Electronic Consent Based Social Security Number Verification (eCBSV) Service

Name of project.

Electronic Consent Based Social Security Number Verification (eCBSV) Service

Unique project identifier.

PID 9563

Contact name and telephone number.

Associate Commissioner

Office of Data Exchange, Policy Publications, and International Negotiations

Social Security Administration

6401 Security Blvd.

Baltimore, MD 21235

Describe the information to be collected, why the information is being collected, the intended use of the information and with whom the information will be shared.

The electronic Consent Based Social Security Number (SSN) Verification (eCBSV), is a fee-based SSN verification service that supports Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (Banking Bill), signed into law by the President of the United States on May 24, 2018. Section 215 of the Banking Bill, titled Reducing Identity Fraud, was passed to reduce the prevalence of synthetic identity fraud, which is a type of fraud where someone combines real and fake information to create a new identity. Section 215 of the Banking Bill requires SSA to provide a permitted entity, which is a financial institution or a financial institution's service provider, subsidiary, affiliate, agency, subcontractor, or assignee, a confirmation (or non-confirmation) of fraud protection data (i.e., name, date of birth, and Social Security number (SSN)) (SSN verification) based on the number holder's written or electronically signed consent.

To meet the requirements of section 215 of the Banking Bill, SSA is developing a new service, the eCBSV service, to perform SSN verifications for permitted entities. The eCBSV service will allow permitted entities to submit to SSA, one or more individual

requests for an SSN verification electronically for real-time machine-to-machine (or similar functionality) responses; and multiple requests electronically, such as those provided in a batch format.

To register with SSA for use of the eCBSV service, we will collect and maintain personally identifiable information (PII) from authorized users of each permitted entity registering to use eCBSV. This information includes point of contact information, such as the names, business phone numbers, and business emails of primary and alternate contact's, and authorizing officials. This information will be used primarily for management information and audit purposes in order to effectively administer eCBSV and ensure the authorized and appropriate use of the eCBSV service. We generally will use this information only as necessary for these administrative purposes or as otherwise authorized by law.

Once registered, permitted entities will be collecting and maintaining within their own systems consent forms, signed by number holders, needed to conduct SSN verifications. Number holders authorizing SSA to disclose the SSN verifications to permitted entities will have several options to sign consents. One option is signing an SSA-89, Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification consent form with a wet signature. Section 215 also permits the use of electronic signatures on agency-approved consent forms, so long as such signatures conform to requirements set forth in section 106 of the Electronic Signatures in Global and National Commerce Act and the eCBSV User Agreement. SSA will not receive consent forms collected and maintained by permitted entities prior to disclosing the SSN verification. However, in accordance with the Banking Bill, SSA will not disclose SSN verification responses to permitted entities unless SSA has received a Permitted Entity Certification, by which each permitted entity and financial institution has certified that it is in compliance with section 215 of the Banking Bill and signed the User Agreement. In accordance with section 215 of the Banking Bill, the terms of the User Agreement, and the number holder's signed consent form, Permitted Entities are only allowed to use the SSN verification for a purpose set forth in section 215 of the Banking Bill. The eCBSV user agreement also prohibits the permitted entities' resale and/or re-disclosure of the SSN verification. SSA is only authorized to use the SSN verification information provided by permitted entities to conduct the match in our systems to respond to the SSN verification requests, and for audit review purposes to ensure a permitted entity's compliance with our consent and other requirements as outlined in the eCBSV user agreement.

Describe the administrative and technological controls that are in place or that are planned to secure the information being collected.

Information Collected and Maintained by Permitted Entities

Permitted entities are required to protect the confidentiality of the physically or electronically signed consent forms, as well as the SSN verification response provided by SSA. Such protection requirements are thoroughly documented in the eCBSV user agreement, which permitted entities are required to review, complete, and sign prior to using the eCBSV service. Any effort to (1) misuse any SSN verification obtained or (2) request an SSN verification regarding a number holder under false pretenses, or without the written or electronically signed consent of the number holder, is unauthorized and violates the criminal provisions of the Privacy Act of 1974, which may subject permitted entities and their authorized users to fines, imprisonment, or both.

We are taking appropriate measures to protect access to, and prevent unauthorized disclosure of the SSN verifications we provide permitted entities. Such measures include but are not limited to:

- Mandating permitted entities provide the required certification to SSA per the Banking Bill before requesting confirmation of fraud protection data to confirm:
    - The entity is a permitted entity;
    - The entity is in compliance with section 215 of the Banking Bill;
    - 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 SSA pursuant to section 215 of the Banking Bill; and
    - The entity will retain sufficient records to demonstrate its compliance with its certification and section 215 of the Banking Bill for a period of not less than 2 years.
- Authenticating permitted entities seeking to access the eCBSV service via our Enterprise Authentication and Authorization for Entities and Affiliates application and by Access Control Utility/DataPower services.
- Only allowing permitted entities to request verifications from us after they have completed and signed an eCBSV User Agreement outlining terms, conditions, and penalties for non-compliance.
- Requiring permitted entities to secure a number holder's consent in a manner consistent with the requirements set forth in the eCBSV User Agreement before submitting SSN verification requests to SSA.
- Requiring permitted entities, when submitting SSN verification requests, to indicate whether each consent received is physically or electronically signed. Input records that do not indicate number holder consent, either wet or electronic, will not be processed through the eCBSV service.

