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.


**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.

**Consent Form** – Form SSA-89 (Authorization for SSA to Release SSN Verification – Exhibit A) with a wet signature or in “pdf fillable” form with an Electronic Signature, or an electronic form of consent that meets SSA’s Written Consent requirements in this user agreement.

**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 the original requesting source for the SSN Verification and either signs this user agreement as the Permitted Entity or 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.

**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.

**Permitted Entity** – A Financial Institution as defined by section 509 of GLBA, 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 of the four items identified in section III.A.1. of this user agreement and
as required by the Banking Bill.

PII - PII is personally identifiable information, or any information about an individual maintained by a Permitted Entity or Financial Institution, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

SSN Verification – The response SSA provides to the Permitted Entity or Financial Institution after conducting a verification of the SSN holder’s Fraud Protection Data

Written Consent – Written Consent, including electronic, authority by which the SSN holder gives SSA permission to release SSN Verification results to the Permitted Entity or Financial Institution 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), the information the SSN holder wants SSA to disclose (e.g., verify name, SSN, date of birth), and, where applicable, during which timeframe the information may be disclosed (see 20 CFR Part 401.100). Written Consent must be provided in one of the following ways:

1. Form SSA-89 (Exhibit A, Authorization for SSA to Release SSN Verification) with a wet signature, or

2. Form SSA-89 in “pdf fillable” form with an Electronic Signature, or

3. Electronically with SSA’s consent language as provided in section IV, which is incorporated into the Permitted Entity’s business process.

C. Legal Authority

Legal authority for providing 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 and Use

SSA will verify SSNs solely for the purpose(s) specified within the Written Consent associated with the SSN Verification request(s). In accordance with the Banking Bill, a Permitted Entity is authorized to request an SSN Verification with valid Written Consent 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 Permitted Entity must use the SSN Verification only for the purpose(s) specified by the SSN holder. Exceeding the scope of the
Written Consent as specified in the Written Consent, violates Federal law and subjects the Permitted Entity or Financial Institution to civil and criminal liability.

SSA recognizes that the Permitted Entity may seek SSN Verifications on behalf of a Financial Institution pursuant to the terms of the SSN holder’s Written Consent. In this case, the Permitted Entity shall require the Financial Institution to agree in writing to use the SSN Verification only for the purpose stated in the Written Consent, and make no further use or disclosure of the SSN Verification. The Permitted Entity shall also require that the Financial Institution comply with all contractual obligations set forth in this user agreement.

The information obtained from SSA’s records is protected by Federal statutes and regulations, including 5 U.S.C. § 552a(i)(3) of the Privacy Act. Under this section, any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses will be guilty of a misdemeanor and fined not more than $5,000.

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. 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. Pursuant to the certification requirement in the Banking Bill, the Permitted Entity must submit a 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 B. The Permitted Entity must complete its own certification and, if it is a Permitted Entity that services a Financial Institution pursuant to a separate agreement as required under section III.A.10, provide to SSA a certification completed by each Financial Institution it services. As required by the Banking Bill, the certification must include the following four declarations set forth in Exhibit B:

   a. The entity is a permitted entity.

   b. The entity is in compliance with the Banking Bill.

   c. The entity is, and will remain, in compliance with its privacy and data security requirements, as described in title V of GLBA (15 U.S.C. § 6801, et seq.), with
respect to information the entity receives from the Commissioner pursuant to the Banking Bill.

d. The permitted 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.

2. For SSA to recognize the Permitted Entity’s successor in interest to this user agreement or the Permitted Entity’s name change, the Permitted Entity must submit written notification electronically to the eCBSV Project Manager within 30 calendar days of the change. Any submission should be accompanied by a new Permitted Entity Certification. Because this user agreement is not assignable, any successor in interest to this user agreement must sign a new user agreement with SSA. Any change resulting in a new user agreement may result in a disruption of the eCBSV service.

3. The Permitted Entity may 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, not to exceed 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.

4. The Permitted Entity must submit SSN Verification requests to eCBSV 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).

5. SSA may change its method of receiving SSN Verification requests and providing SSN Verification results to the Permitted Entity at any time. 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.

6. The Permitted Entity will implement and use an Electronic Signature or electronic signature process on the Consent Form that meets the standards as set forth by SSA.

