Sample Identity Theft Prevention Policy

PURPOSE

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account. To provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, and South Carolina Act 190 of 2008; Financial Identity Fraud and Identity Theft Protection Act.

DEFINITIONS

Covered Account: means an account that an entity or department of _____(County/entity name) offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions for which there is a reasonably foreseeable risk to customers or to the safety and soundness of account information from identity theft, including financial, operational, compliance, reputation or litigation risks.

Financial Identity Fraud: as defined in SC Code of Laws §16-13-510.

Identity Theft: means fraud committed or attempted using the identifying information of another person without authority, and includes any terms and definitions as defined in SC Code of Laws §16-13-510.

Personal Identifying Information: means personal information as defined in SC Code of Laws §16-13-510(D). It does not mean information about vehicular accidents, driving violations, and driver's status.

Security Breach: means an incident of unauthorized access to and acquisition of records or data that was not rendered unusable through encryption, redaction, or other methods containing personal identifying information that compromises the security, confidentiality, or integrity of personal identifying information maintained by a person when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer.

Red Flag: means a pattern, practice or specific activity that indicates the existence of possible identity theft.

PROGRAM

_____ (County/entity) establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;

2. Detect red flags that have been incorporated into the Program;

3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;

4. Eliminate risk factors that are determined to increase the risk of a security breach;

5. Minimize the instances that lawfully obtained personal identifiable information is disseminated as required pursuant to applicable portions of South Carolina Act 190 of 2008;

6. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor form identity theft.

ADMINISTRATION

1. _____ (the entity's governing body, an appropriate committee of the entity or a designated person at the level of senior management) shall be responsible for the development, implementation, oversight and continued administration of the program;

2. The Program shall train staff as necessary, to effectively implement the program; and

3. The Program shall exercise appropriate and effective oversight of service provider arrangements.

MANAGEMENT AND SECURITY OF PERSONAL IDENTIFYING INFORMATION

_____ (the entity's governing body, an appropriate committee of the entity or a designated person at the level of senior management) shall enact procedures to manage and secure lawfully obtained personal identifying information maintained so that it shall only be disseminated internally for use by employees of the entity for legitimate business reasons, and externally to the general public only for reasons authorized by state, federal or local statutes;

_____ (county entity) shall disclose a breach in the security data to a resident of this state whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person, when the illegal use of the information has occurred or is reasonably likely to occur. Disclosure shall be done in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement

as provided in SC Code of Laws §1-11-490(C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

IDENTIFICATION OF RED FLAGS

1. The Program shall include relevant red flags from the following categories as appropriate:

a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
b. The presentation of suspicious documents;
c. The presentation of suspicious personal identifying information;
d. The unusual use of, or other suspicious activity related to, a covered account; and
e. Notice from customers, victims of identity theft, law enforcement authorities, state, federal or local government entities, or other persons regarding possible identity theft in connection with covered accounts.

2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:

a. The types of covered accounts offered and maintained;
b. The methods provided to open covered accounts;
c. The methods provided to access covered accounts; and
d. Its previous experience with identity theft.

3. The program shall incorporate relevant red flags from sources such as:

a. Incidents of identity theft previously experienced;
b. Methods of identity theft that reflect changes in risk; and
c. Applicable supervisory guidance.

DETECTION OF RED FLAGS

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information, and verifying the identity of a person opening a covered account; and

2. Authenticating individuals, monitoring transactions, and verifying the validity of change of account information requests in the case of an existing covered account.

RESPONSE

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent and mitigate identity theft;

4. Changes in the business arrangements of the organization.

OVERSIGHT OF THE PROGRAM

Oversight of the Program shall include:

1. Assignment of specific responsibility for implementation of the program;

2. Review of reports prepared by staff regarding compliance; and

3. Approval of material changes to the Program as necessary to address changing risks of identity theft.

Reports shall be prepared as follows:

1. Staff responsible for development, implementation and administration of the Program shall report to _____ (appropriate designated person/committee) at least annually on compliance by the organization with the Program.

2. The report shall, at a minimum, address material matters related to the program and evaluate the following:

a. The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
b. The minimum standards that vendors must adhere to pursuant to a Service provider agreement;
c. Significant incidents involving identity theft and management's response; and
d. Recommendations for material changes to the Program.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The organization shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

DUTIES REGARDING DATA DISCREPANCIES

The organization shall develop policies and procedures designed to enable the organization to form a reasonable belief that customer data relates to the consumer for whom it was requested if the organization receives a notice of discrepancy from a nationwide consumer reporting agency indicating the data given by the consumer differs from data contained in the consumer report.

1. The organization may reasonably confirm that account data is accurate by any of the following means:

a. Verification of the data with the consumer;
b. Review of the utility's records;
c. Verification of the data through third-party sources; or
d. Other reasonable means.

2. If accurate data is confirmed, the organization shall furnish the consumer's data to the nationwide consumer reporting agency from which it received the notice of discrepancy if:

a. The organization establishes a continuing relationship with the consumer; and
b. The organization, regularly and in the ordinary business, furnishes information to the consumer reporting agency.