. The Permitted Entity acknowledges that a requirement to register for using the eCBSV system and signing this user agreement, is to provide to SSA a consent for SSA to access its Employer Identification Number (EIN). The Permitted Entity agrees to notify SSA if its EIN has changed since signing this user agreement.
3. Pursuant to the certification requirement in the Banking Bill, the Permitted Entity must submit a Permitted Entity Certification at the outset of this user agreement and at least every two (2) years thereafter by using the template attached to the user agreement as Exhibit A. Permitted Entities cannot deviate from the language provided in Exhibit A. The Permitted Entity must complete its own Permitted Entity Certification. If the Permitted Entity services a Financial Institution pursuant to a separate agreement as required under section III.A.1, the Permitted Entity acknowledges that each Financial Institution must provide to SSA a Permitted Entity Certification before SSA will provide SSN Verifications to the Financial Institution.
4. The Permitted Entity must submit written notification to SSA of any name change 30 calendar days before submitting any requests for SSN Verifications under the new name. This change may result in a disruption of the eCBSV service.
5. If the Permitted Entity wants SSA to recognize the Permitted Entity's successor in interest to this user agreement, it must submit written notification to SSA 30 calendar days before submitting any requests for SSN Verifications as the successor in interest. The Permitted Entity also shall submit a new Permitted Entity Certification and, because this user agreement is not assignable, must enter into a new user agreement with SSA. This change may result in a disruption of the eCBSV service.
6. The Permitted Entity must submit requests for SSN Verifications either in one or more individual requests electronically for real-time machine to machine or similar functionality for accurate electronic responses within a reasonable period of time from submission, or in batch format for accurate electronic responses within 24 hours. All SSN Verification requests must conform to the Banking Bill and specify the full name (including first name and any family or forename or surname), date of birth (including the month, day, and year), and SSN of each SSN holder whose SSN the

Permitted Entity seeks to verify. For SSA's eCBSV Technical Requirements, see SSA's internet website at: <https://www.ssa.gov/dataexchange/eCBSV/>.

7. The Permitted Entity must submit SSN Verification requests to the eCBSV system only: (1) pursuant to the Written Consent, including electronic, received from the SSN holder; and (2) in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act (15 U.S.C. § 1681b).
8. If a Permitted Entity has SSN Verification requests that do not meet the requirements of the Banking Bill, including but not limited to services it provides other entities that do not meet the definition of a Financial Institution, or such requests are for a purpose outside of the Banking Bill, the Permitted Entity must not submit such SSN Verification requests to the eCBSV system.
9. When the Written Consent includes reference to
  - a. a static or general purpose (see Exhibit C, Option 1), the Permitted Entity or Financial Institution must:
    - i. Maintain evidence that documents the specific purpose of the SSN Verification request;
    - ii. Maintain the evidence required by paragraph III.A.9.a., above, in a way that clearly links the specific purpose of the transaction to the relevant Written Consent; and
    - iii. Maintain the evidence required by paragraph III.A.9.a., above, for a period of five years from the date of the SSN Verification request that preserves the accuracy and integrity of the records, and that is accessible to SSA and SSA's auditors.
  - b. a specific purpose (see Exhibit C, Option 2), the Permitted Entity or Financial Institution is not required to maintain the records specified in paragraph III.A.9.a.i., above, as maintaining Exhibit C, Option 2 for the requisite period will suffice.
10. SSA may change its method of receiving SSN Verification requests and providing SSN Verification results to the Permitted Entity at any time; however, SSA will provide as much notice as is possible to the Permitted Entity. If SSA decides to change its method of receiving SSN Verification requests or providing SSN Verification results, the Permitted Entity will bear its own costs incurred to accommodate such changes.
11. To use a Written Consent received electronically, the Permitted Entity, or each Financial Institution that obtains the Written Consent and is being serviced by a Permitted Entity, must obtain the SSN Holder's electronic signature, as defined in section 106 of the Electronic Signatures in Global and National Commerce Act (15

U.S.C. § 7006), and meet the requirements in the Banking Bill and in this user agreement, including section IV.E, below.