7. The Permitted Entity must not alter the Consent Form either before or after the SSN holder completes the Consent Form. 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 Consent Form, including by a new Electronic Signature meeting SSA requirements. Alterations do not include fax date/time stamps, barcodes, quick response codes or tracking/loan numbers added to the margin of a form.
8. 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.

9. 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 all eCBSV activities of itself and if operating as a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution, for all Financial Institutions serviced by the Permitted Entity for all SSN Verification requests.

10. 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.

11. 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 PII of the confidential nature of the information and the administrative, technical, and physical safeguards required to protect the information from improper disclosure. The Permitted Entity will store all confidential information in an area that is physically safe (i.e., password protected hard drive, USB drive or disk) from unauthorized access at all times.

12. The Permitted Entity 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.

13. The Permitted Entity must not submit an SSN Verification request to SSA before the Permitted Entity receives the requisite Written Consent, which has been properly completed by the SSN holder. Any SSN Verification request submitted to SSA without a properly completed Written Consent is subject to legal penalties and could lead to termination of this user agreement.

14. The Permitted Entity, if it is a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution will notify SSA within 30 calendar days if any of the Financial Institution(s) they represent change(s).

15. With respect to advertising, the Permitted Entity acknowledges 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. SSA has the right to review the records associated with the eCBSV program of the Permitted Entity and in the case of a Permitted Entity servicing a Financial Institution, the Financial Institution at any time.

e. The Permitted Entity cannot advertise that eCBSV will eliminate synthetic ID fraud.

16. The Permitted Entity must bear all costs it incurs for site preparation, connection, operating costs, and any other miscellaneous costs to participate in eCBSV. 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 confidential information and adherence to terms of this user agreement.

17. 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” for future reference.

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 eCBSV SSN Verification requests and results, conduct audits, generate reports, and conduct site visits of the Permitted Entity and each of its Financial Institutions, if any, as needed to ensure proper use to deter fraud and misuse 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 the following Consent Forms:

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

   b. SSA-89, in a “pdf fillable” form, signed electronically by the SSN holder, with an Electronic Signature that meets SSA’s Electronic Signature requirements, set forth at www.ssa.gov/dataexchange/eCBSV; or

   c. An electronic form of consent, which can be incorporated into the Permitted Entity’s or Financial Institution’s electronic workflow or business process, and which includes SSA’s requirements for a valid Written Consent, signed electronically by the SSN holder with an Electronic Signature that meets SSA’s requirements. See SSA’s Written Consent Template, attached and incorporated into this user agreement as Exhibit C.

2. The Permitted Entity must use the SSA Written Consent Template if not using the SSA-89, which includes the following requirements:

   a. The Consent Form incorporated into the Permitted Entity’s or Financial Institution’s existing business process must contain the title of SSA’s consent section in “bold” font followed directly by the SSA-provided language.
b. The following items must also be present on the same electronic screen as the bolded title:
   i. The SSN holder’s name, SSN, and date of birth;
   ii. The name and address of the Permitted Entity and Financial Institution, if applicable;
   iii. The Electronic Signature of the SSN holder;
   iv. The statement that SSA may disclose the SSN Verification to the party listed on the Consent Form;
   v. A specific timeframe during which SSA may disclose the SSN Verification, if different than 90 days from the date the SSN holder signs the Consent Form; and
   vi. The purpose for which the Permitted Entity or Financial Institution will use the information, limited only to the purpose(s) specified in the Banking Bill.

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

4. Written Consents that do not meet these requirements must be returned to the SSN holder with an explanation of why the Written Consent is deficient.

5. The Permitted Entity or Financial Institution, if any, may not alter the Written Consent either before or after the SSN holder completes the Consent Form. 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 SSA’s requirements.

6. 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 must retain the signed Written Consent for a period of five (5) years from the date of the SSN Verification request, either electronically or on paper. The Permitted Entity 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 must also protect the Written Consent from loss or destruction by taking the measures below. (See section V.B for procedures on reporting loss of PII).

If the Permitted Entity chooses to retain the Written Consent in paper format, the Permitted Entity must store the Written Consent in a locked, fireproof and waterproof storage receptacle. The Permitted Entity shall restrict access to all confidential information 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.17, the
stored data must not be reused. However, the Permitted Entity can mark its own records as “verified” or “unverified” for future reference. The Permitted Entity cannot reuse a Written Consent to submit another SSN Verification request or for different purposes.

