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

A. Technical Specifications and Systems Security

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

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

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

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

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

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

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

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

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

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

also ensure that SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands). The Permitted Entity shall ensure that any entity involved with storing the SSN Verifications are United States based entities bound by the laws within the United States (notwithstanding the physical location of the business). .

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

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

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

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

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

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

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

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

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

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

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