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

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 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 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.