If the Permitted Entity chooses to retain the Written Consent electronically or store it on removable electronic media (such as CDs), the Permitted Entity and any Financial Institutions it services, if any, must make sure such method accounts for integrity of signed records 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.

When storing the Written Consent electronically, the Permitted Entity must destroy the original paper consent 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, 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 and the information contained therein and to assess overall system security.

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

D. Requests from SSN holder’s Parents or Legal Guardians

The Permitted Entity cannot 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. The Permitted Entity must submit such SSN Verification requests based on an SSA-89 signed with a wet signature. If the request is for a minor child (under age 18), a parent or legal guardian must sign the Form SSA-89. If the request is for a legally incompetent adult, a legal guardian must sign the Form SSA-89.

If the parent or legal guardian signs the Form SSA-89, the Permitted Entity shall retain proof of the relationship, e.g., a copy of the birth certificate or court documentation proving the relationship. A third party (e.g., a spouse, an appointed representative, an attorney, a third party with a power of attorney) are not authorized to execute the Form SSA-89 on the SSN holder’s behalf. SSA does not recognize Power of Attorney for consent purposes.

E. Electronic Signature Requirements

The Permitted Entity or any Financial Institution(s) it services, if any, will use an Electronic Signature process that meets or exceeds SSA’s requirements, consistent with section 106 of the E-SIGN Act (15 U.S.C. § 7006) and as defined in the Electronic Signature Requirements for Permitted Entities on SSA’s internet website at https://www.ssa.gov/dataexchange/eCBSV/index.html.
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/technical_information.html, 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 confidential information under the immediate supervision and control of Authorized Users in a manner that will protect the confidentiality of the records; prevent the unauthorized use of confidential information; and prevent access to the records by Unauthorized Users.

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.


   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. The Permitted Entity that is not using federation must have all Authorized Users register to obtain accounts issued by SSA. The Permitted Entity is required to recertify each Authorized User who has an SSA-issued account every 90 days.

6. The Permitted Entity that is not using federation must notify the eCBSV Project Team within 24 hours when an Authorized User’s relationship with the entity has been terminated.

B. Protecting and Reporting the Loss of PII

1. The Permitted Entity’s Responsibilities in Safeguarding PII

The Permitted Entity shall establish, maintain, and follow its own policy and procedures to protect PII, including policies and procedures for reporting lost or compromised, or potentially lost or compromised PII. It is the Permitted Entity’s responsibility to safeguard PII or in the case of the permitted entity servicing Financial Institutions, the Financial Institution and the Permitted Entity, who handle the PII. In addition, the Permitted Entity shall, within reason, take appropriate and necessary action to: (1) educate Financial Institutions on the proper procedures designed to protect PII; and (2) enforce their compliance with the policy and procedures prescribed.

All Permitted Entities, Financial Institutions, and Authorized Users shall properly safeguard PII from loss, theft, or inadvertent disclosure. Each Permitted Entity, Financial Institution, and Authorized User is responsible for safeguarding this information at all times, regardless of whether or not the user is at his or her regular duty station.

2. Reporting Lost, Compromised, or Potentially Compromised PII

(a) When the Permitted Entity, including any Financial Institution(s) it services, if any, becomes aware or suspects that PII has been lost, compromised, or potentially compromised, the Permitted Entity or the Financial Institution, in accordance with its incident reporting process, shall provide immediate 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 immediately notify an SSA alternate, if the name of the alternate has been provided. (See Section XV for the phone numbers of the designated primary and alternate SSA contacts.) 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 PII 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 PII 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 confidential information 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 confidential information; 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 five tiers, 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/fees.html. If transactions are not used within that tier range during the 365-day agreement year, they will be 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 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 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 for a higher tier or stop transactions for the year once the threshold has been met. The Permitted Entity can only select a higher tier when a new tier level is selected during the agreement year, which will begin a new 365-day agreement period. Upon completion of an original 365-day agreement, the Permitted Entity can select a lower 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 Annual Renewal

A. Duration and Termination of User Agreement

This user agreement is effective upon signature of both parties, payment in full of all fees due and owing, and shall remain in effect until 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, at which point this user agreement and any related payments are no longer valid as of the date of dissolution. 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 certification statement of this user agreement (Exhibit B), 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 the first three (3) 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 12 U.S.C. § 1818, as defined in 12 U.S.C. § 1813(q), 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 12 U.S.C. § 1818, as defined in 12 U.S.C. § 1813(q), or has any Type I or Type II noncompliance violations will be subject to an audit every year; or
   c. The Permitted Entity and the Financial Institutions it services, if any, are subject to random audits at SSA’s discretion.

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 a copy of this signed user agreement and all applicable exhibits in their entirety; and
   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. 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 PII at risk or have resulted in unauthorized disclosure of PII 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 PII;
   B. Multiple instances of Type II noncompliance examples;
   C. Other issues determined by SSA to place a significant quantity of PII at risk; and/or
   D. 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 in this user agreement; and/or
   D. Permitted Entity submitted an SSN Verification request to SSA based on Written Consent that did not contain a proper purpose.
3. Type III noncompliance consists of failures that are minor in nature because they would not result in either unauthorized disclosure of PII 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 the 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 PII
   Office of Data Exchange, Policy Publications, and International Negotiations
   Project Manager: Michael Wilkins 410-966-4965
   Alternate Contact: Curtis Miller 410-966-2370

B. Permitted Entity Contacts

**REMEMBER: Report changes to SSA within 30 days.**

Company Name: ____________________________________________________________

Primary Contact: __________________________________________________________
XVI. **Authorizing Signatures and Dates**

The signatories below warrant and represent that they have the competent authority on behalf of their respective entities to enter into the obligations set forth in this user agreement.

The signatories may sign this document electronically by using an approved electronic signature process. Each signatory 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.

<table>
<thead>
<tr>
<th>Social Security Administration</th>
<th>Permitted Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegated SSA Official</td>
<td>Company Official Signature</td>
</tr>
<tr>
<td></td>
<td>Company Official Name</td>
</tr>
<tr>
<td></td>
<td>Company Official’s Title</td>
</tr>
<tr>
<td></td>
<td>Permitted Entity’s Name</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Printed Name:</th>
<th>Date of Birth:</th>
<th>Social Security Number:</th>
</tr>
</thead>
</table>

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 name and SSN to the Company and/or the Company's Agent, if applicable, for the purpose I identified. I am the individual to whom the Social Security number was issued or the parent or legal guardian of a minor, or the legal guardian of a 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 to be 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(e) and 1106 of the Social Security Act, as amended, allow us to collect this information. Furnishing us this information is voluntary. However, failing to provide all or part of the information may prevent us from releasing information to a designated company or company's agent.

We will use the information to verify your name and Social Security number (SSN). In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of routine uses is available in our Privacy Act System of Records Notice (SORN) 60-0068, entitled Master Files of SSN Holders and SSN Applications. Additional information and a full listing of all our SORNs are available on our website at www.socialsecurity.gov/foia/bluebook.

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3501, 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 control number. We estimate that it will take about 3 minutes to complete the form. You may send comments on our time estimate above to SSA, 6401 Security Blvd., Baltimore, MD 21236-8401. Send to this address only comments relating to our time estimate, not the completed form.

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/ocs/v/docs/SampleUserAgreement.pdf.
Autorización para que la Administración del Seguro Social Divulgue la Verificación de un Número de Seguro Social (SSN)

<table>
<thead>
<tr>
<th>Nombre en letra de molde:</th>
<th>Fecha de nacimiento:</th>
<th>Número de Seguro Social:</th>
</tr>
</thead>
</table>

Razón para autorizar la divulgación: (Favor de marcar una)
- [ ] Para solicitar una hipoteca
- [ ] Para solicitar un préstamo
- [ ] Para cumplir con requisitos de una licencia
- [ ] Para abrir una cuenta de banco
- [ ] Para abrir una cuenta de jubilación
- [ ] Otra razón (explique)
- [ ] Para solicitar una tarjeta de crédito
- [ ] Para solicitar un trabajo

Con la siguiente empresa ("la Empresa"):

Nombre de la empresa:

Dirección de la empresa:

Nombre y dirección del agente de la empresa (si aplica):

Nombre del agente:

Dirección del agente:

Autorizo a la Administración del Seguro Social a que verifique mi nombre y Número de Seguro Social (SSN, por sus siglas en inglés) con la empresa o con el agente de la empresa, si aplica, para el propósito que he identificado. Yo soy la persona a quien el Número de Seguro Social fue emitido o el representante legal de un menor o el representante legal de una persona quien ha sido declarada por la corte como adulto incompetente. Yo declaro y afirmo bajo pena de perjurio que la información contenida aquí es verdadera y correcta. Yo reconozco que si hago alguna representación, que yo sé que es falsa, para obtener información de los registros del Seguro Social, puedo ser declarado culpable de un delito menor y penalizado con una multa de hasta $5,000.

