OMB No. 0960-0817

User Agreement

Between

the Social Security Administration (SSA)

And

{Insert Permitted Entity's Name}

For the electronic Consent Based Social Security Number (SSN) Verification (eCBSV) Service

I. Purpose and Definitions

A. Purpose

The purpose of this user agreement is to establish the conditions, terms, and safeguards under which SSA will provide the Permitted Entity with verifications of Fraud Protection Data.

B. Definitions

Authorized User – Employee of the Permitted Entity who has been authorized by the Permitted Entity to submit SSN Verification requests and has successfully registered through the Permitted Entity to use the eCBSV system.

Banking Bill - Section 215 titled, "Reducing Identity Fraud," of the "Economic Growth, Regulatory Relief, and Consumer Protection Act," (Pub. L. No. 115-174), as amended.

Client or SSN holder – Individual who authorizes SSA to verify his or her SSN to the Permitted Entity or Financial Institution by providing Written Consent.

Cloud Service Provider - A third-party company offering a cloud-based infrastructure or storage services.

Electronic Signature – 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, as defined in section 106 of the Electronic Signatures in Global and National Commerce (E-SIGN) Act.

Financial Institution – Has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (GLBA). A Financial Institution is a permitted entity under the Banking Bill and can be either (1) the original requesting source for the SSN Verification and is signing this user agreement as the Permitted Entity; or (2) enters into a contractual relationship or other express written agreement with a Permitted Entity, who is a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of the Financial Institution to obtain SSN Verifications from SSA. References to a Financial Institution throughout this user agreement means a Financial Institution that is seeking an SSN Verification from SSA through a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of the Financial Institution.

Fraud Protection Data – As defined by the Banking Bill, a combination of the SSN holder's name (including the first name and any family forename or surname of the individual), SSN, and date of birth including the month, day, and year.

Managed Service Provider - Delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their Managed Service Provider's data center (hosting), or in a third-party data center.

Permitted Entity – A Financial Institution as defined by section 509 of GLBA and as defined in this section, or a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution, who is signing this user agreement as a Permitted Entity.

Permitted Entity Certification – Certification provided to SSA at least every 2 years by the Permitted Entity and each Financial Institution, if applicable, as required by the Banking Bill. The Permitted Entity Certification must meet the requirements under section III.A.3 of this user agreement and in Exhibit A.

SSN Verification –The response SSA discloses to the Permitted Entity or Financial Institution after conducting a comparison of the SSN holder's Fraud Protection Data with the information recorded in SSA's records. SSA will disclose a verification result as a ***"yes" or "no"*** match response, including explanatory information identifying the data element(s) that does not match the information in SSA's records. The SSN verification result will also include an indication of death, if such data is present in SSA records.

Supporting Documentation – All records or information necessary for SSA to conduct audits as required in section VIII of the user agreement. Supporting Documentation may include: all completed and signed Written Consents; evidence documenting the specific purpose for each Written Consent, if not referenced within the individual Written Consent; SSN Verifications; and audit logs or audit trails if required in accordance with sections III.A.14 and IV.E of the user agreement. Supporting Documentation must be maintained in an accessible electronic format, when available. If not available, paper documentation will suffice.

Written Consent – Written Consent, including electronic, by which the SSN holder gives SSA permission to disclose SSN Verification results to the Permitted Entity or Financial Institution (or both) in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act (15 U.S.C. § 1681b). The Written Consent must meet SSA's requirements in section IV of this user agreement and SSA's regulations. The Written Consent must clearly specify to whom the information may be disclosed (the Permitted Entity and Financial Institution, if different), that the SSN holder wants SSA to disclose the SSN Verification, and, where applicable, during which timeframe the SSN Verification may be disclosed (see 20 C.F.R. § 401.100). Written Consent must identify the purpose for which the SSN holder gives SSA permission to disclose SSN Verification results. Written Consent must be provided by the SSN holder in one of three ways described in section IV of the user agreement. *See* Exhibit B, Form SSA-89 (Authorization for SSA to Release SSN Verification) and Exhibit C, SSA's Written Consent Template.

C. Legal Authority

Legal authority for SSA disclosing SSN Verifications to the Permitted Entity or Financial Institution is the SSN holder's written, including electronic, consent as authorized by the Privacy Act at 5 U.S.C. § 552a(b), section 1106 of the Social Security Act, codified at 42 U.S.C. § 1306, and SSA regulation at 20 C.F.R. § 401.100, and the Banking Bill.