- Minimizing the information we provide in response to eCBSV verification requests to a "yes", "no", or "death indicator" and not providing any additional PII about the number holder to the permitted entity.
- Informing permitted entities through the eCBSV User Agreement that the SSN verifications we provide should be used solely to fulfill the purpose of section 215 of the Banking Bill, which is to reduce synthetic identity fraud, not to identity proof and/or authenticate an individual.
- Outlining in the eCBSV user agreement requirements that permitted entities must safeguard the SSN verifications and Written Consents in a manner consistent with applicable system security and privacy requirements.
- Subjecting permitted entities to periodic audits conducted by an independent private sector Certified Public Accountant who will document and report findings to us.
- Having the ability to make onsite inspections of a permitted entity's place of business and electronic systems/repositories associated with the SSN verifications and written consents under section 215 of the Banking Bill to ensure compliance with all applicable requirements outlined in the eCBSV user agreement.

Information Collected and Maintained by the Social Security Administration

The Office of Information Security has performed an authentication and security risk analysis for the eCBSV service. The latter includes an evaluation of security and audit controls proven to be effective in protecting the information collected, stored, processed, and transmitted by this information system. These include technical, management, and operational controls (i.e., Single Sign On role-based access via personal identity verification cards, storing records in secure areas accessible only to those SSA employees who require the information to perform their official duties, and requiring all employees who access information systems that maintain PII to sign a systems sanctions document annually that acknowledges penalties for unauthorized access to, or disclosure of, such information) that permit the safeguarding of, and access to, our information only to our employees with a "need to know," and the minimum amount of access that allows them to perform their job functions. Audit mechanisms are in place to record sensitive transactions as an additional measure to protect information from unauthorized disclosure or modification.

Describe the impact on individuals' privacy rights.

We collect information (including PII) only where we have specific legal authority to do so in order to administer our responsibilities under the Social Security Act or other applicable laws.

We will only collect and maintain the minimum amount of information necessary from permitted entities and their authorized users to administer our responsibilities under section 215 of the Banking Bill.

For the purposes of eCBSV, Permitted entities are limited to collecting, maintaining, and submitting number holders names, dates of birth, and Social Security numbers per section 215(b)(3) of the Banking Bill.

We advised participants of eCBSV of our legal authority for requesting information, the purposes for which we will use and disclose the information, and the consequences of not providing any or all of the requested information in the Supporting Statement for Electronic Consent Based Social Security Number Verification, published in the Federal Register on [December 5, 2019] at 84 FR 66704.

Are individuals afforded an opportunity to decline to provide information?

Yes, permitted entities and their authorized users can decline to provide information at time of registration or when submitting SSN verification requests. However, failing to provide all or part of the information requested may prevent them from participating in the eCBSV program or receiving accurate and timely responses to SSN verification requests they submit.

Number holders may decline to sign the consent presented by the permitted entity authorizing SSA to disclose the SSN verification. However, doing so may prevent or delay them from receiving the requested product or service they are seeking to obtain from the permitted entity.

Are individuals afforded an opportunity to consent to only particular uses of the information?

Number holders for whom we disclose an SSN verification must consent to allowing us to disclose to the permitted entity the SSN verification response. The use of the SSN verification response by the permitted entity and their authorized users is limited to the purpose(s) specified in the eCBSV user agreement.

Does the collection of this information require a new System of Records Notice (SORN) under the Privacy Act (5 U.S.C. § 552a) or an alteration to an existing SORN?

A SORN is not required for the information we collect from permitted entities' authorized users for the purposes of registering them to use the eCBSV service, as such information is associated with corporations and organizations, which do have any

Privacy Act rights (5 U.S.C. § 552(a)(2). Additionally, any information associated with individuals collected for the purposes of registering a permitted entity will not be retrieved by personal identifier and therefore, not maintained in a manner that constitutes a SORN under the Privacy Act.

A SORN is not required for the collection of the number holders' information on the consents to disclose the SSN verification. The information captured on these consent forms is maintained by permitted entities and will not be retrieved using personal identifiers. Therefore, they do not constitute a System of Records (SOR) under the Privacy Act.

A SORN is not required for the fraud protection data we receive and maintain from permitted entities for the purposes of providing a SSN verification and auditing since such information will not be maintained in a manner that constitutes a SOR under the Privacy Act. Retrieval of this data will not be through the use of any personal identifiers. Instead, retrieval will be via permitted entity name and date range.

There is currently a SORN that covers the system we will use to verify the information submitted to us from permitted entities. This system is covered under SORN 60-0058, Master Files of Social Security Numbers (SSN) Holders and SSN Applications.

PIA CONDUCTED BY PRIVACY OFFICER, SSA:

7/13/20

_____ _____

Matthew D. Ramsey DATE

Executive Director

Office of Privacy and Disclosure

PIA REVIEWED BY THE SENIOR AGENCY PRIVACY OFFICIAL, SSA:

7/15/2020

Royce Min DATE

General Counsel

Senior Agency Official for Privacy