Este consentimiento es válido para un solo uso. Este consentimiento es válido por solo 90 días a partir de la fecha en que es firmado, a menos que se indique lo contrario por la persona nombrada en el encabezamiento. Si desea cambiar este límite de tiempo, favor de llenar la siguiente información:

Este consentimiento es válido por _______ días desde la fecha en que es firmado. _______ (Sus iniciales)

Firma: _______ Fecha en que firmó: _______

Parentesco (si no es la persona a quien le pertenece el SSN):

DECLARACIÓN DE LA LEY DE CONFIDENCIALIDAD DE USO Y RECOLECCIÓN DE INFORMACIÓN PERSONAL

Las secciones 205(a) y 1106 de la Ley del Seguro Social, según enmendada, nos autorizan a recopilar la información que se solicita en este formulario. No está obligado a proporcionar la información que se solicita. No obstante, si no nos proporciona parte o toda la información solicitada, podría impedir que divulguemos esta información a la empresa o al agente de la empresa nombrado en este formulario. Usaremos la información que nos proporciona para verificar su nombre y Número de Seguro Social (SSN). Además, es posible que compartamos esta información en cumplimiento de la Ley de Privacidad y otras leyes federales. Por ejemplo, si las leyes nos autorizan, es posible que esta información se use en programas de comparación de datos de computadoras, en los cuales nuestros registros son comparados con otros registros para establecer o verificar el derecho de una persona a los programas de beneficios federales y para el pago de deudas incorrectas o morosas bajo estos programas. Puede encontrar una lista de usos rutinarios en nuestro aviso de sistemas de computadoras titulado «Privacy Act Systems of Records Notice» (SORN, por sus siglas en inglés) 60-0058, titulado «Master Files of SSN Holders and SSN Applications», información adicional y una lista completa de todos nuestros SORN están disponibles en nuestro sitio de internet en www.sociaiSecurity.gov/fisa/bluebook (estos sistemas de computadoras y toda la demás información solo están disponibles en inglés).

DECLARACIÓN DE LA LEY DE REDUCCIÓN DE DOCUMENTOS DE TRÁMITES — La recopilación de esta información cumple con los requisitos de 44 U.S.C. § 3507, según enmendada por la sección 2 de la Ley de Reducción de Documentos de Trámites de 1995. No tiene que contestar estas preguntas a menos que la mostremos un número de control de la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés). Calcularán que le tomará alrededor de 3 minutos en llenar este formulario. Puede enviar comentarios sobre nuestro cálculo de tiempo a: SSA, 9401 Security Blvd. Baltimore, MD 21235-8401. Envíe solo los comentarios sobre nuestro cálculo de tiempo a esta dirección, pero no envíe el formulario.

AVISO PARA EL DIARIO DEL NÚMERO DE SEGURO SOCIAL

La Empresa o su agente han firmado un acuerdo con la Administración del Seguro Social que, entre otras cosas, incluye restricciones en cuanto a la divulgación y uso adicional de la verificación del número de Seguro Social. Para ver una copia del acuerdo modelo completo, visite https://www.ssa.gov/ibsv/docs/SampleUserAgreement.pdf (solo disponible en inglés).
CERTIFICATION STATEMENT FOR
PERMITTED ENTITIES USING THE SSN VERIFICATION PROCESS
(Signature required biennially)

Name and address of company:
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

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

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

1. The permitted 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 permitted 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 2 years old or the permitted entity cannot attest to any one of the four declarations.

[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.]

Name__________________________________________________________
Title___________________________________________________________
Phone Number____________________________________________________
Signature__________________________________________ Date___________
Exhibit C – SSA Written Consent Template

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

I authorize the Social Security Administration (SSA) to verify my Social Security number (SSN) (to match my name, SSN, and date of birth with information in SSA records) and to provide [name of Financial Institution/Permitted Entity] a match or no-match response concerning the results of the SSN verification for the following purpose(s):

[Electronic Signature that meets SSA’s electronic signature requirements]