II. SSN Verification Does Not Provide Proof or Confirmation of Identity

SSA's SSN Verification does not provide proof or confirmation of identity. ***eCBSV is designed to provide a permitted entity with only a "yes" or "no" verification of whether the SSN verified with SSA's records and explanatory information in the case of a "no" match response that identifies the data element(s) that does not match the information in SSA's records. If SSA's records show that the SSN holder is deceased, eCBSV returns a death indicator. SSN Verifications do not verify an individual's identity. eCBSV does not verify employment eligibility, nor does it interface with the Department of Homeland Security's (DHS) verification system, and it will not satisfy DHS's I-9 requirements.***

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 Act1 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), 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 for a purpose not authorized by the Written Consent. The Permitted Entity and any Financial Institution(s) it services may mark their own records as "verified" or "unverified." The Permitted Entity and any Financial Institution(s) may not publicly release any analysis or research concerning the provided SSN Verification, including reviews of SSA's business process(es) associated with the SSN verification.

22. In the case of a "no" match SSN Verification result, the Permitted Entity must not share the explanatory information identifying the data element(s) that does not match the information in SSA's records with the SSN holder.

23. 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).

B. **SSA Responsibilities**

1. SSA will compare the Fraud Protection Data provided in the Permitted Entity's SSN Verification request with the information in SSA's Master File of SSN Holders and

SSN Applications and provide SSN Verification results in an appropriate format and method based on the submission format and method.

2. SSA or an SSA designated third party will review all Supporting Documentation, conduct audits, generate reports, and conduct site visits limited to eCBSV-related systems of the Permitted Entity and each of its Financial Institutions, if any, as needed to ensure proper use of and to deter fraud and misuse of the eCBSV system. SSA, in its sole discretion, will determine the need for audits, reports, or site visits upon its review of the Permitted Entity's submissions, results, or SSA obtained certified public accounting (CPA) report.

3. Upon SSA discovery of any violation of the Banking Bill or this user agreement, the Commissioner shall forward any relevant information pertaining to the violation(s) to the appropriate agency in accordance with paragraphs (1) through (7) of the GLBA section 505(a) (15 U.S.C. § 6805(a)) for enforcement by the agencies described in or included by reference in those paragraphs, for purposes of enforcing the Banking Bill, this user agreement, and maintaining the integrity of the eCBSV service.

4. Upon SSA discovery of any violation of this user agreement as a result of SSA's review of an audit or other discovery, SSA may terminate or suspend the eCBSV services in accordance with the terms in this user agreement.

5. SSA will ensure the eCBSV system has commercially reasonable uptime and availability.

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)

2. 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).

3. 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.

V. Technical Specifications and Systems Security and Related Business Process Requirements

A. Technical Specifications and Systems Security

1. The Permitted Entity may use a real-time service or batch functionality, when available. All fees charged by SSA to the Permitted Entity will be applied regardless of the methods of service it uses.

2. Detailed technical requirements and procedures for using the eCBSV system are set forth on SSA's internet website at: https://www.ssa.gov/dataexchange/eCBSV/, which SSA may amend at its discretion.

3. If the Permitted Entity accesses the eCBSV system through the real-time platform client application, the Permitted Entity must maintain an automated audit trail record for five (5) years identifying either the Authorized User or the system process that initiated a request for information from SSA. Every SSN Verification request must be traceable to the Authorized User or the system process that initiated the transaction. The Permitted Entity shall process all SSN Verifications and Written Consents in a manner that will protect the confidentiality of the records and prevent the unauthorized use of the SSN Verifications and Consent Forms.

4. The Permitted Entity should integrate with SSA's entity services using identity federation. Identity federation requires the Permitted Entity to:

    a. Identity proof Authorized Users in a manner that meets National Institute of Standards and Technology (NIST) Special Publications (SP) 800-63-3 Identity Assurance Level (IAL) 2, require that authentication meets NIST SP 800-63-3 Authenticator Assurance Level (AAL) 2, and enable single sign-on for individuals that will use federation to access SSA web applications.

    b. Follow the session management guidelines for AAL2, found in NIST SP 800-63-3 B, Chapter 7 - https://pages.nist.gov/800-63-3/sp800-63b.html#sec7.

    c. Ensure controls are in place to properly set attributes that allow Authorized Users access to the eCBSV service.

    d. Recertify attributes that allow Authorized Users access to SSA web sites every 90 days.

    e. Ensure private keys are protected to prevent unauthorized access as outlined in NIST SP 800-57, "Recommendation for Key Management."

5. Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures to ensure that SSN Verifications are encrypted at rest and in transit.

6. The Permitted Entity shall also ensure that 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 U.S. Virgin Islands). The Permitted Entity shall ensure that any entity involved with storing the SSN Verifications are United States based entities bound by the laws within the United States (notwithstanding the physical location of the business).

B. Protecting and Reporting the Loss of SSN Verifications or Written Consents

1. The Permitted Entity's Responsibilities in Safeguarding SSN Verifications or Written Consents

   The Permitted Entity and/or Financial Institutions it services, if any, shall maintain, and follow its own policy and procedures to protect SSN Verifications and Written Consents, including the policies and procedures it has established for reporting lost or compromised, or potentially lost or compromised non-public information of its consumers. It is the Permitted Entity's and/or Financial Institutions' responsibility to safeguard SSN Verifications and Written Consents to which each entity has access. In addition, the Permitted Entity or Financial Institution that has access to the SSN Verification or Written Consents shall, within reason, take appropriate and necessary action to: (1) educate its Authorized Users on the proper procedures designed to protect SSN Verifications and Written Consents; and (2) enforce compliance with the policy and procedures prescribed.

   The Permitted Entity, any Financial Institutions it services, and Authorized Users shall properly safeguard SSN Verifications and Written Consents to which it has access from loss, theft, or inadvertent disclosure. The Permitted Entity, any Financial Institution it services, and Authorized Users are responsible for safeguarding this information at all times.

2. Reporting Lost, Compromised, or Potentially Compromised SSN Verifications or Written Consents

(a) When the Permitted Entity, including any Financial Institution(s) it services, if any that has access to an SSN Verification or Written Consent, becomes aware or suspects that SSN Verifications or Written Consents have been lost, compromised, or potentially compromised, the Permitted Entity or the Financial Institution, in addition to its own reporting process, shall provide <u>immediate</u> notification of the incident to the primary SSA contact. If the primary SSA contact is not readily available, the Permitted Entity or the Financial Institution shall <u>immediately</u> notify an SSA alternate, if the name of the alternate has been provided. (<u>See Section XV for the phone numbers of the designated primary and alternate SSA contacts</u>.) The Permitted Entity shall act to ensure that each Financial Institution has been given information as to who the primary and alternate SSA contacts are and how to contact them.

(b) The Permitted Entity shall provide the primary SSA contact or the alternate, as applicable, with updates on the status of the reported loss or compromise as they become available but shall not delay the initial report.

(c) The Permitted Entity shall provide complete and accurate information about the details of the possible SSN Verifications or Written Consents loss to assist the SSA primary contact or alternate, including the following information:

1. Contact information;
2. A description of the loss, compromise, or potential compromise (i.e., nature of loss/compromise/potential compromise, scope, number of files or records, type of equipment or media, etc.) including the approximate time and location of the loss;
3. A description of safeguards used, where applicable (e.g., locked briefcase, redacted personal information, password protection, encryption, etc.);
4. Name of SSA employee contacted;
5. Whether the Permitted Entity or the Financial Institution has contacted or been contacted by any external organizations (i.e., other agencies, law enforcement, press, etc.);
6. Whether the Permitted Entity or the Financial Institution has filed any other reports (i.e., Federal Protective Service, local police, and SSA reports); and
7. Any other pertinent information.

C. The Permitted Entity is responsible for authorization, tracking, and misuse by Employees and Authorized Users.

The Permitted Entity and all Financial Institutions it services, if any, shall process all SSN Verifications or Written Consents to which it has access under the immediate supervision and control of an Authorized User in a manner that will protect the confidentiality of the records; track the dissemination of the records; prevent the unauthorized use of SSN Verifications and Written Consents; and prevent access to the records by unauthorized persons.

VI. Costs of Service

The Permitted Entity must provide SSA with advance payment for the full annual cost of all services rendered under this user agreement, and submit to SSA proof of such advance payment each year in the manner directed by SSA. SSA will not perform any services under this user agreement for any year until the Permitted Entity provides such advance payment, and proof of such advance payment, to SSA. Moreover, SSA may incur obligations by performing services under this user agreement only on a 365-day agreement year basis.

SSA will use a tiered subscription-based pricing model. The Permitted Entity must select from one of the tiers offered by SSA, depending on annual estimated number of transactions. Information on the current tiers and pricing model can be found on SSA's internet website at: https://www.ssa.gov/dataexchange/eCBSV/. If transactions are not used within that tier range during the 365-day agreement year, they will not be rolled over to the next year.

The Permitted Entity must provide advance payment using Pay.gov either by credit card (up to the limit set by the Department of the Treasury, found at the Department of Treasury's internet website at: https://tfm.fiscal.treasury.gov/v1/p5/c700.html, Section 7045.10-Transaction Maximums) or ACH credit or debit. SSA will not accept checks or credit card information received in the mail by any method.

Prior to the start of each new 365-day agreement year, the Permitted Entity must submit full payment of fees (including, as applicable, initial and renewal administrative fees) for estimated requests for that annual agreement period with a completed user agreement on file. Transactions will be provided only up to the maximum volume within the selected tier level. The Permitted Entity will remain in active status as long as its account balance is positive. When balances are low, SSA will notify the Permitted Entity and the Permitted Entity must decide whether to enter into a new 365-day agreement period at any tier level or stop transactions for the year once the threshold has been met. If the Permitted Entity selects a new tier level during the agreement year, a new 365-day agreement period begins. Upon completion of an original 365-day agreement, the Permitted Entity can select any tier for the next 365-day agreement. No interest shall accrue to the advance payment.

At least annually, SSA will review its costs related to providing the eCBSV services, recalculate the fees necessary for SSA to recover full costs, and adjust the fees accordingly. SSA will notify the Permitted Entity before any change to the fees goes into effect.

VII. Duration of User Agreement, Suspension of Services, and Waiver of Right to Judicial Review

A. Duration and Termination of User Agreement

The effective date of this user agreement is the date upon which the Permitted Entity signs this user agreement. This user agreement will be in effect for a period of two (2) years from the effective date unless terminated or cancelled as follows:

1. SSA and the Permitted Entity may mutually agree in writing to terminate this user agreement, in which case the termination will be effective on the date specified in such termination agreement;

2. SSA terminates this user agreement upon determining, in its sole discretion that the Permitted Entity or any Financial Institution(s) it services has failed to comply with its responsibilities under this user agreement or the Banking Bill. This includes, without limitation, the Permitted Entity's obligation to make advance payment, requirement to collect Written Consent in accordance with this user agreement, and responsibilities under section III, Responsibilities, including failure to correct its non-compliance within 30 days of SSA's notice of such non-compliance;

3. This user agreement or the eCBSV service is prohibited by any applicable law or regulation, at which point this user agreement will be null and void as of the effective date specified in such law or regulation;

4. SSA terminates this user agreement and the eCBSV program due to a change of SSA's statutory requirements. In case of such cancellation of eCBSV program, SSA will provide all participants in the eCBSV program with advance written notice of SSA's decision;

5. If the Permitted Entity is dissolved as a corporate entity (including acquisition by another corporate entity that results in the dissolution of the Permitted Entity) this user agreement and any related payments are no longer valid as of the date of dissolution. Within 30 days of dissolution or the termination of this user agreement (per the terms of this user agreement or the expiration of the effective period of this user agreement), the Permitted Entity must provide SSA through a mutually agreeable process copies of all Written Consents supporting the Permitted Entity's (and Financial Institution(s)) requests for SSN Verifications for the 3- year period prior to the date of the dissolution or termination, unless otherwise excepted by SSA. Any new corporate entity purporting to acquire the Permitted Entity's interest in this user agreement must sign a new user agreement and submit payment. The Permitted Entity's rights and obligations under this user agreement cannot be assigned to another entity whether through purchase, acquisition, or corporate reorganization.

SSA reserves the right to determine whether to issue refunds under this section. SSA will issue no refunds when SSA terminates the user agreement, or the Permitted Entity is at fault.

B. Suspension of Services

1. Suspension of eCBSV services by SSA is a temporary action for a designated period until certain requirements are met or rectified. Suspension is immediate upon notice by SSA. SSA will send a notice of suspension to the Permitted Entity via email with the specific reason(s) for the suspension, and the suspension remains in effect until lifted by SSA.

2. If the Financial Institution serviced by the Permitted Entity, if any, is suspended, the Financial Institution is prohibited from submitting SSN Verification requests through another permitted entity during the period of suspension.

3. Noncompliance with this user agreement, including with the declarations set forth in the Permitted Entity Certification of this user agreement (Exhibit A), or the Banking Bill, is grounds for suspension of eCBSV services at the sole discretion of SSA.

4. If the Permitted Entity disputes SSA's decision to suspend its access, the Permitted Entity may elect to write a letter to SSA specifying the reasons for contesting the suspension. Such letters must be sent via e-mail to eCBSV@ssa.gov and must be received by SSA within 30 calendar days from the date that SSA transmitted the notice of suspension to the Permitted Entity.

5. After reviewing the Permitted Entity's letter, SSA may make the final determination to: 1) lift the suspension; 2) continue the suspension; or 3) terminate the Permitted Entity's user agreement. SSA will provide the Permitted Entity with written notice via email of its final decision.

6. The Permitted Entity's use of the eCBSV system may be suspended for any of the following reasons:
   a. Non-payment, or
   b. Violation of user agreement terms, or
   c. Violation of the Banking Bill.

Notwithstanding section VII.A and B immediately above, all provisions in section IV.B and section V as to data security and safeguards shall remain in effect for all information SSA provides to the Permitted Entity under this user agreement for as long as Permitted Entity or the Financial Institution retains such information.

C. Waiver of Right to Judicial Review

The Permitted Entity and all Financial Institutions the Permitted Entity services specifically waives any right to judicial review of SSA's decision to cancel the provision of eCBSV services or suspend or terminate this user agreement.

VIII. Audit Requirements

A. Mandatory Audits

The Permitted Entity agrees that it will be subject to mandatory audits conducted by SSA as follows:

1. Initial Audit

   a. Every Permitted Entity enrolled in eCBSV will be subject to an initial audit once in the first year after executing this user agreement;
   b. Every Financial Institution serviced by the Permitted Entity, if any, will be subject to an initial audit once within five (5) years after the Permitted Entity executes this user agreement.

2. Subsequent Audit

   a. If the Permitted Entity is subject to regulatory enforcement and oversight actions under section 505(a)(1)-(7) of GLBA and has no Type I or Type II noncompliance violations as defined in section IX A, below, in the most recent audit, will be subject to an audit once every 5 years after the first audit;
   b. If the Permitted Entity is not subject to regulatory enforcement or oversight actions under section 505(a)(1)-(7) of GLBA, or has any Type I or Type II noncompliance violations, will be subject to an audit every year;
   c. The Permitted Entity and the Financial Institutions it services, if any, are subject to audits at SSA's discretion at any time.

B. Initiating the Audit

1. An SSA-appointed CPA firm will perform an annual audit in accordance with paragraph A above to ensure that all SSN Verification requests are in compliance with this user agreement and the Banking Bill. The CPA firm will perform the audit in accordance with the standards established by the American Institute of Certified Public Accountants and contained in the Generally Accepted Government Audit Standards (GAGAS).
2. SSA will send a notice to the Permitted Entity identifying the name of the retained CPA firm and its designated contact.

C. Permitted Entity's Cooperation with Audit

The Permitted Entity will:

A. Provide to the reviewing CPA all requested Supporting Documentation in their entirety;
B. In the case where the Permitted Entity is servicing a Financial Institution(s), inform all Financial Institutions of the requirement to produce Supporting Documentation upon the CPA's request for purposes of the audit.
C. The Permitted Entity will receive a copy of the CPA firm's report 30 calendar days after the report is provided to SSA.

D. SSA

If the results of the CPA's review indicate that the Permitted Entity and/or Financial Institution has not complied with any term of this user agreement or the Banking Bill, SSA, in addition to referring the matter to the appropriate regulatory enforcement agency in accordance with the Banking Bill, may:

A. Perform its own onsite inspection, audit, or compliance review;
B. In accordance with federal law, refer the report to its Office of the Inspector General for appropriate action, including referral to the Department of Justice for criminal prosecution;
C. Suspend eCBSV services;
D. Terminate this user agreement; and/or,
E. Take any other action SSA deems appropriate.

IX. Noncompliance Categories, Penalties, Reinstatement

A. Types of Noncompliance

1. Type I noncompliance is the most serious of categories of noncompliance as SSA deems them to significantly place SSN Verifications or Written Consents at risk or have resulted in unauthorized disclosure of SSN Verifications or Written Consents and are systemic in nature. Type I noncompliance may consist of one or more of the following:

A. Multiple failures to comply with this user agreement requirements determined by SSA to be detrimental to the protection of SSN Verifications or Written Consents;
B. Multiple instances of Type II noncompliance examples;
C. Fraudulent use of the eCBSV service system's access privileges;
D. Other issues determined by SSA to place a significant quantity of SSN Verifications or Written Consents at risk; and/or
E. A violation of securely storing Written Consents.

2. Type II noncompliance consists of one or more of the following:

   A. SSN Verification request submitted to SSA but not authorized by an SSN holder including missing, unsigned, or fraudulently-submitted Written Consents;
   B. Permitted Entity submitted an SSN Verification request to SSA based on an outdated Written Consent;
   C. A violation of the retention requirements, including missing Supporting Documentation, in this user agreement;
   D. Permitted Entity submitted an SSN Verification request to SSA based on a Written Consent related to a purpose outside of the Banking Bill; and/or
   E. Permitted Entity's use of SSN Verification or Written Consent for a purpose not authorized by the Written Consent or this user agreement.

3. Type III noncompliance consists of failures that are minor in nature because they would not result in either unauthorized disclosure of SSN Verifications or Written Consents or unauthorized SSN Verification requests being submitted to SSA.

   Type III noncompliance may consist of one or more of the following:

   A. Illegible Written Consents;
   B. Permitted Entity submitted an SSN Verification request to SSA based on a Written Consent that did not contain the Permitted Entity's or Financial Institution's address; and/or
   C. Permitted Entity untimely submitted a required audit report to SSA.

B. Penalties For Each Type of Noncompliance

The penalty schedule for each type of noncompliance is as follows:

1. Type I – Suspension of Permitted Entity privileges for **90 days**.
2. Type II – Suspension of Permitted Entity privileges for **60 days**.
3. Type III – Suspension of Permitted Entity privileges for **30 days**.

SSA will impose penalties on the Permitted Entity in accordance with this user agreement. If the Permitted Entity services any Financial Institutions, SSA will hold the Permitted Entity accountable for all instances of noncompliance of each of its Financial Institutions. MULTIPLE PENALTIES IMPOSED MAY LEAD TO TERMINATION OF THIS USER AGREEMENT AT THE SOLE DISCRETION OF SSA.

C. Reinstatement of eCBSV Services after a Suspension

After serving its suspension, the Permitted Entity may apply for reinstatement of eCBSV services. To apply, the Permitted Entity must provide SSA with a corrective action plan that outlines how it rectified any areas of noncompliance. Upon receipt of the corrective action plan, SSA will make a determination of reinstatement and notify the Permitted Entity within ten (10) business days of its decision.

X. Unilateral Amendments

SSA reserves the unilateral right to amend this user agreement at any time to implement the following:

1. Minor administrative changes, such as changes to SSA contact information; or

2. Procedural changes, such as method of transmitting requests and results and limits on the number of SSN Verification requests.

SSA will notify the Permitted Entity of any unilateral amendments under this section. If the Permitted Entity does not wish to be bound by any such unilateral amendment, the Permitted Entity may terminate this user agreement with 30 calendar days' notice.

XI. Indemnification

Notwithstanding any other provision of this user agreement, the Permitted Entity and Financial Institution will indemnify and hold SSA harmless from all claims, actions, causes of action, suits, debts, dues, controversies, restitutions, damages, losses, costs, fees, judgments, and any other liabilities caused by, arising out of, associated with, or resulting directly or indirectly from, any acts or omissions of the Permitted Entity or Financial Institution, including but not limited to the disclosure or use of information by the Permitted Entity or Financial Institutions, or any errors in information provided to the Permitted Entity under this user agreement. SSA is not responsible for any financial or other loss incurred by the Permitted Entity or any Financial Institution serviced by the Permitted Entity, whether directly or indirectly, through the use of any data provided pursuant to this user agreement. SSA is not responsible for reimbursing the Permitted Entity or Financial Institution for any costs the Permitted Entity or Financial Institution incurs pursuant to this user agreement.

XII. Disclaimers

SSA is not liable for any damages or loss resulting from errors in information provided to the Permitted Entity or Financial Institution under this user agreement. Furthermore, SSA is not liable for damages or loss resulting from the destruction of any materials or data provided by the Permitted Entity. All information furnished to the Permitted Entity or Financial Institution will be subject to the limitations and qualifications, if any, transmitted with such information. If, because of any such error, loss, or destruction

attributable to SSA, SSA must re-perform the services under this user agreement, the additional cost thereof will be treated as a part of the full costs incurred in compiling and providing the information and will be paid by the Permitted Entity.

SSA's performance of services under this user agreement is authorized only to the extent that they are consistent with performance of the official duties and obligations of SSA. If for any reason SSA delays or fails to provide the services, or discontinues all or any part of the services, SSA is not liable for any damages or loss resulting from such delay, failure, or discontinuance.

Nothing in this user agreement is intended to make any person or entity who is not a signatory to this user agreement a third-party beneficiary of any right created by this user agreement or by operation of law.

XIII. Integration

This user agreement and the accompanying exhibits, along with any affirmations required by SSA and made by the Permitted Entity during any initial or subsequent registrations for the eCBSV system, constitute the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties or promises made outside of this user agreement. This user agreement shall take precedence over any other documents that may be in conflict with it.

XIV. Resolution Mechanism

In the event of a disagreement between the parties to this user agreement, the parties will meet and confer to attempt to negotiate a resolution. If the parties cannot agree on a resolution, the parties will submit the dispute in writing to the Deputy Commissioner, Office of Budget, Finance, and Management, of SSA, who will render a final determination binding on both parties.

XV. Contacts:

A. SSA Contacts

1) eCBSV Project Team
Email: eCBSV@ssa.gov
Call: 866-395-8801

2) Billing and Payment Issues
Physical address via U.S. Postal Service or overnight carrier
ATTN eCBSV Mailstop 2-O-2 ELR DRAC IABT
Social Security Administration
6401 Security Blvd
Baltimore MD 21235
410-597-1673
Email: OF.DRAC.eCBSV@SSA.GOV

PO Box address:
ATTN eCBSV
Social Security Administration
PO Box 17042
Baltimore MD 21235

3) Reporting Lost, Compromised or Potentially Compromised SSN Verifications or Written Consents
Office of Data Exchange, Policy Publications, and International Negotiations
Project Manager: Christopher David 410-966-4320
Alternate Contact: Barbara Kocher 410-966-5763

B. Permitted Entity Contacts

REMINDER: Report changes to SSA within 30 days.

Company Name: _____

Primary Contact: _____
Title: _____

Address: _____
_____
_____

Telephone: _____
Fax: _____
Email: _____

Alternate Contact: _____
Title: _____
Address: _____
_____
_____

Telephone: _____
Fax: _____
Email: _____

XVI. Authorizing Signature and Date

The signatory below warrants and represents that he/she has the competent authority on behalf of its entity to enter into the obligations set forth in this user agreement.

The signatory may sign this document electronically by using an approved electronic signature process. By providing a signature, the Permitted Entity is accepting SSA's offer to participate in eCBSV and agreeing to abide by the terms of this user agreement.

The signatory, if electronically signing this user agreement agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the user agreement, and that it has the same meaning as his/her handwritten signature.

Permitted Entity

_____

Company Official Signature

_____

Company Official Name

_____

Company Official's Title

_____

Permitted Entity's Name

Date:_____

Exhibit A - Certification Statement {INSERT PERMITTED ENTITY's NAME}

CERTIFICATION STATEMENT FOR
PERMITTED ENTITIES USING THE SSN VERIFICATION PROCESS
(Signature required biennially)

Name and address of Permitted Entity:

_____
_____
_____
_____

The following certification must be completed prior to SSA authorizing use of the eCBSV system.

I, _____on behalf of the company listed above, certify that this entity attests to each of the following four (4) declarations:

1. The entity is a Permitted Entity.
2. The entity is in compliance with the Banking Bill.
3. The entity is, and will remain, in compliance with its privacy and data security requirements, as described in title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801, et seq.), with respect to information the entity receives from the Commissioner pursuant to the Banking Bill.
4. The entity will retain sufficient records to demonstrate its compliance with its certification and the Banking Bill for a period of not less than two (2) years.