12. The Permitted Entity must not alter the Written Consent either before or after the SSN holder signs 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 from SSA unless the SSN holder annotated and initialed this change in the space provided on the Written Consent, including by a new Electronic Signature meeting requirements set forth in section IV.E. Alterations do not include fax date/time stamps, barcodes, quick response codes or tracking/loan numbers added to the margin of a form.
13. The Permitted Entity must not rely upon the Written Consent to request an SSN Verification unless the SSN Verification request is submitted within the time specified on the Written Consent, either 90 calendar days from the date the SSN holder signs the Written Consent, or by an alternate date established on the Written Consent.
14. The Permitted Entity will be responsible for all SSN Verification requests made through its real-time client application and for complying with the requirement to maintain an audit trail to track its eCBSV activities. If operating as a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution, the Permitted Entity will track incoming requests it receives from each Financial Institution, and ensure that each Financial Institution tracks its own activities associated with obtaining Written Consent and initiating requests with the Permitted Entity.
15. The Permitted Entity will inform all of its Authorized Users, and if it services a Financial Institution, will ensure the Financial Institution informs all employees with access to the SSN Verification or Written Consent of the confidential nature of the SSN Verification and Written Consent and the administrative, technical, and physical safeguards required to protect the SSN Verification and Written Consent from improper disclosure. Whichever entity obtains the Written Consent from the SSN holder and receives or otherwise has access to the SSN Verification will store the information in an area that is physically safe (i.e., password protected hard drive, USB drive or disk) from unauthorized access at all times.
16. The Permitted Entity, and Financial Institution(s) it services, if any, acknowledges that SSA's SSN Verification verifies that the Fraud Protection Data provided by the Permitted Entity matches or does not match the data in SSA records. SSA's SSN Verification does not authenticate the identity of the SSN holder or conclusively prove that the SSN holder is who he or she claims to be.
17. The Permitted Entity must not submit an SSN Verification request to SSA before the Permitted Entity (or a Financial Institution) receives the requisite Written Consent, which has been properly completed by the SSN holder. Any Permitted Entity that submits an SSN Verification request to SSA without a properly completed Written

Consent is subject to legal penalties and could lead to termination of this user agreement.

18. The Permitted Entity, if it is a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution must notify SSA of each Financial Institution it represents prior to submitting an SSN Verification request on behalf of that Financial Institution.
19. With respect to advertising, the Permitted Entity, and any Financial Institution it services, if any, acknowledges and agrees to the following:
  - a. Section 1140 of the Social Security Act authorizes SSA to impose civil monetary penalties on any person who uses the words “Social Security” or other program-related words, acronyms, emblems, and symbols in connection with an advertisement, solicitation, or other communication, “in a manner which such person knows or should know would convey, or in a manner which reasonably could be interpreted or construed as conveying, the false impression that such item is approved, endorsed, or authorized by the Social Security Administration . . . .” 42 U.S.C. § 1320b-10(a).
  - b. The Permitted Entity, and in the case of a Permitted Entity servicing a Financial Institution(s), the Financial Institution, is specifically prohibited from using the words “Social Security” or other eCBSV program-related words, acronyms, emblems, and symbols in connection with an advertisement for “identity verification.”
  - c. The Permitted Entity, and in the case of a Permitted Entity servicing a Financial Institution, the Financial Institution, is specifically prohibited from advertising that an SSN Verification provides or serves as identity verification.
  - d. The Permitted Entity, and in the case of a Permitted Entity servicing a Financial Institution, the Financial Institution, cannot advertise that eCBSV will eliminate synthetic identity fraud or any type of fraud.
  - e. The Permitted Entity cannot advertise in any way that it maintains a repository of data verified by SSA, including advertising to prospective or current clients, Financial Institutions, consumers, or otherwise to the public. The Permitted Entity must not represent that any verifications it provides based on its own marked records are SSA-verified data or SSN Verifications. The Permitted Entity must represent that such verifications are verifications from its own records and information, and the Permitted Entity bears full responsibility for the accuracy of its verification representations. This requirement remains after the termination of this user agreement and applies to any successor of interest to the Permitted Entity.
20. The Permitted Entity must bear all costs it incurs for site preparation, connection, system testing (including External Testing as described in the Technical User Guide,

which can be found on SSA's internet website at: [https://www.ssa.gov/dataexchange/eCBSV/technical\\_information.html](https://www.ssa.gov/dataexchange/eCBSV/technical_information.html)), operating costs, and any other miscellaneous costs to participate in eCBSV. The Permitted Entity acknowledges that SSA reserves the right to conduct on-site visits to review the Permitted Entity's and each of its Financial Institution's, if any, documentation and in-house procedures for protection of and security arrangements for the SSN Verification and Written Consent and adherence to terms of this user agreement

21. The Permitted Entity and any Financial Institution(s) it services must not reuse the SSN Verification. The Permitted Entity and any Financial Institution(s) it services may mark their own records as "verified" or "unverified."
22. Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures that: 1) ensure the security and confidentiality of the SSN Verifications, and 2) ensure SSN Verifications that are maintained in a Managed Service Provider or Cloud Service Provider are encrypted at rest and in transit, and 3) assess the sufficiency of these policies and procedures on an ongoing basis. The Permitted Entity must not provide the Managed Service Provider or Cloud Service Provider the key to unencrypt the SSN Verification maintained in their environment. The Permitted Entity must also ensure that the SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands).