IV. Consent

B. Retention

The Permitted Entity or Financial Institution it services, if any, that creates, receives, or has access to Supporting Documentation must retain the Supporting Documentation for a period of five (5) years from the date of the SSN Verification request, either electronically or in paper form. The Permitted Entity obtaining or having access to the Written Consent 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 or Financial Institution, if any, with access to the Written Consent, evidence documenting specific purpose, or SSN Verification must also protect those records from loss or destruction by taking the measures below. (See section V.B for procedures on reporting loss of SSN Verifications or Written Consents). The Permitted Entity or Financial Institution it services shall restrict access to the Written Consent and SSN Verification 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.20, the stored Written Consent and SSN Verification must not be reused.

If the Permitted Entity or Financial Institution obtaining the Written Consent in paper format and chooses to retain the Written Consent in paper format, that entity must store the Written Consent in a manner that meets all regulatory requirements

If the Permitted Entity or Financial Institution obtains Written Consents electronically, or chooses to convert original paper copies of Written Consents to electronic versions, the Permitted Entity and any Financial Institutions it services, if any, must retain the Written Consents in a way that accounts for integrity of the Written Consents 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. SSN Verifications must also be protected in this manner.

When storing a Written Consent electronically, the Permitted Entity must destroy any original Written Consent in paper form.