Justification for Non-Substantive Changes for Electronic Consent Based Social Security Number Verification
20 CFR 401.100
OMB No. 0960-0817

Background

On March 19, 2025, the Acting Commissioner of the Social Security Administration released a statement entitled "Social Security Announces Cost Reduction and Enhancements Plan." This plan comprises three key components related to the Electronic Consent Based Social Security Number Verification (eCBSV) service. The first component does not require changes to the eCBSV information collections. However, the second component focuses on the necessity for enhancements to the service, responding to the findings of the 2024 GAO audit and the financial industry's robust backing for expanding the no-match response, which is seen as an essential measure in addressing synthetic identity fraud and improving customer identity verification processes. These enhancements require us to update our eCBSV User Agreement.

Along with the enhancements to the service, previous feedback from the financial industry hinted at additional changes to the eCBSV User Agreement including the removal of the obligation for the Permitted Entity to select a higher tier upon renewal for the advanced tier.

To that end, we are making revisions to the eCBSV User Agreement and accompanying consent Form, SSA-89, and the Consent Template language we include along with the User Agreement.

We expect to implement these revisions on **May 31, 2025**. Therefore, we are requesting OMB approval no later than **Tuesday, May 27, 2025**, to ensure we have adequate time to complete post approval activities prior to implementation.

Note: Once we obtain OMB approval for this Change Request, we will begin the full OMB approval process to ensure the public can comment on these changes.

Justification for Non-Substantive Changes to the Collection

We are making the following revisions to this collection:

- **Change #1:** SSA will enhance the no-match results provided by eCBSV via the application programming interface (API). We will complete this through providing details specifying which data element(s) do not align with its records in the response.

  Justification #1: This enhancement addresses stakeholder requests and the findings of the 2024 GAO audit, which called for more detailed information to assist in decision-making for combating synthetic identity fraud and enhancing customer identity verification processes.

- **<u>Change #2</u>:** We are revising sections I, 'Purpose and Definitions,' and II, 'SSN Verification Does Not Provide Proof or Confirmation of Identity,' of the eCBSV User Agreement to include clarifying details about the data element(s) that do not align with the information in SSA's records:
    - Revision to section I, Purpose and Definitions:
        - **From:**
          SSN Verification –The response SSA discloses to the Permitted Entity or Financial Institution after conducting a verification of the SSN holder's Fraud Protection Data.

        - **To:**
          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

    - Revision from section II, 'SSN Verification Does Not Provide Proof or Confirmation of Identity:
        - **From:**
          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.***

        - **To:**
          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.***

Justification #2: These revisions are necessary to incorporate the additional disclosure regarding the verification result of a 'no' match response.

- **Change #3:** We are revising section III, 'Responsibilities' of the eCBSV User Agreement to include clarifying details that 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. Also, that the 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.
    - **From:**

      21. The Permitted Entity and any Financial Institution(s) it services must not reuse the SSN Verification. The Permitted Entity and any Financial Institution(s) it services may mark their own records as "verified" or "unverified."

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

    - **To:**

      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).

Justification #3: This change is essential to address the increased disclosure risk faced by the agency, as well as to implement mitigation strategies.

Note: There is no change to the language in the last bullet; however, we have renumbered it to #23 as we added a new #22 to the revised section.

- **Change #4:** We have revised section VI, 'Cost of Service,' of the User Agreement to remove the obligation for the Permitted Entity to select a higher tier upon renewal for the advanced tier and to revise the language discussing the tiers:
  - **Revision to 2nd Paragraph:**
    - **From:**
      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.

    - **To:**
      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.

  - **Revision to 4th Paragraph:**
    - **From:**
      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 any tier, including a lower tier, for the next 365-day agreement. No interest shall accrue to the advance payment.

    - **To:**
      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.

Justification #4: We are making these changes to respond to requests from the financial industry for increased flexibility in both costs and service utilization.

- **Change #5:** We are revising section VII, 'Duration of User Agreement, Suspension of Services, and Waiver of Right to Judicial Review' of the User Agreement to clarify legal responsibilities if the Permitted Entity is dissolved as a corporate entity, and to revise the language to allow for the possibility of a new corporate entity purporting to acquire the Permitted Entity's User Agreement:
  - **From:**

    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.

  - **To:**

    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.

Justification #5: We are making this change to clarify this language to acknowledge that we require companies to provide SSA with a copy of each consent collected in the last 3 years, before a company decides not the renew, terminates, or is dissolved, to ensure that SSA will have documentation to support each SSN verification disclosed, if needed. This helps to ensure that the company collected consent, as required under the user agreement, prior to requesting an SSN verification from SSA.

If someone contests SSA's verification under the Privacy Act, this will ensure that SSA has access to necessary information to support SSA's defense. Access to the records could also assist the agency in determining whether to engage in future data exchanges with this company should it seek to reestablish the relationship in the future. Absent this mitigating action, a company could elude the audit process that would otherwise identify compliance concerns.

- **Change #6:** We are revising section VIII, 'Audit Requirements,' of the User Agreement to state that every Financial Institution serviced by the Permitted Entity, if any, will be subject to an initial audit once within the first five (5) years:
  - **From:**

    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.

  - **To:**

    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.

Justification #6: We are updating the audit requirements for all eCBSV customers, including both those in good standing and those with previous violations. We believe that the current violation percentage (8%) falls within the agency's acceptable risk threshold. Also, by modifying the timing we can significantly reduce the cost of the audit cycle while improving overall efficiency and audit readiness.

- **Change #7:** We are revising Section XV, 'Contacts,' of the User Agreement to update the SSA contacts listed in #3:
  - **From:**

    3) Reporting Lost, Compromised or Potentially Compromised SSN Verifications or Written Consents
    Office of Data Exchange, Policy Publications, and International Negotiations
    Project Manager: Vivian Adebayo 410-965-1702
    Alternate Contact: Curtis Miller 410-966-2370

  - **To:**

    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

Justification #7: We are making this change to ensure we include the names and phones numbers for the new SSA contacts appear in the User Agreement.

- **Change #8:** In 'Exhibit B – Form SSA-89 and SSA-89-SP' of the eCBSV User Agreement, we are revising the paragraph under the main consent section of Form SSA-89 (Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification) to include clarifying details about the data element(s) that do not align with the information in SSA's records:
    - **From:**
      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 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 is false to obtain information from Social Security records, I could be found guilty of a misdemeanor and fined up to $5.000.

    - **To:**
      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 response 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.

  Justification #8: We are making this change to incorporate the additional disclosure regarding the verification result of a 'no' match response, and to update the consent language based on our agreement with the Office of Management and Budget (OMB).

- **Change #9:** In 'Exhibit C - SSA Written Consent Template of the eCBSV User Agreement,' we are revising both options to include clarifying details about the data element(s) that do not align with the information in SSA's records:
    - **From:**
      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. 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. 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.

- **To:**

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.

Justification #9: We are making this change to incorporate the additional disclosure regarding the verification result of a 'no' match response. In addition, the updated language reflects the agreed-upon revisions to the consent language based on our discussions with OMB.

SSA will proceed with the implementation of the IT modifications, User Agreement, SSA-89, and changes to the Consent Language once OMB approval is granted. These changes will not impact the public reporting burden. We aim to incorporate these screens in a release anticipated for May 31, 2025. Therefore, we are requesting OMB approval no later than **Tuesday, May 27, 2025**, to ensure we have adequate time to complete post approval activities prior to implementation

Note: Once we obtain OMB approval for this Change Request, we will begin the full OMB approval process to ensure the public can comment on these changes.