The permitted entity will provide this Certification to SSA, and not submit any SSN Verification request to SSA if the Certification is older than two (2) years old or the permitted entity cannot attest to any one of the four (4) declarations.

The signatory, if electronically signing this document, agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

[Please clearly print or type your designated company official's name, title, and phone number and have him/her provide an electronic or wet signature and date below.]

Company Official Name_____
Company Official Title _____
Company Official Phone Number_____
Signature_____Date_____

Exhibit B - Form SSA-89

Form **SSA**-89 (04-2025)
Discontinue Prior Editions
Social Security Administration

Page 1 of 1
OMB No.0960-0760

Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification

Printed Name:	Date of Birth:	Social Security Number:

Reason for authorizing consent: (Please select one)

- ☐ To apply for a mortgage
- ☐ To apply for a loan
- ☐ To meet a licensing requirement
- ☐ To open a bank account
- ☐ To open a retirement account
- ☐ Other
- ☐ To apply for a credit card
- ☐ To apply for a job

With the following company ("the Company"):

Company Name:

Company Address:

The name and address of the Company's Agent (if applicable):

Agent's Name:

Agent's Address:

I authorize the Social Security Administration to verify my SSN (to match my name, SSN, and date of birth with information in SSA records and provide the results of the match) to the Company or Company's Agent, if applicable, for the purpose I identified. I also authorize SSA to disclose the basis for a no-match to the Company and/or Company Agent, when it is a Permitted Entity as defined by section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act. I am the individual to whom the SSN was issued or the parent or legal guardian of a minor or legally incompetent adult. I declare and affirm under the penalty of perjury that the information contained herein is true and correct. I acknowledge that if I make any representation that I know is false to obtain information from Social Security records, I could be found guilty of a misdemeanor and fined up to $5,000.

This consent is valid only for one-time use. This consent is valid only for 90 days from the date signed, unless indicated otherwise by the individual named above. If you wish to change this timeframe, fill in the following:

This consent is valid for _____ days from the date signed. _____ (Please initial.)

Signature:	Date Signed:

Relationship (if not the individual to whom the SSN was issued):

Privacy Act Statement Collection and Use of Personal Information Sections 205(a) and 1106 of the Social Security Act, as amended, allow us to collect this information, which we will use to verify your Social Security Number to a company or company's agent. Providing this information is voluntary, but not providing such may prevent us from assisting you with the request. As law permits, we may use and share the information you submit, including with other Federal agencies, contractors, and others, as outlined in the routine uses within System of Records Notice 60-0058, available at www.ssa.gov/privacy. The information you submit may also be used in computer matching programs for Federal benefits eligibility and to recoup debts under these programs.

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget (OMB) control number. We estimate that it will take about 20 minutes to read the instructions, gather the facts, and answer the questions. ***Send only comments regarding this burden estimate or any other aspect of this collection, including suggestions for reducing this burden to:*** SSA, 6401 Security Blvd., Baltimore, MD 21235-6401. .

----------TEAR OFF----------

NOTICE TO NUMBER HOLDER

The Company and/or its Agent have entered into an agreement with SSA that, among other things, includes restrictions on the further use and disclosure of SSA's verification of your SSN. To view a copy of the entire model agreement, visit http://www.ssa.gov/cbsv/docs/SampleUserAgreement.pdf.

Exhibit C – SSA Written Consent Template

Option 1: Static Purpose:

Authorization for the Social Security Administration to Disclose Your Social Security Number Verification

I authorize the Social Security Administration (SSA) to verify and disclose to [Name of Financial Institution] through [Name of Service Provider, (if one), their service provider] for the purpose of this transaction whether the name, Social Security Number (SSN) and date of birth I have submitted matches information in SSA records, including the basis for a no-match response. My consent is for a one-time validation within the next [number of days].

Option 2: Dynamic Purpose:

Authorization for the Social Security Administration to Disclose Your Social Security Number Verification

I authorize the Social Security Administration (SSA) to verify and disclose to [Name of Financial Institution] through [Name of Service Provider, (if one), their service provider] for the purpose of [insert specific purpose] whether the name, Social Security Number (SSN) and date of birth I have submitted matches information in SSA records, including the basis for a no-match response. My consent is for a one-time validation within the next [number of days].

*NOTE: The Permitted Entity or Financial Institution must maintain evidence documenting the specific purpose in accordance with sections III, IV, and VIII of the user agreement.